

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ “ВАСИЛ ЛЕВСКИ”

ФАКУЛТЕТ “АРТИЛЕРИЯ, ПВО И КИС”

Катедра “Информационна сигурност”

**НАУЧНА КОНФЕРЕНЦИЯ
с международно участие**

ОБЛАЧНИТЕ СТРУКТУРИ И ЗАЩИТАТА НА ИНФОРМАЦИЯТА

СБОРНИК НАУЧНИ ТРУДОВЕ

**ШУМЕН
2016**

КЪМ ЧИТАТЕЛИТЕ ...

Сборникът научни трудове е съставен от докладите, изнесени на научна конференция на тема „Облачните структури и защитата на информацията“, проведена във Факултет „Артилерия, противовъздушна отбрана и комуникационни и информационни системи“ към Националния военен университет „Васил Левски“ - гр. Шумен, на 12 и 13 май 2016 г.

Докладите са представени за издаване от авторите без допълнително редактиране от издателите. Отговорността за фактологическите, технически, езикови грешки и произтичащите от това последствия носят изцяло авторите.

Съгласно чл. 31 от Закона за защита на класифицираната информация авторите сами определят грифа за сигурност на докладите си и носят лична отговорност за публикуване на класифицирана информация в тях.

Всеки доклад е рецензиран от две хабилитирани лица.

От редакционната колегия

Редакционна колегия:

полк. инж. доц. д-р Сашо Стефанов Евлогиев – председател;
полк. инж. доц. д-р Росен Атанасов Богданов,
проф. д.в.н. Манол Петков Млеченков,
доц. д-р Николай Йорданов Досев,
доц. д-р Жанета Николова Савова-Ташева - членове;
Светлана Маркова Зотова, Христо Пеев Христов - сътрудници

Рецензенти:

Председател: полк. доц. д-р инж. Сашо Стефанов Евлогиев
Полк. доц. д-р Велико П. Петров – направление „Държава и сигурност“
Проф. д.в.н. Манол П. Млеченков – направление „Информационна сигурност“
Доц. д-р Георги Н. Мазаджиев - направление „Информационна сигурност“
Доц. д-р Жанета Н. Ташева - направление „Информационна сигурност“
Доц. д-р Николай Й. Досев - направление „Държава и сигурност“

©НВУ „В. Левски“ – Факултет „Артилерия, ПВО и КИС”

Шумен, 2016

с/о Jusautor, Shumen

ISBN 978-954-9681-73-4

СЪДЪРЖАНИЕ

ПЛЕНАРНА СЕСИЯ	6
<i>Б. Ив. Симитчиев, ОБЛАЧНИТЕ ИНФОРМАЦИОННИ ТЕХНОЛОГИИ И ЗАЩИТАТА НА ИНФОРМАЦИЯТА</i>	6
<i>О. А. Исмаилов, ДОБРИ ПРАКТИКИ И СТАНДАРТИ ЗА ФИЗИЧЕСКА СИГУРНОСТ ПРИ РАБОТА В ОБЛАКА.....</i>	24
<i>В. Ц. Целков, ТЕХНОЛОГИЧЕН МОДЕЛ ЗА ОБРАБОТКА НА ДАННИ В ОБЛАКА.....</i>	32
<i>Marián Babjak, Zdeněk Matoušek, Ján Ochodnický, BINARY INTRAPULSE MODULATIONS FOR RADAR PULSE COMPRESSION</i>	41
<i>Roman Berešík, APPLICATIONS OF SOFTWARE DEFINED RADIOS IN WIRELESS SENSOR NETWORKS.....</i>	50
<i>A. T. Peshev, BEST PRACTICES IN BUILDING PRIVATE CLOUD</i>	55
<i>Ц. Цолов, ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ И НОВИТЕ ЕВРОПЕЙСКИ РЕГУЛАЦИИ</i>	63
<i>Ив. П. Иванов, Н. Т. Стоянов, АНАЛИЗ НА АРХИТЕКТУРИ ЗА ОБЛАЧНИ УСЛУГИ.....</i>	85
<i>Д. Ст. Караколев, г. В. Ахмедова, ТЕНДЕНЦИИ В ДЕЙНОСТТА НА ИЗПЪЛНИТЕЛНА АГЕНЦИЯ ЕСМИС ЗА ПРИЛАГАНЕТО НА ОБЛАЧНИ ТЕХНОЛОГИИ В СФЕРАТА НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ.....</i>	94
<i>М. В. Захариев, Д. Е. Кръстева, АВТОМАТИЗИРАНО ПРОФИЛИРАНЕ В КОНТЕКСТА НА ГАРАНТИРАНЕ НА НАЦИОНАЛНАТА СИГУРНОСТ... ..</i>	101
<i>А. Н. Инков, Д. Л. Полимирова, НАБЛЮДЕНИЕ НАД ХАРАКТЕРИСТИКИ ЗА СИГУРНОСТ И ТЯХНОТО ПРИСЪСТВИЕ И СТОЙНОСТИ СРЕД БЪЛГАРСКИТЕ УЕБ САЙТОВЕ</i>	113
ДЪРЖАВА И СИГУРНОСТ	119
<i>Д. С. Манолов, МЯСТО НА ИНФОРМАЦИОННА СИСТЕМА „ЛОГИСТИКА НА БА“ В СТРАТЕГИЧЕСКОТО УПРАВЛЕНИЕ НА СНАБДЯВАНЕТО В БЪЛГАРСКАТА АРМИЯ.....</i>	119
<i>Д. С. Манолов, КРИТЕРИЙ ЗА ОЦЕНЯВАНЕ НА ЕФЕКТИВНОСТТА НА УПРАВЛЕНИЕТО НА ОБЩЕСТВЕНИТЕ ПОРЪЧКИ В МИНИСТЕРСТВО НА ОТБРАНАТА.....</i>	123
<i>Д. С. Манолов, ОСНОВНИ НАПРАВЛЕНИЯ В ПОДГОТОВКАТА И ОРГАНИЗИРАНЕТО НА ПРОЦЕДУРА ЗА ВЪЗЛАГАНЕ НА ОБЩЕСТВЕНА ПОРЪЧКА В МИНИСТЕРСТВО НА ОТБРАНАТА</i>	129
<i>С. Д. Салтирова-Радкова, ДОГОВОРЪТ ЗА ВОЕННА СЛУЖБА СПОРЕД ДЕЙСТВАЩОТО БЪЛГАРСКО ЗАКОНОДАТЕЛСТВО.....</i>	134
<i>С. Д. Салтирова-Радкова, ПРЕСТЪПЛЕНИЯТА СРЕЩУ МАЛОЛЕТНИ И НЕПЪЛНОЛЕТНИ КАТО ЗАПЛАХА ЗА СИГУРНОСТТА НА СТРАНАТА</i>	141

<i>С. Д. Салтирова-Радкова, СТАТУТ НА ДЪРЖАВНИТЕ СЛУЖИТЕЛИ В МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ.....</i>	145
<i>Д. В. Диманова, ОПАСНОСТ ОТ ХИМИЧЕСКИ АВАРИИ</i>	152
<i>Д. В. Диманова, НАЦИОНАЛНА СИСТЕМА ЗА ЗАЩИТА ПРИ БЕДСТВИЯ</i>	156
<i>Д. В. Диманова, ФУНКЦИИ НА ОРГАНИТЕ НА ИЗПЪЛНИТЕЛНА ВЛАСТ ЗА ЗАЩИТА ПРИ БЕДСТВИЯ.....</i>	161
<i>К. М. Марков, ПРОБЛЕМЪТ ЗА РИСКА В ОРГАНИЗАЦИЯТА.....</i>	165
<i>В. П. Петров, К. А. Илиев, ГЛОБАЛНАТА БОРБА С ИЗМЕНЕНИЕТО НА КЛИМАТА</i>	170
<i>К. А. Илиев, В. П. Петров, СЪВРЕМЕННИ ЗАПЛАХИ ЗА НАЦИОНАЛНАТА СИГУРНОСТ ОТ ВОЕНЕН ХАРАКТЕР</i>	180
<i>К. А. Илиев, МЕЖДУНАРОДНОТО ХУМАНИТАРНО ПРАВО – ФАКТОР В СЪВРЕМЕННИТЕ ВОЕНИ КОНФЛИКТИ.....</i>	190
<i>К. А. Илиев, НАЦИОНАЛНИТЕ СЪВМЕСТНИ СИЛИ - ГАРАНТ ЗА СИГУРНОСТ.....</i>	196
<i>Х. А. Христов, МОДЕЛ ЗА УПРАВЛЕНИЕ НА ОПЕРАЦИЯ ЗА РЕАГИРАНЕ ПРИ КРИЗА, ВЪЗНИКНАЛА ВСЛЕДСТВИЕ НА БЕДСТВИЕ ИЛИ АВАРИЯ</i>	202
<i>Х. А. Христов, КООРДИНАЦИЯ, ВЗАИМОДЕЙСТВИЕ И СЪТРУДНИЧЕСТВО ПРИ ПРЕОДОЛЯВАНЕ НА КРИЗИ, ПОРОДЕНИ ОТ БЕДСТВИЯ И АВАРИИ.....</i>	210
ИНФОРМАЦИОННА СИГУРНОСТ	217
<i>В. Ц. Целков, О. А. Исмаилов, М. Г. Божилова, ОДИТ НА СИГУРНОСТТА НА ИНФОРМАЦИОННИ СИСТЕМИ, СВЪРЗАНИ С ИНТЕРНЕТ.....</i>	217
<i>А. А. Колев, С. Р. Маринов, И. П. Иванов, ОБЛАЧНА СРЕДА НА КОМУНИКАЦИОННО-ИНФОРМАЦИОННА СТРУКТУРА ЗА МРЕЖОВО-ЦЕНТРИЧНИ ОПЕРАЦИИ.....</i>	227
<i>И. П. Иванов, АРХИТЕКТУРА НА ОБЛАЧНА МРЕЖА ЗА РАДИОДОСТЪП ЗА НУЖДИТЕ НА СИГУРНОСТТА И ОТБРАНАТА</i>	235
<i>И. Н. Лилов, И. Й. Георгиев, ПРИЛОЖЕНИЕ НА ЛИНЕЙНОТО ОПТИМИРАНЕ В УПРАВЛЕНИЕТО НА СИСТЕМИТЕ ЗА ИНФОРМАЦИОННА СИГУРНОСТ</i>	241
<i>Д. Т. Дойчинов, МОДЕЛИ ЗА КОНТРОЛ НА ДОСТЪПА ДО ИНФОРМАЦИЯ</i>	248
<i>В. Т. Стоянова, ВЪЗМОЖНОСТИ ЗА КОМПЮТЪРНА СТЕГАНОГРАФИЯ В ОБЛАЧНИТЕ ТЕХНОЛОГИИ.....</i>	257
СТУДЕНТСКО-ДОКТОРАНТСКА СЕКЦИЯ	262
<i>Ф. Цв. Филипов, ОБРАБОТКА НА АКУСТИЧНИЯ СИГНАЛ ПРИ ЛОКАЛИЗАЦИЯ НА ЗВУКОВИ ИЗТОЧНИЦИ</i>	262

<i>Вл. П. Крумов</i> , ПРОЕКТЪТ ЗА НАЦИОНАЛНА СТРАТЕГИЯ ЗА КИБЕР СИГУРНОСТ И ОТРАЖЕНИЕТО МУ ВЪРХУ ПОДОБРЯВАНЕ НА ЕФЕКТИВНОСТТА НА УПРАВЛЕНИЕТО НА ИНЦИДЕНТИ В ИНФОРМАЦИОННАТА СИГУРНОСТ	268
<i>Ал. Д. Куманов, А. С. Чучуков</i> , ПРАВЕН РЕЖИМ НА ЗАЩИТАТА НА ИНФОРМАЦИЯТА В БЪЛГАРСКОТО ЗАКОНОДАТЕЛСТВО	272
<i>С. А. Алиев, С. С. Станев</i> , КОЛАБОРАЦИЯТА И ИНТЕГРАЦИЯТА МЕЖДУ ОБЛАЧНИТЕ УСЛУГИ С ИНТЕРНЕТ НА НЕЩАТА – СИГУРНОСТ И ЗАЩИТА НА ДАННИТЕ	277
<i>Д. А. Еминов, С. И. Хасанова, Г. И. Зекерие, С. Д. Ниязиев</i> , ЗАЩИТАТА НА ОБЛАЧНАТА СИГУРНОСТ И АТАКИТЕ КЪМ НЕЯ	283
<i>Ст. А. Петкова</i> , ЗАЩИТА НА ИНФОРМАЦИЯТА В ОБЛАЧНИТЕ ТЕХНОЛОГИИ	289

ПЛЕНАРНА СЕСИЯ

ОБЛАЧНИТЕ ИНФОРМАЦИОННИ ТЕХНОЛОГИИ И ЗАЩИТАТА НА ИНФОРМАЦИЯТА

Бойко Ив. Симитчиев

Асоциация на комуникационните и информационни специалисти

I. Необходимост от въвеждане на новите технологии в държавното управление

Необходимостта от въвеждане на новите технологии в държавното управление е продиктувана от световните и европейски тенденции за търсене на методи и средства за значително повишаване на ефективността и ефикасността на управленческите процеси. Освен това е свързано и с необходимостта за значително намаляване на ресурсите (финансови, човешки и материални), заделени в сферата на държавното управление. Това може да се постигне чрез усъвършенстването на организацията на системата за управление на държавата и с въвеждането на нови иновативни технологии. Тези нови технологии позволяват да се постигнат преимущества пред сега използваните подходи за изграждане на информационните системи за управление като:

- снижаване цената на обработката на информацията за сметка на значителното увеличение на коефициента на натоварване на оборудването;
- повишаване на надеждността на съхраняване на данните;
- изискване за минимален начален капитал за създаване на инфраструктура на информационните системи;
- простота на обхвата на технологическите възможности на информационните системи;
- решаване на проблема, свързан с недостига на високо квалифицирани специалисти, за сметка на намаляване на техния брой и по тясна специализация;
- уеднаквяване управленческите процеси и технологии в ежедневието, по време на кризи и във военно време в органите и структурите на държавната и местна власт, съдебната и законодателна власт, администрациите създадени със специални закони.

С въвеждането на новите информационни технологии ще се постигне и изпълнението на целите и задачите, поставени в редица стратегически документи, разработени от държавата, а именно:

- „Стратегия за развитие на електронното управление в Република България 2014 – 2020 г.“, чрез изграждане на единна информационна среда за реализацията на базови услуги на електронното управление.

- Изискване за повишаване ефективността в работата на държавната администрация на централно, регионално и местно ниво, залегнало в „Стратегията за раз-

витие на държавната администрация 2014 -2020“ и „Доклад за състоянието на администрацията 2014 г.“ където е посочено, че чрез ускорено изграждане и развиване на електронно управление, правителството се стреми да осигури по-качествени и достъпни услуги за гражданите и бизнеса, да подобри ефикасността и ефективността на администрацията, да повиши прозрачността и отчетността, да намали корупцията, да създаде нови възможности за участие на структурите на гражданското общество в управлението. **Свързването на всички структури в единната информационна среда е основна предпоставка за развитието на е-управление.** Това ще доведе не само до съкращаване на допълнителните разходи на администрациите за достъп до интернет, но и до бърз трансфер на данни и ще намали употребата на документи на хартиен носител“.

В Доклада за състоянието на администрацията за 2014 г. е отбелязано, че към края на отчетния период броя на заетите в държавното управление служители е над 133 575 души. Те разполагат с 114 093 броя компютри, от които 15 017 преносими и 99 076 настолни.Общият брой на сървърите е 5 817 бр. Не е известен точният брой на допълнително инсталирани системи за съхранение на данни. Ако се приеме, че с тях общия брой ще достигне 6000 бр. бихме могли да направим следните приблизителни разчети:

1	Обща консумирана електрическа мощност за сървъри и устройства за съхранение на данни.	3000 kW
2	Обща консумирана електрическа мощност от системите за климатизация на сървърните помещения.	3000 kW
3	Годишни разходи за електроенергия.	6 млн. 923 хил. лева
4	Разположение на сървърите и устройствата за съхранение.	250-300 помещения; Обща площ - над 10 000 кв. м
5	Брой на използваните UPS за сървърите.	250-300 бр.
6	Общо годишни разходи за поддръжка и развитие на хардуера.	15 милиона лв.
7	Общо годишни разходи за поддръжка на сървърни лицензи и антивирусен софтуер.	15 милиона лева
8	Годишни разходи за алтернативни доставчици на Интернет.	1 597 668 лв.
9	Броят на заетите в поддръжка и развитие на ИКТ структури и специалисти.	Специализирани дирекции – 21 бр. Специализирани отдели - 45 бр. Отделни специалисти – 282 души. Договори за абонаментна поддръжка – 205 бр.
10	Общият брой служители, отговарящи за поддръжка и развитие на ИКТ в администрацията.	3592 души
11	Общо годишни разходи за поддръжка и развитие на ИКТ.	80 милиона лв.

- Отстраняване на констатираните недостатъци в **Одитен доклад № 0300000812 за извършен одит на развитието на електронното управление за периода от 01.01.2010 г. до 30.06.2012 г. на Сметната палата**, за по-ефективното и целесъобразно изразходване на заделените финансови средства за развитие на ИТ технологиите.

По оценките от одитния доклад за дейности по реализиране на електронното управление за целия период 2011 -2015 г. е усвоен публичен финансов ресурс в размер на не по-малко от 376 млн. лв. по текущи цени за 2011 г. По предварителен прогнозен разчет за периода 2015-2020 г. за електронно управление са предвидени над 1 млрд. лева. **Отсъствието на функционираща национална система за отчитане на разходите по хоризонтални политики не позволява идентифициране на общия размер на изразходваните средства за реализация на електронното управление в България.**

Задълбочения анализ на данните, посочени в тези документи показва, че държавата е заделяла и ще заделя не малък финансов ресурс за усъвършенстване на системата за управление на страната – приблизително по 200 – 250 млн лева годишно за ИТ. Това е ресурс, който ако се е използвал и използва ефективно би дал значителен ефект за усъвършенстване на управлението на страната. За съжаление данните не показват това. **Преди всичко това се дължи на липсата на каквато и да било интеграция на изгражданите ИТ проекти в отделните структури на държавната власт.** Това е довело до създаването на собствени, напълно несъвместими с други, информационни системи. Освен това % на използване на изчислителния ресурс е изключително нисък – не повече от 30 % . Освен това за поддръжка на тези системи се ползва значителен финансов и човешки ресурс.

С прилагането на новите информационни технологии в държавното управление“ ще се създаде **единна съвместна информационна среда (ЕСИС)**, която да е достъпна и използвана от всички държавни ведомства и администрации в Р България.

Това ще доведе до:

- рационално и целево използване на ресурсите за един кратък период от време ще повиши ефективността на управленческите възможности на държавата и ускори процеса на осъществяване на електронното управление в страната;

- повишаване на своевременността, достоверността, надеждността, сигурността и съвместимостта на обмена на информацията както между държавните структури, така също и между тях и гражданите и ефективността на използваните ресурси;

- създаване на цифрова администрация, особено за онези администрации, които не разполагат с финансов ресурс и квалифициран състав да внедряват електронното управление.

II. Прилагане на облачните информационни технологии

Създаването на единна съвместна информационна среда (ЕСИС) може да се извърши чрез използването на иновативни информационни технологии. През последните няколко години, в света на информационните технологии широка популярност добиха така наречените облачни изчисления (cloud computing), или още - облачни технологии.

Погледнато през призмата на времето, облачните технологии не са нещо ново и революционно. Историята, а и хората, занимавали се през 70-те, 80-те, 90-те

години на миналия век с информационни технологии, помнят така наречените "Изчислителни центрове", чиято съвременна форма са центровете за данни. В изчислителните центрове бе реализирана концентрация на голям за времето си изчислителен ресурс, който се ползваше на споделен принцип, в малка част от локални и в по-голямата си част от отдалечени потребители. Достъпът до изчислителните ресурси се осъществяваше чрез терминали, много наподобяващи днешните "тънки" клиенти, с използване на собствени или наети комуникационни линии между потребителите и центъра. В зависимост от привилегиите си, потребителите получаваха достъп до някакво готово приложение (например за резервация на самолетни билети), програмни езици и библиотеки, както и пространство за съхранение на собствени данни, или административен достъп, позволяващ им да контролират и управляват в определена степен хардуера и софтуера, до който имат достъп. Не звучи ли познато?

В днешния облак получаваме чрез компютърните мрежи софтуер като услуга (SaaS), платформа като услуга (PaaS) и инфраструктура като услуга (IaaS).

Чрез SaaS получаваме достъп до едно или повече приложения, предлагани от доставчика на услугата и какво пречи, едно от тях да бъде софтуер за резервация на самолетни билети?

Чрез PaaS имаме възможност да разработваме в облака собствени приложения, чрез програмните инструменти, предоставени от доставчика, както и да създадем собствени бази данни.

Чрез IaaS получаваме права да администрираме в определена степен хардуера и софтуера на предоставения от доставчика ресурс.

"Sub sole nihil novi est" (Нищо ново под слънцето), както са казали римляните.

Инфраструктурната и техническата реализация на изчислителните центрове в миналото е осъществявана или в полза на една отделна, териториално обособена организация, като например научно-изследователски институт, университет или предприятие, или в полза на една отделна териториално разпръсната организация, като например такава с няколко филиала, или за споделено ползване от няколко отделни организации, групирани обикновено на териториален принцип. Не звучи ли отново познато? Частен (private) облак на един университет, общностен (community) облак на консорциум от няколко търговски фирми или пък публичен (public) облак, предоставящ на клиентите си услуги чрез Internet.

За да бъдем в крак с новостите, следва да споменем, че напоследък публичност добиват още четири модела на облачни услуги: SaaS - System as a Service, SaaS - Security as a Service, DaaS - Data/Database as a Service и BaaS - Backend as a Service.

Моделът "System as a Service" предоставя на потребителя достъп до една или повече физически системи, собственост на доставчика и разположени в инфраструктура на последния. При този модел се избягват първоначалните разходи за придобиване, като примерно в 3 годишен план може да се спестят над 20% [i] от разходите, в сравнение със случая на придобиване.

Моделът "Security as a Service" предоставя на потребителя услуги като антивирусна защита, откриван на проникване (IDS), предотвратяване на проникване (IPS), защитни стени и др.

Моделът "Data/Database as a Service" предоставя на потребителя достъп до (бази) данни, събрани и анализирани от доставчика на услугата. По този начин потре-

бителят си спестява ресурса (труд, време, пари), който иначе би трябвало да изразходи, за да получи същите резултати, които доставчика му предоставя наготово.

И накрая, моделът "Backend as a Service" предоставя, главно на разработчиците на приложения за мобилни устройства, унифициран начин за достъп на тези приложения до облачни услуги като социални мрежи, дисково пространство и др.

Основното при тези технологии е, че чрез интегриране на изчислителните ресурси и използването на „виртуалните“ изчислителни машини се постига значително повишаване на % на натоварване на изчислителните ресурси, намаляване на консумираната електроенергия и финансовите средства за изграждане на различните инженерни съоръжения, необходими за надеждното функциониране на тези информационни системи. Предимствата на облачните информационни технологии пред останалите, използвани до сега е показана в сравнителната таблица:

Сравнение между облачни и традиционни решения	Облачни сървъри	Собствени физически сървъри	Наети физически сървъри	Наети виртуални сървъри
Първоначални инвестиции	Много ниски	Високи	Ниски	Много ниски
Оперативни разходи (вкл. за ел. енергия, климатизация, охрана, поддръжка и др.	Ниски	Високи	Средни	Ниски
Динамични разходи - спрямо потреблението	Да	Не	Не	Не
Възможност за краткосрочно използване	Да	Не	Да	Да
Надеждност на решението	Много висока	Ниска	Средна до висока	Ниска
Еластичност и гъвкавост при нужда и промяна	Много висока	Ниски	Ниски	Средни
Производителност на решението	Висока до много висока	Висока до много висока	Висока до много висока	Ниска до средна
Автоматизация, средства за само-обслужване и отдалечен контрол	Много високи	Ниски или никакви	Средни	Средни
Време за внедряване	Много ниско	Високо до много високо	Средно	Ниско
Време за отстраняване на технически проблеми	0 или много ниско	Много високо	Средно до високо	Средно до високо
Наличие на Single Point Of Failure (SPOF)	Не	Да	Да	Да

1. Предимства и ползи от Облака за постигане целите на държавното управление

С внедряването на Облака се постига оптимизация на разходите за жизнено осигуряващи системи (електро захранване, климатизация, защита и др.), хардуер,

системен софтуер и експлоатационни разходи, повишаване на устойчивостта на системите чрез централизирано управление, запазване принципите за отговорност относно достоверността и своевременност при обработка на съдържанието (данните).

Прилагането на Облака позволява да се постигнат целите на държавното управление в следните направления:

1. Съкращаване на сроковете и подобряване на качеството на вземаните управленчески решения в ежедневно дейност и при кризи от различен характер;
2. Подобряване на оперативната съвместимост и взаимодействието между органите за държавно и местно управление;
3. Подобряване на взаимодействието с външни за организацията контрагенти;
4. Повишаване ефективността в работата и подобряване на взаимодействието между държавната администрация на централно, регионално и местно ниво.
5. Редукция на цената и персонала за осигуряване на електронни информационни услуги
6. Повишаване на надеждността и устойчивостта на техническата платформа.

Ползи от внедряването на Облака:

1. Устойчивост и непрекъснатост на държавното управление чрез унификация на процедурите и осигуряване на висока квалификация на персонала, осигуряващ облачните услуги и изграждане на виртуални хранилища с тестови оперативно съвместими и лицензирани приложения.

2. Значително се улеснява/ускорява процеса на възстановяването на съсредоточени информационните ресурси след срыв (Disaster Recovery), чрез използване на оптимален брой резервни системи и центрове за данни, както и осигуряване на необходимото резервиране/архивиране на информацията.

3. Подобряване на адаптивността спрямо бъдещите нужди и повишаване на възможностите за стандартизиране на приложенията/услугите. Създава се естествена възможност за окрупняване и стандартизиране на заявките за осигуряване на бъдещите нужди на отделните административни структури от информационни ресурси.

4. Подобряване на качеството на услугите (администрация към администрация) поради осигуряването на по-добра свързаност на основните бази данни на отделните административни структури чрез единна електронна съобщителна мрежа (EECM).

5. Предимства при контрола на потребителския достъп и възможност за създаване, поддържане и контрол на унифицирани процедури и точки за достъп на потребителите в облака.

6. Подобрява се контрола на натоварването на ресурсите, с възможност за поддържане на дежурен персонал (поддържан и в момента) и осигуряване на мониторинг на оборудването в режим 24/7.

7. Използват се информационните ресурси според реалната необходимост. Създават се механизъм/механизми за оценка и формално „остойностяване“ на използваните от административните структури облачни услуги.

8. Лесни за използване от потребителите „хранилища“ за стандартизирано/оперативно съвместими приложения, изградени на принципа на Microsoft или

Google Store, в рамките на частния облак и достъпни само от оторизирани потребители.

9. Улесняват се механизмите за бързо внедряване на нови технологични решения, на базата на съсредоточаване на информационните ресурси и премахване на административно-бюрократичните пречки.

10. Намалени разходи за издръжка на управлението поради:

- Намаляване на общия брой на физическите сървъри и системи за съхранение на данни (сторидж) и на броя на обслужващия/поддържащия персонал. **Намалява се броя и съответно разходите за персонал, необходим за поддръжката и развитието на ИКТ от 2 до 4 пъти;**

- Намаляване на общия брой инженерно-технически системи (ел. захранване, гарантирано ел. захранване, климатизация, водоснабдяване, пожарогасене, видеонаблюдение и физическа сигурност) ,на броя на обслужващия/поддържащия персонал и на консумираната ел. енергия и вода. **Постига се намаляване на разходите за електроенергия за технологични и спомагателни нужди между 4 и 6 пъти** за сметка на съкращаване на броя на физическите устройства (сървъри и сторидж), активните комуникационни устройства , осигуряващи свързаността, както и броя и мощността на използваната климатична техника и UPS;

- Намаляване на броя на договорите за поддръжка и осигуряване на допълнителна свързаност (Интернет).

11. Икономия на финансови ресурси се реализират и чрез максимализиране на ползите от вече изградената/изграждаща се инфраструктура.

12. Намаляват се и разходите за свързаност, чрез окрупняване на договорите за доставка на Интернет от външни доставчици и наемане, където е възможно капацитет от Телеком операторите за осигуряване на свързаност на отдалечени териториални администрации.

13. Намаляват се разходите за сървърни и антивирусни лицензи.

14. Гарантират се за всички административни структури безплатни и сигурни базови информационни услуги – e-mail, гласови услуги между администрациите базирани на VoIP (съответно намаляване на разходите за тях поне на 50%), WEB и др.

15. Опростява се модела на определяне/планиране на разходите, тъй като административните структури ще насочат вниманието си основно към планиране на средства за придобиване и поддръжка на крайни устройства и специфични софтуерни приложения. Средствата за придобиване и поддръжка на сървъри, сторидж, осигуряване на свързаност и облачен софтуер ще се планират централизирано.

16. Подобряват се екологичните показатели и защита на околната среда поради намаляване на потреблението на ел. енергия (от там –индиректно-на количеството вредни емисии от въглероден диоксид в атмосферата).

17. Увеличена прозрачност и граждански контрол на процесите в държавата.

18. Подобро взаимодействие със структури на ЕС и НАТО.

19. Подобро взаимодействие на структурите на държавното и местно управление

20. Подобро взаимодействие на администрациите с бизнеса.

21. Създаване на условия за задоволяване на потребностите от информационни услуги на все повече държавни органи и администрации.

Проблеми при облачните технологии

Доскоро cloud технологиите се определяха като не напълно надеждни и сигурни. Всеобщото мнение бе, че е много по-добре информацията да се съхранява в собствен център за данни, отколкото да се разчита на шумелите нови технологии.

Колкото повече нови неща се появяват в света на cloud сигурността, толкова по-често се оказва, че доскорошното схващане е погрешно. Разбира се, има не дотам сигурни облачни среди, но същото може да се каже и за технологиите, използвани и до този момент за съхраняване на данни.

Има четири ключови аспекта, над които всеки, който е решил да ползва облачни базирани услуги, трябва да намери отговор:

1. Как ще бъде криптирана информацията, запазена в облака?
2. По какъв начин ще се осъществява достъпът?
3. Колко от облачната инфраструктура е излишна?
4. Как са защитени уеб приложенията?

Повечето създатели на облачни технологии автоматично използват SSL връзка за всеки Web проект, но това осигурява сигурност само между уеб приложението и клиента. Тук най-доброто решение е създаването на хибриден частен облак, така че всеки базиран на облачна технология ресурс да стои зад корпоративна защита и най-сензитивната информация ще остане физически при клиента. Повечето облачни доставчици предлагат частна мрежа, Virtual Private Network, до своята облачна инфраструктура и така осигуряват криптирана връзка между услугата и офиса. Други доставчици пък предлагат отделни VPN услуги, базирани на някакъв софтуер за създаване на криптирана връзка до доставчика.

Ключов момент за запазване на по-голяма сигурност е създаването на по-малки облаци, които да са по-близо до доставчика. Използва се VPN за връзка с облачната мрежа, но съществуват няколко различни групи, които работят с различни сървъри.

Вече се предлага автоматична защита на данните чрез използване на криптирани файлови системи и бекъп в реално време до отдалечена точка, която гарантира максимална сигурност на данните, дори и при кражба или взлом в системата на клиента. Някои доставчици разполагат с няколко точки на присъствие и клиентът избира в коя да разположи част от оборудването си, за да създаде географско независима инфраструктура, т.е. дори и една от точките да бъде недостъпна, услугите да продължат да работят.

Може би най-големият проблем на защитата на облачните технологии се състои в самите уеб приложения и в това как те са свързани с останалата информация. Предизвикателството е да се виртуализират колкото се може повече защитни устройства или приложения като firewall-ите например. Най-големите доставчици на облачни услуги вече добавят тези опции към своя списък, така че IT специалистите да пренасят информацията си в облаци и в същото време да запазват нивото на сигурност.

Също така се предоставя вградена защитна стена към всеки облачен сървър, който работи отделно от сървъра и не зависи от операционната система. По този начин потребителите могат да създават сигурни инфраструктури, до които достъп имат само определени адреси. Като допълнение към това самата среда осигурява

пълно изолиране на един сървър от друг с цел предпазване на трафика на клиентите.

Облачните технологии бавно, но сигурно достигат едно високо ниво на защита. В бъдеще сигурността ще бъде още по-голяма, а и именно такива са тенденциите в развитието на съвременните технологии и интернет услуги. **Но едно е сигурно – в момента облачните услуги предоставят същото ниво на сигурност и същата възможност за управление на нивото на достъп, както и традиционните инфраструктури**, с тенденция в бъдеще все по-нови, по-сигурни и по-гъвкави услуги за сигурност да бъдат внедрени.

III. Визия за въвеждане на облачните технологии в държавното управление

Визията описва вижданията и схващанията за развитието на комуникационните и информационни ресурси чрез въвеждане на облачни технологии, съобразени с добрите практики за електронно управление, съвременните тенденции за развитие на информационното общество и предоставянето на електронни услуги на гражданите на Р. България. Тя показва начините за постигане на ново технологично ниво на комуникационно информационно осигуряване, което би позволило уеднаквяване на управленческите процеси в мирно и военно и по време на кризи, разширяване възможностите за съвместно използване на мрежата и съпътстващата я инфраструктура от всички държавни органи и институции и създаване на условия за ефективно използване на направените инвестиции с отбранително предназначение.

Тя предвижда внедряване на нови технологии за постигане оптимизация на разходите за жизнено осигуряващи системи (електро захранване, климатизация, защита и др.), хардуер, системен софтуер и експлоатационни разходи, повишаване на устойчивостта на системите чрез централизирано управление, запазване принципите за отговорност относно достоверността и своєвременност при обработка на съдържанието (данните).

1. Единна мрежова среда. Развитие на комуникационната мрежа за подобряване на свързаността

Държавната комуникационна мрежа, изградена и поддържана от ИА ЕСМИС, осигурява свързаност на администрациите на законодателната, изпълнителната и съдебната власт. Към настоящия момент ИА ЕСМИС управлява, съхранява, поддържа и експлоатира 24/7/365 дни в годината повече от 6 300 км. оптични кабелни линии, близо 700 опорни възли и възли за достъп в различни сгради на територията на цялата страна, свързваща над 1200 различни структури и подразделения от държавната и местна администрация. С този ресурси мрежата осигурява цялостна организационна свързаност на 20% от администрацията и техните териториални подразделения, за останалите свързаността е частична.

Развитието на комуникационната инфраструктура ще се осъществява в три основни направления:

Първо - осигуряване на необходимата комуникационна свързаност между централите за данни;

Второ - осигуряване на необходимата комуникационна свързаност на ведомствата (потребители) до централите за данни;

Трето - осигуряване на достъп до центровете за данни по защитени канали (VPN) през Интернет за потребителите извън обхвата на ЕЕСМ и не разполагащи със собствена мрежа.

2. Изграждане на центрове за данни в обектите от ЕЕСМ

Броят на центровете ще се определи в зависимост от тяхната локация, комуникационна свързаност към ЕЕСМ, нивото на оборудване, както и от общия капацитет на услугите, които ще се предоставят. Като минимум се определят три центровете за данни - два напълно взаимно заменяеми и един резервен.

Инфраструктурата на всеки център за данни в неговата цялост ще се състои от две основни групи компоненти: компоненти на физическата инфраструктура и IT компоненти.

Първата група компоненти включва: сградния фонд, резервирано електрозахранване, климатизация, инфраструктурно окабеляване, апаратни шкафове, пожароизвестяване, пожарогасене, наблюдение, контрол на достъпа и др.

Втората група компоненти се формират от изградения процесорен ресурс, дисково пространство, компютърни мрежи, компонентите за информационна сигурност, средства за виртуализация и средствата за автоматизиране на процесите.

В центровете за данни ще се предоставят следните възможни сценарии за разполагане и използване на оборудване:

1. Предоставяне на условия за **колокация в отделни зали** с ограничен достъп с осигуряване на наблюдение и поддръжка от собственика на оборудването.

Този сценарий е предвиден за случаите изискващи ограничен физически и логически достъп до изчислителните ресурси. Сценарий на логическо разделяне предвижда в зони за всяко от ведомствата да се формират допълнителни логически разделени мрежови сегменти, в които да се разполага колокирано оборудване на отделните потребители (ведомства).

Управлението на инженерните съоръжения, осигуряващи функционирането на оборудването, както и конфигурирането на политики за физически достъп ще е част от общата система за управление на центъра за данни.

Управлението на техническите и програмните средства в логическите сегменти ще се извършва чрез системи и техники по решение на отделните ведомства - независими от общата система на управление на центъра за данни. По решение на ведомството – собственик могат да бъдат прилагани и допълнителни механизми за сигурност и защита на достъпа.

2. Предоставяне на условия за **колокация на оборудване в общи зали в центровете за данни** с осигурено непрекъснато наблюдение и техническо обслужване.

Този сценарий предвижда логическо разделяне с групиране на споделените услуги. Същевременно отделните потребители (ведомства) ще могат да разполагат с логически разделени мрежови сегменти на собственото оборудване. Управлението на техническите и програмните средства в „демититаризирани зони“ ще е част от общата система на управление на центъра за данни.

3. Използване на виртуална среда, предоставяна от изградената инфраструктура в центровете за данни.

Сценарият предвижда съчетаване възможностите на колокираното оборудване с облачни услуги – Инфраструктура като услуга (IaaS) и – Платформа като услуга

(PaaS). Това ще позволи на потребителите (ведомствата) в средносрочен и дългосрочен план без допълнителни инвестиции да увеличават изчислителния ресурс на собствените си ИТ инфраструктури, както и бързо да покриват недостиг на такъв за определен времеви прозорец.

Дейностите по изграждането и оборудването на центровете за данни ще се извършва на етапи и фази посредством изпълнение на съответните проекти при спазване на изискванията на действащите регламенти и стандарти.

3. Облачни услуги

Миграцията към услуги в облака ще се извършва едновременно с неговото развитие и добавяне на нови възможности. В началния етап ще се очаква потребителите да направят преглед на текущото състояние на ИТ инфраструктурите си. В резултат на прегледа ще стартира плавно мигриране на част от компонентите в облачната среда (physical to virtual – P2V), като се започне от тези с най-ниски натовареност и изисквания за непрекъсваемост. На втори и следващ етап процесът ще продължи с мигриране на по-сложни компоненти и системи като се избягват действия от типа „виртуализация на всяка цена“. При проектиране и въвеждане в експлоатация на нови компоненти и системи, както и при подобряване на същите ще се анализира първо възможността за използване на облачни услуги.

Самите услуги ще се развиват и ще са налични за потребители по етапно и в най-общия случай ще са разделени в три фази: **Инфраструктура като услуга** (Infrastructure As a Service-IaaS), **Платформа като услуга** (Platform As a Service-PaaS) и **Софтуер като услуга** (Software As a Services – SaaS).

1.Предоставяне на инфраструктура като услуга (IaaS)

Услугата ще бъде налична на първата фаза след изграждането на два центъра за данни съпроводен с план за нарастване на обема на услуги в зависимост от броя на потребителите (присъединени администрации) и елементи от центъра за наблюдение и управление.

2.Предоставяне на платформа като услуга (PaaS)

Услугата ще бъде налична частично на първата фаза и в пълния и обхват на втора фаза. На тази фаза се предлага изграждането на центъра за данни необходим в случай на бедствие/криза. Осигуряването на PaaS ще се осъществява чрез предоставяне на компютърни платформи или пакетно решение във вид на услуга.

3.Предоставяне на приложения (софтуер) като услуга (SaaS)

Услугата ще започне да се предоставя през трета фаза съпроводена с пълно изграждане на трите центрове за данни (с изискуем изчислителен ресурс), както и напълно развърнат центъра за наблюдение и управление, с възможности за наемане и управление на облачни услуги от външни доставчици, както и управление и доставки на лицензи и лицензионни права.

4. Управление и осигуряване на достъпа

Управлението и наблюдението на облачната инфраструктура позволяват да се гарантира нейната оптимална производителност. Това изисква използването на съответния софтуерен инструментариум, чрез който ще се осъществява управление и контрол на дефинираните системи, приложения и мрежи. Този инструментариум ще даде възможност не само за да се гарантира производителността, но също така

и по-добре да се извършва динамично управление (оркестрация) и автоматизиране на процесите по конфигуриране и доставка на ресурсите.

От друга страна използваните инструменти за управление и наблюдение ще дават възможност за проследяване на изпълнението на отделните процеси, както и мониторинг на състоянието на всички компоненти, които поддържат предоставянето на услуги: хардуер, софтуер, мрежовата инфраструктура и др.

За осигуряване на достъп на потребителите до облачните услуги, както и за администрирането на самата среда на частния облак ще се създадат необходимите портали като част от системата за наблюдение и управление:

Портал за администриране, който чрез технически, системни и други инструменти, в зависимост от технологичното решение, ще управлява самата инфраструктура;

Потребителски портал, чрез който потребителите ще заявяват, конфигурират и използват облачните услуги. Последното от една страна ще позволява те да са непосредствени участници в процеса, а от друга ще осигурява висока степен на автоматизирането му.

5. Стандартни базови услуги за общ достъп и пакети от информационни услуги

Този вид услуги ще бъдат достъпни веднага след изграждането на поне един център за данни.

Предвижда се на крайните потребители в зависимост от използваната комуникационна свързаност и независимо от използваните хардуерни, системни или потребителски платформи да се предоставят достъп до следните пакети услуги:

1. WEB достъп до публични или локални ресурси;
2. Публикуване и управление на информация в публично или локално пространство;
3. Електронна поща (e-mail) и обмен на кратки съобщения в реално време;
4. Предоставяне на пространство за съхранение на файлове (file servers);
5. Директорийни услуги и политики за сигурност в активна директория;
6. Достъп до система за групов работен процес или до специфични (специализирани) информационни системи.
7. Гласова услуга - В зависимост от конкретните потребности ще е предвидена възможност за предоставяне на гласова услуга (Voice over IP – VoIP). Технологичното решение ще е скалируемо. Услугата ще може да се интегрира със съществуващи мрежи за пренос на глас и ще се предоставя както в частни затворени среди така и при свързването и към публични мрежи.

6. Система за сигурност на информацията и услугите

Системата за сигурността на информацията ще гарантира опазване на поверителността, точността, целостта, достъпността, използваемостта, автентичността и надеждността на информацията, създавана, пренасяна и съхранявана в облака, чрез прилагане на:

- технически средства за физическа защита;
- съвременни технологични решения в областта на информационната и комуникационна техника;

- управляема рамка на организационни мерки като политики, процедури, указания, инструкции и свързаните с тях ресурси, на базата на добрите практики в информационните и комуникационни технологии, за постигане на нивото на услугите, регламентирано в споразуменията (Service Level Agreement-SLA) и в съответствие с изискванията на законовите и нормативни документи, стандартите и директиви.

7. Взаимодействие на държавния облак със съществуващите ведомствени облаци на държавни организации

Създаваният държавен облак осигурява базови услуги за държавните ведомства които поради спецификата на информацията изграждат или поддържат собствени частни облаци. Чрез ресурсите на съвместната информационна среда информационните ресурси се обединяват и се осигурява достъп за обмен на услуги с другите администрации, бизнеса и гражданите.

Обединяването на ресурсите на държавния облак и ведомствените облаци на големите държавни организации позволява да се реагира на ситуации свързани със защита на националната сигурност както и да се обслужват клиенти, които използват много и различни услуги, както и потребители или наематели с временни или мащабируеми услуги. Тези услуги могат да бъдат настроени да посрещнат нуждите на всеки клиент.

8. Съблюдаване на изискванията за защита на класифицираната информация

Защитата на класифицираната информация от нерегламентиран достъп при нейното създаване, обработка, съхраняване и пренасяне се осигурява от система криптографски методи и средства.

На базата на изградената от ЕЕСМ комуникационна свързаност, спазвайки изискванията на Закона за защита на класифицираната информация (ЗЗКИ) и съответните регламентиращи документи, могат да се изградят ведомствени криптографски мрежи.

В част от центровете за данни могат да се обособят защитени зони, за обработка и съхранение на класифицирана информация. Използването на единна комуникационна инфраструктура от различни ведомства налага сегментиране на класифицираните мрежи. При форсмажорни ситуации, кризи от военен характер или други обстоятелства, изискващи обмен на класифицирана информация може да осигури незабавна свързаност между различните ведомства.

9. Приложение на „зелени“ технологии

Реализацията на проектите за внедряване на облачните информационни технологии имат пряко и косвено отражение за приложението на енергоспестяващи решения и опазването на природната среда. Преките въздействия ще се постигнат с отпадане на необходимостта за строителство на нови обекти и съоръжения, гарантирано електрозахранване, системи за охрана и други. Косвените ползи са свързани с намаляване на консумираната електроенергия, поради намаляване на броя на центровете за данни, колокация на същите в обектите на агенцията. Предварителните разчети показват че разходите за електроенергия от сегашните ще намалят два пъти.

Целева архитектура

1. АРХИТЕКТУРА НА ОБЛАЧНАТА СИСТЕМА

Общата архитектура на облачната система се явява по същество обобщен концептуален модел от високо ниво и служи като ефективен инструмент при формиране изискванията, структурата и функционирането ѝ. В архитектурата са определени: състава на участниците, дейността и функциите им и взаимоотношенията между участниците в тези системи

Изхождайки от свойствата на общият вид на модела архитектурата на облачната система ще има пет главни действащи структури:

- потребители на облачни услуги;
- доставчик на облачни услуги за държавното управление;
- одитор на облачни услуги;
- посредник (брокер) на облачни услуги;
- доставчици на външни услуги.

1. Потребители на облачни услуги

Това са органите за управление на министерства, ведомства, на местната власт и техните администрации, които ще използват услугите, предоставяни от облачни доставчик.

2. Доставчик на облачни услуги

Структура, отговаряща за достъпността на облачната услуга за потребители.

Доставчикът на облачни услуги изпълнява задачи в различните модели за предоставяне на услуги чрез:

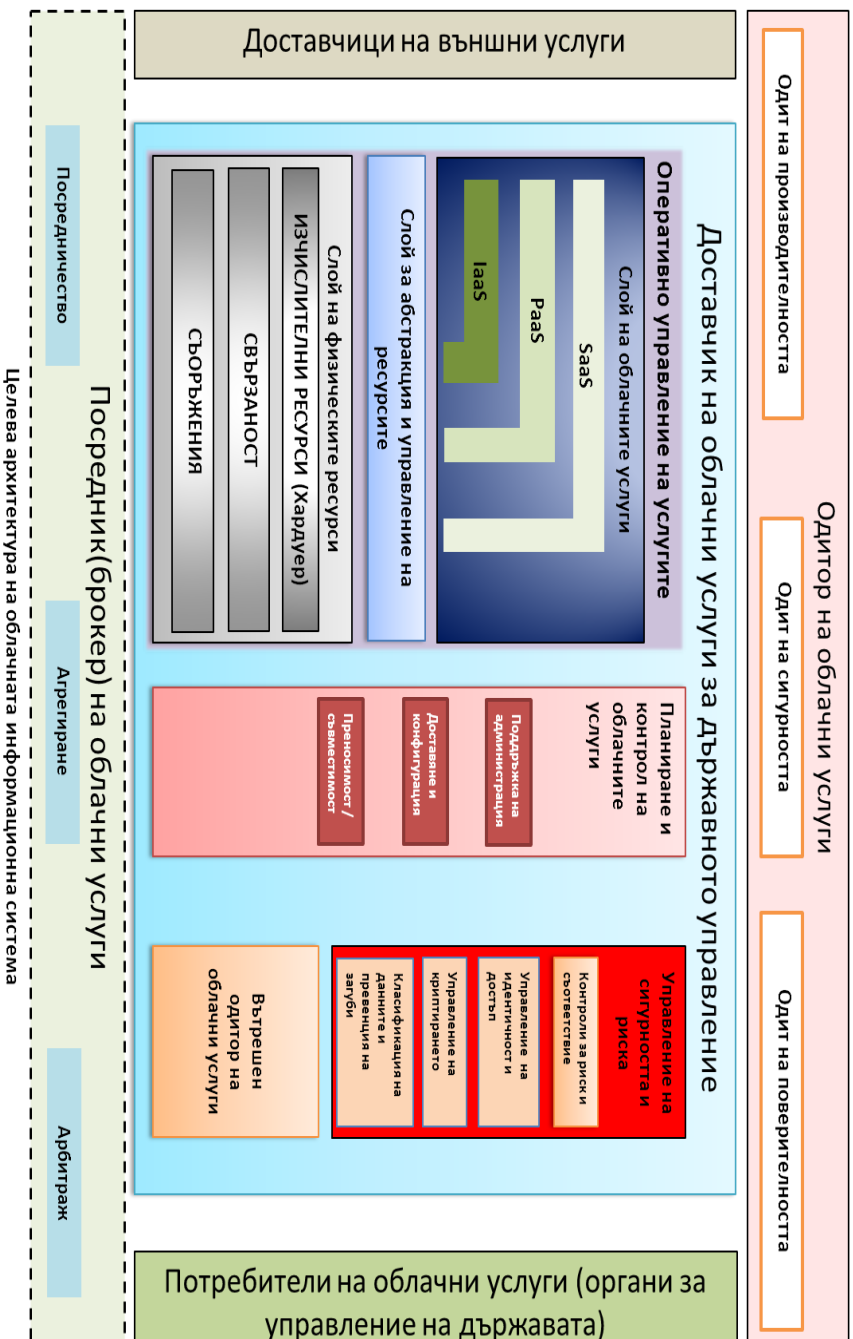
- **Оперативно управление на услугите на три слоя:**

Слой на облачните услуги - определя базовите услуги, предоставяни от доставчика:

- SaaS - Установява, управлява, съпровожда и поддържа програмно осигуряване, разгънато в облачната инфраструктура;
- PaaS - Предоставя и управлява облачна инфраструктура и свързващо програмно осигуряване за платформата за потребителите; предоставя инструменти за разработка, разгръщане и администриране на потребителските платформи;
- IaaS - Предоставя и управлява физически изчислителни мощности, системи за съхранение, мрежи и хостинг - обкръжение, както и облачна инфраструктура за IaaS-потребители.

Слой абстракции и управление на ресурсите -Предоставя елементи на програмно осигуряване, такива като хипервайзор, виртуални хранилища на данни и поддържащи програмни компоненти, използвани за реализация на облачна инфраструктура, върху която може да се установят облачните услуги. Широко ще се използват технологиите на виртуалните машини;

Слой на физическите ресурси - включва всички физически ресурси - изчислителните ресурси (хардуер), инженерните съоръжения и комуникационната свързаност, която предоставя на облачните потребители достъп до облачни услуги чрез мрежови, телекомуникационни и други средства за достъп. Такава роля в настоящият момент играе ЕЕСМ, изградена и поддържана от ИА ЕСМИС и различни арендовани връзки от телекомуникационните оператори.



- **Планиране и управление на облачните услуги** - включва всички свързани с услугите функции, необходими за управление и функциониране на същите, предлагани на облачните потребители като - поддръжка на дейностите на администрацията, доставяне и конфигуриране и преносимост/оперативна съвместимост.

- **Управление на сигурността и риска** – идентифициране и оценка на заплахите и уязвимостите относно всеки компонент, участващ в реализирането на облачните услуги и прилагане на подходящи механизми за защита с цел смекчаване на въздействието.

Освен това на облачния доставчик се възлага:

- Организацията по разгръщане на облачните услуги чрез изграждането на държавен облак, осигуряващ базови услуги за държавните ведомства, а чрез ресурсите на съвместната информационна среда се осигури достъп на частните ведомствени облаци за обмен на услуги с другите администрации, бизнеса и гражданите.

- **Вътрешен одитор на облачни услуги.** Вътрешна структура на доставчика на услуги, който ще извършва текущият контрол и оценка на обслужването на информационните системи, производителността и сигурността на облака.

1. Одитор на облачни услуги

Организация (орган), извършващ проверки в съответствие със стандарт БДС EN ISO19011:2011.

В процеса на проверка се извършва преглед за релевантност на реалното състояние със заложените изисквания за сигурност, функционалност, качество и други.

Одиторът на облачните услуги може да дава оценка на услугите, представяни от облачния провайдер, в термини на контрола на сигурността (*security control*), съблюдаване на поверителност (*privacy impact*), производителност (*performance*), и т.н.

Тази задачи може да се изпълняват от оторизираните и сертифицирани за това държавни организации.

2. Посредник (брокер) на облачни услуги

Функциите на Посредника на облачни услуги са свързани с използването, производителността и предоставянето на облачни услуги, както и установяваща отношения между външните доставчици на облачни услуги и потребители на облачни услуги.

Основните услуги, предоставяни от посредника на облачни услуги включват:

- сервизно посредничество;
- агрегиране на услугите;
- арбитраж на услугите.

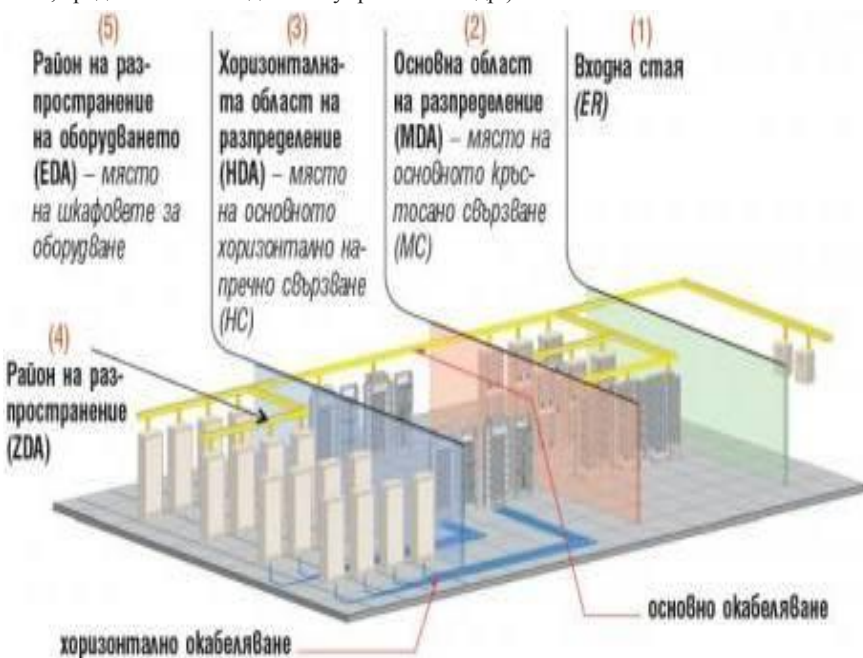
Функциите на посредника на облачни услуги могат (препоръчително е) да се изпълняват от ИА ЕСМИС с цел наемане на капацитет и услуги за резервиране или предоставяне на такива, които в определените етапи за изграждане не са достъпни от собствената инфраструктура, а се изискват за определени цели на електронното управление. Определянето и изпълнението на тази функция от ИА ЕСМИС ще позволи преодоляването на част от проблемите които могат да възникнат във връзка с оперативната съвместимост и мрежова и информационна сигурност.

3. Доставчици на външни услуги

Това са всички тези облачни, комуникации и специализирани услуги и лизинг на поддръжката на хардуер и софтуер за поддържане на съвместната информационна среда, които доставчика на услуги не може или е не ефективно да предостави на потребителите. В този случай доставката на услугите се осигурява чрез Облачния брокер по единни правила и процедури за качество на услуга и сигурност от различни доставчици.

2. АРХИТЕКТУРА НА ЦЕНТРОВЕТЕ ЗА ДАННИ

Архитектурата на центровете за данни в основната си част включва няколко зони (пространства) в които се разполага основното оборудване (сървъри и комуникационни шкафове, дискови масиви за съхранение на данни и др.), спомагателното оборудване (елементи на структурното окабеляване, технически устройства и др.) и допълнително оборудване (токозахранващи устройства и батерии (UPS), климатично оборудване и вентилация, пожарогасително оборудване, електроагрегати, средства за наблюдение и управление и др.).



Центърът за данни трябва да осигурява следните 3 важни условия:

- непрекъсваемост на информационните ресурси и достъпа до тях;
- висока консолидация, скалируемост и гъвкавост, базирани на прилагане на облачни технологии и виртуализация;
- надеждна защита и съхранение на информацията.

Измерители за резултатност при въвеждане на Облака за държавно управление

Реализирането на ползите от въвеждането на облачните технологии в държавното управление се постига с въвеждането на следните измерители за резултатност:

1. Процентът на покритие на органите за държавното управление с облачни услуги от 0% през 2014 г. да достигне на 100% през 2020 г.

2. Процентът на покритие на органите на местното управление с облачни услуги след завършване на третия етап на стратегията от 0% през 2014г. да достигне 50% през 2020 г.. Развитието на мрежата за свързаност и широколентов достъп, реализирани в изпълнение на стратегията за 50% от посочените органи ще им позволи ползването на услуги от облачната среда на другите държавни органи или наемане на облачни услуги от външни доставчици.

3. Процент на натовареност на информационните ресурси по категории (процесори, устройства за съхранение, комуникационни канали и др.) - на сървърите повече от 70%(при сегашно ниво под 30%), на комуникационните канали над 90% (при сегашно ниво до 20%).

4. Процент на осигуреност на базови пакети от услуги на 100 %.

5. Осигуреност с допълнителни услуги на 20 %.

6. Средно време за осигуряване на услуги/ пакет от услуги не повече от 1 секунда.

7. Надеждност на услугите (средно време между отказите)- 99,995%.

8. Средното време за възстановяване на услугите да не надхвърля 10 минути.

9. Удовлетвореност на потребителите, измерването на която ще се извършва чрез използването на концептуален модел. В модела се включат базови елементи на облачните информационни технологии като: сигурност, ефикасност, адаптивност, цена и др. Освен тях ще се отчитат елементи като: конфиденциалност, наличност и рестрикции за използване, резервиране и възстановяване, време за реакция, използваемост, ориентация към клиента, гъвкавост, оперативна съвместимост, мащабируемо съхранение, цена на хардуер, цена на софтуер и др.

IV. Ключови проекти

За реализацията на стратегията за изграждане на облачна инфраструктура на държавната администрация се предвиждат реализация на 6 (шест) проекта.

ПРОЕКТ 1:Облачни услуги и обучение

ПРОЕКТ 2:Изграждане на центрове за данни и центрове за наблюдение и управление на ЕСИС.

ПРОЕКТ 3:Развитие на комуникационната мрежа за подобряване на свързаността и обучение.

ПРОЕКТ 4:Управление на облачните услуги и обучение.

ПРОЕКТ 5:Система за сигурност на информацията и услугите.

ПРОЕКТ 6:Поддръжка на облачната среда в жизнения цикъл.

ДОБРИ ПРАКТИКИ И СТАНДАРТИ ЗА ФИЗИЧЕСКА СИГУРНОСТ ПРИ РАБОТА В ОБЛАКА

Орхан А. Исмаилов

*Министерство на отбраната на Р. България,
София, 1000, ул. „Дякон Игнатий” № 3*

BEST PRACTICES AND STANDARDS FOR CLOUD PHYSICAL SECURITY

Orhan A. Ismailov

ABSTRACT: *The paper presents some of the major issues related to new information technology and physical security of IT resources. Basic definitions are based on NIST SP 800-145 of September 2011. Global trends and standards for physical security are considered.*

KEY WORDS: *Privacy, Data protection, Physical security, Security, Security risks, Work in the cloud, The right to be forgotte.*

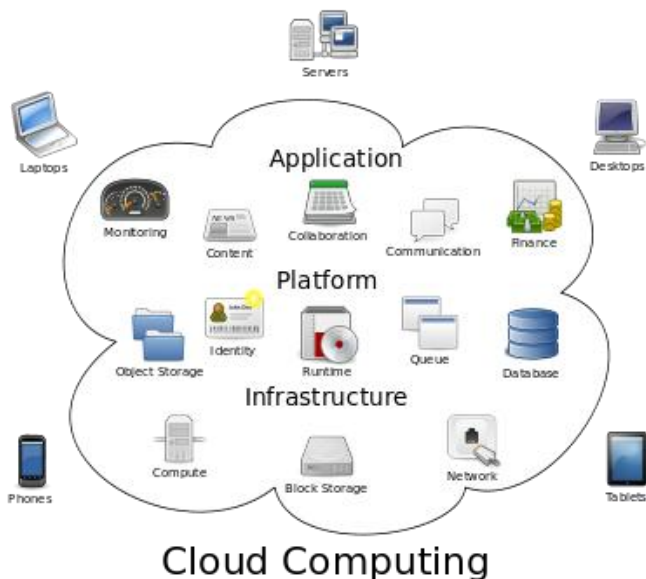
1. ВЪВЕДЕНИЕ

Развитието на новите комуникационни и информационни технологии и по-конкретно Интернет и работата в облака, поставят нови предизвикателства пред комуникациите между хората и институциите и защитата на информацията. Новите предизвикателства за защита на информацията са свързани с правилното разбиране и интерпретиране на новите понятия, на първо място Работа в Облака (Cloud computing) и в частност на физическата сигурност, като основен компонент на системата за информационна сигурност.

Работа в облака (cloud computing)

Какво е работа в облака

Работата в облака е използването на компютърни (изчислителни) ресурси (хардуер и софтуер), които се предоставят като услуга (най-често абонаментна) по мрежата (обикновено Интернет). Името му идва от използването на символ с формата на облак като абстракция на комплексната инфраструктурата, която се съдържа в системните диаграми. Работата в облака осигурява отдалечени услуги с потребителски данни, софтуер и подходящата им обработка. Работа в облака е авторски превод на Cloud computing, който много често се среща като Облачни изчисления (включително и в официални документи на Европейския съюз). Определено може да се каже, че Работа в облака е смисленият и по точен превод на Cloud computing, отразяващ същността на технологиите и възможностите на Облака (Интернет технологията).



Фиг. 1. Работа и услуги в облака

Характеристики на облака

Характеристиките на работа в облака са:

- Самообслужване по желание (On-demand self-service);
- Широк достъп до мрежата (Broad network access);
- Групиране на ресурсите (Resource pooling);
- Бърза мащабируемост (Rapid elasticity);
- Измерване на услугата (Measured service).

Самообслужване по желание

В такъв случай потребителят може да прекрати едностранно възможности за използване на компютърни ресурси, като сървърно време и мрежово съхранение, когато е необходимо автоматично, без да се изисква взаимодействието с доставчика на услуги.

Широк достъп до мрежата

Възможностите на мрежата са достъпни чрез стандартни механизми, които позволяват използването от разнородни платформи за „тънък или дебел клиент“ (thin or thick client platforms) (например, мобилни телефони, таблети, лаптопи и работни станции).

Групиране на ресурсите

Доставчиците на компютърни ресурси се обединяват, за да осигурят услугите на множество потребители, като използват един мулти-наемател модел (a multi-tenant model), с динамично назначени и преназначени различни физически и вирту-

ални ресурси, в съответствие с потребителското търсене. Поражда се чувството за независимост поради това, че клиентът обикновено няма контрол или познания върху точното местоположение на предоставените ресурси, но може да бъде в състояние да определи местоположението на по-високо ниво на абстракция (например, област, държавата, или центровете за данни). Примери за ресурси включват съхранение, обработка, памет и скорост на мрежата.

Бърза мащабируемост

Ресурсите могат да бъдат бързо резервирани и освободени, навън и навътре, в повечето случаи автоматично, за да са съизмерими с търсенето. На потребителя, възможностите за осигуряване на ресурси често изглеждат неограничени и могат да бъдат използвани в каквото и да е количество по всяко време.

Измерване на услугата

Системите за работа в облака автоматично контролират и оптимизират използването на ресурсите чрез повишаване на капацитета за измерване на някакво ниво на абстракция, подходящо за вида услуга (например, съхраняване, обработка, честотна лента, и активни потребителски сметки). Използването на ресурсите може да се наблюдава, контролира и съобщава, и това осигурява прозрачност, както за доставчика и така и за потребителите на използваната услуга.

Услуги в облака

Основните услуги за работа в облака са:

- Инфраструктура като услуга ([Infrastructure as a service](#), IaaS);
- Платформа като услуга ([Platform as a service](#), PaaS);
- Софтуер като услуга ([Software as a service](#), SaaS);

2. ФИЗИЧЕСКА СИГУРНОСТ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ, БАЗИРАНИ НА ОБЛАЧНИТЕ ТЕХНОЛОГИИ

2.1. Цели

Основни цели на физическата сигурност са:

- Предотвратяването на неоторизиран достъп, повредите и физическите увреждания на помещенията и информацията на Организацията;
- Предотвратяването на загуба, повреждане или компрометиране на активите или прекъсване на дейностите на Организацията;
- Предотвратяването на компрометиране или кражба на информация и устройствата за информационните процеси.

2.2. Дейности

Осигуряването на физическата сигурност обхваща следните дейности:

- Защита;
- Откриване;
- Реакция;
- Възстановяване.

Защитата се постига чрез използването на физически, процедурни и психологически баристри, за да забави или да предотврати неоторизиран достъп.

Откриването включва използването на подходящи устройства, системи и процедури, за да сигнализира, че се е появил опит за или при действителен неотORIZИ-ран достъп.

В контекста на физическата сигурност *реакцията* води до прилагането на мерки, за да гарантират, че инцидентите, свързани със сигурността, се докладват на съответните длъжностни лица за сигурност и непосредствена и дългосрочна коригиращи действия, предприети своевременно. *Възстановяването* се отнася до възстановяването на всички нива на предоставяне на услуги след инцидента.

3. ДОБРИ ПРАКТИКИ за одит на физическата сигурност

3.1. Стандарти BS 7799 и ISO 17799:2000

Въпросите, свързани с одита на сигурността на информационните системи, базирани на BS 7799, са разделени в десет основни направления, както едно от най-важните направления за осигуряване на физическата сигурност.

Въпросите са групирани както следва:

- Охранявана зона (зони за сигурност);
- Сигурност на оборудването;
- Общ контрол.

Стандартът ISO 17799:2000 е развитие на BS 7799 и съдържа препоръки за управление на информационната сигурност на една Организация. Той обхваща различни аспекти на сигурността като:

- Планиране на кризисни ситуации;
- Физическа сигурност;
- Въпроси на сигурността, свързани с персонала;
- Контрол на достъпа до информационните системи;
- Сигурност при разработка и поддръжка на информационни системи.

Въпросник за одит на сигурността на информационните системи базиран на BS 7799

Включени са областите и въпросите както следва:

Охранявана зона (зони за сигурност)

1. Има ли физическа сигурност на периметъра ?
2. Съществува ли контрол на физическия достъп ?
3. Има ли защита на офиси, стаи и съоръжения ?
4. Извършва ли се работа в защитени зони ?
5. Съществува ли изолиране на зоните за доставки и областите за зареждане?

Сигурност на оборудването

6. Има ли точно определено място за разполагане на оборудването ?
7. Защитени ли са захранващите системи (UPS, генератори и др.)?
8. Съществува ли процедура за сигурност на кабелните системи ?
9. Поддръжката извършва ли се по определена процедура ?
10. Съществува ли процедура за защита на оборудването извън периметъра ?
11. Дефинирани ли са мерки за спазване на сигурността при повторно използване на оборудване ?

Общ контрол

12. Изградена ли е политика за “чисто бюро и чист екран” ?
13. Възможно ли е да се приема отвън оборудване, информация или софтуер без съответното разрешение ?

3.2. Стандарт ISO/IEC 27002:2005

Въпросите свързани с физическа сигурност и сигурност на околната среда в ISO/IEC 27002, обхващат:

- Области за сигурност
 - Физическа сигурност на периметъра
 - Физическа контроли на входните точки
 - Сигурност на офиси, стаи и съоръжения
 - Защита срещу външни заплахи и срещу заплахи от средата
 - Работа в областите за сигурност
 - Обществен достъп, доставка и товарни зони
- Сигурност на оборудването
 - Разполагане на оборудването и защита
 - Допълнителни средства (услуги)
 - Защитено окабеляване
 - Поддръжка на оборудването
 - Защита на оборудването извън зоната (обекта)
 - Сигурност на унищожаването или на повторното използване на оборудването
 - Премахване на собствеността

3.3. Стандарт ISO/IEC 27002:2013

Втората версия на стандарта ISO/IEC 27002:2013 („Information technology — Security techniques — Code of practice for information security management“) е от октомври 2013 г. и е развитие и конкретизация на стандарта ISO/IEC 27002:2005. Обхванати са въпросите за:

- Области за сигурност;
- Оборудване.

3.4. Методология за оценка на информационната сигурност на Националната агенция за сигурност на САЩ

В областта на физическата сигурност основно внимание се обръща на:

- Дефиниране на:
 - Периметър;
 - Сгради;
 - Зони за сигурност;
 - Помещения с ограничен и контролиран достъп;
 - Входни и изходни точки:
 - Ежедневни;
 - Аварийни;
- Контрол на достъпа:
 - В периметъра;
 - В сградите;

- В зоните за сигурност;
 - В помещенията с ограничен и контролиран достъп;
- Сървъри и мрежово оборудване:
 - Защитени помещения;
 - Зона за сигурност;
 - Ограничен и контролиран достъп;
 - Климатично и противопожарно осигуряване
- Работни станции;
- Видео наблюдение;
- Охрана и сили за реакция;
- Посетители:
 - Режим за посетители;
 - Заявки и разрешения;
 - Цел;
 - Време;
 - Място;
 - Отговорник;
 - Придружител;
- Дневник;
 - На заявките;
 - На разрешенията;
 - На посещенията;
- Идентификация на:
 - Персонал;
 - Посетители;
 - Охрана и сили за реакция;
- Технически средства.

4. СПЕЦИФИКАЦИИ НА ЕЛЕМЕНТИТЕ ЗА КОНТРОЛ НА ДОСТЪПА

Едни от основните компоненти в системата за Информационна сигурност Контролът на достъпа е ключов елемент от системата за физическа е използването сигурност. За осъществяване на ефикасен контрол на достъп е необходимо специфицирането и интегрирането на следните елементи:

- Зони за достъп;
- Сигурност на периметъра;
- Места за контрол на достъпа;
- Средствата за контрол на достъпа.

4.1. Зони за достъп

Дефинират се следните 5 (пет) зони на достъп:

- Публична зона;
- Зона за посрещане;
- Работна (операционна) зона;
- Зона за сигурност;
- Зона с най-висока степен за сигурност.

Йерархична структура на зоните за достъп

Съществуват две големи групи зони:

- Зони със свободен достъп;
- Зони с ограничен достъп.

Йерархията на зоните за достъп е както следва:

Зони със свободен достъп

Зоните със свободен достъп биват:

- Публична зона;
- Зона за посрещане (приемна);

Зони с ограничен достъп

Зоните с ограничен достъп биват:

- Работна зона;
- Секретна зона;
- Строго секретна зона.

4.2. Сигурност на периметъра

Осигуряването на сигурността на периметъра обхваща:

- Контрол на периметъра;
- Преглед на района, разположението на сградите и топографията;
- Услуги при извънредни ситуации;
- Осветление на района.

4.3. Места за контрол на достъпа

Контролът на достъпа се осъществява на:

- Входовете. Могат да се категоризират според критериите:
 - Основни и резервни
 - За хора и превозни средства
- Проверка на влизащите в зоните. В зависимост от влизащите:
 - Хора;
 - Превозни средства;
 - Предмети;
 - Поща.
- Зоните за предаване и получаване;
- Паркинги;
- Коридори;
- Сервизни помещения;
- Работни помещения.

4.4. Средства за контрол на достъпа

Контрол на достъпа до зоните с ограничен достъп се осъществява посредством:

- Идентификационни карти;
- Карти (баджове) за достъп;
- Електронен контрол на достъпа;
- Видео-наблюдение;
- Контролен център;

- Зони за чувствителни дискусии;
- Секретни стаи;
- Охрана (гардове) за сигурност

4.5. Други

Други елементи на системата за физическа сигурност, които не са обект на настоящия доклад а :

- Метални каси, шкафове и заключващи механизми
- Зони за сигурност
- Контрол на физическия достъп
- Охрана
- Видеонаблюдение
- Защита на периметъра
- Физически огради
- Точки за достъп
- Контрол на точките за достъп през физическата ограда
- Контрол на периметъра

ЗАКЛЮЧЕНИЕ

В доклада е споделен опитът на автора за изграждането на системата за физическа сигурност в държавните и частните структури в Република България, опитът като зам. председател на Държавната комисия по сигурността на информацията, лекции и упражненията, водени от автора в Университета по библиотекознание и информационни технологии (УниБИТ). Основната цел в условията на терористично противопоставяне и нови заплахи би трябвало да бъде: **РАЗВИТИЕ НА СПОСОБНОСТИ ЗА УВЕЛИЧАВАНЕ НА СИГУРНОСТТА В СИТУАЦИИ НА ИЗВЪНРЕДНИ СЪБИТИЯ ИЛИ ПОВИШЕНА ЗАПЛАХА.**

ЛИТЕРАТУРА

1. Закон за защита на класифицираната информация
2. Методика за изграждане и оценка на средствата и системите за физическа сигурност на класифицираната информация
3. Целков, В., Н. Стоянов и О. Исмаилов, Международни стандарти и добри практики за защита на информацията, За буквите – О писменехъ, София, 2010, 231 стр., ISBN 978-954-8887-67-0
4. Целков В., Работа в облака, големите данни и защита на личните данни, Информационен бюлетин на Комисията за защита на личните данни, брой 3 (42), ноември 2013, стр. 125 - 131
5. Tselkov V., Cloud Computing, Big Data, Accountability and New Challenges for Protection of Personal Data, 16th meeting, Central Eastern Europe Data Protection Authority (CEDPA) , 2-3 April 2014, Skopje, Macedonia
6. Tselkov V., New Challenges for Privacy and Personal Data Protection in Digital World, Regional Conference “Privacy in Digital Age”, 27-28 January 2015, Pristina, Kosovo
7. NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment.

8. NIST Special Publication 800-145, The NIST Definition of Cloud Computing.
9. ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security management.
10. National Security Agency (NSA) Information Assessment Methodology (IAM).
11. <http://www.nist.gov>.
12. <http://www.nsa.gov>.

ТЕХНОЛОГИЧЕН МОДЕЛ ЗА ОБРАБОТКА НА ДАННИ В ОБЛАКА

Веселин Ц. Целков

*Комисия за защита на личните данни
София, 1592, бул. „Професор Цветан Лазаров” № 2*

A TECHNOLOGICAL MODEL FOR DATA PROCESSING IN THE CLOUD

Veselin Ts. Tselkov

ABSTRACT: *This paper presents a hierarchical technological model in the digital world. Some of the main problems associated with data protection are addressed. Global trends and principles of data protection are [discussed](#) through the interpretation of the author.*

KEY WORDS: *Privacy, data protection, Internet, work in the cloud, devices connected to the Internet, big data*

1. ВЪВЕДЕНИЕ

Развитието на новите комуникационни и информационни технологии и по-конкретно Интернет и социалните мрежи поставят нови предизвикателства пред комуникациите между хората и защитата на личните им данни и неприкосновеността на личността. Потребителите на новите технологии използват услугите, които предоставя глобалната мрежа. Интернет и комуникират с приятели и колеги, използвайки услугите на социалните мрежи (Facebook, Twitter и др.). Новото поколение технологии поставят за отговор и множество въпроси:

- Запознати ли са потребителите с възможностите и услугите в мрежата?
- Запознати ли са потребителите със заплахите в мрежите?
- Как ви са мащабите и обемите на съхраняваните и обработвани лични данни?
- Как се използват личните данни от потребителите, от доставчиците на услуги и какви са параметрите за настройка?
- Какви са правата на хората да бъдат информирани за съхраняваните и обработвани техни лични данни и какви са механизмите за тяхното заличаване?

2. ЙЕРАРХИЧЕН ТЕХНОЛОГИЧЕН МОДЕЛ В ЦИФРОВИЯ СВЯТ

Новите предизвикателства за защита на личните данни са свързани с дефинирането на йерархичен технологичен модел в цифровия свят, както следва:

- **Първо ниво** – Интернет (Internet);
- **Второ ниво** - Работа в Облака (Cloud computing);
- **Трето ниво** – Интернет свързани устройства (Internet of Things);
- **Четвърто ниво** – Мобилни приложения (Mobile Applications);
- **Пето ниво** - Големите данни (Big data).

2.1. ПЪРВО НИВО - ИНТЕРНЕТ

Информационната инфраструктура, технологичните възможности и услугите изграждащи и предоставяни от Интернет са в основата на Йерархичния технологичен модел в цифровия свят.



Фиг. 1. Интернет

2.2. ВТОРО НИВО - РАБОТА В ОБЛАКА

Какво е работа в облака

Работата в облака е използването на компютърни (изчислителни) ресурси (хардуер и софтуер), които се предоставят като услуга (най-често абонаментна) по мрежата (обикновено Интернет). Името му идва от използването на символ с формата на облак като абстракция на комплексната инфраструктурата, която се съдържа в системните диаграми. Работата в облака осигурява отдалечени услуги с потребителски данни, софтуер и подходящата им обработка. Работа в облака е авторски превод на Cloud computing, който много често се среща като Облачни изчисления (включително и в официални документи на Европейския съюз). Определено може да се каже, че Работа в облака е смисленият и по точен превод на Cloud computing, отразяващ същността на технологиите и възможностите на Облака (Интернет технологията).



Фиг. 2. Работа в облака

Характеристики на облака

Характеристиките на работа в облака са:

- Самообслужване по желание (On-demand self-service);
- Широк достъп до мрежата (Broad network access);
- Групиране на ресурсите (Resource pooling);
- Бърза мащабируемост (Rapid elasticity);
- Измерване на услугата (Measured service).

Услуги в облака

Основните услуги за работа в облака са:

- Инфраструктура като услуга ([Infrastructure as a service](#), IaaS);
- Платформакато услуга ([Platform as a service](#), PaaS);
- Софтуер като услуга ([Software as a service](#), SaaS);

Допълнителни услуги за работа в облака са:

- Съхранение като услуга ([Storage as a service](#), STaaS);
- Сигурност като услуга ([Security as a service](#), SECaaS);
- Данни като услуга ([Data as a service](#), DaaS);
- Тестова среда като услуга ([Test environment as a service](#), TEaaS);
- Десктоп като услуга ([Desktop as a service](#), DaaS);
- Потребителски програмен интерфейс като услуга ([API as a service](#), APIaaS);
- Резервни копия като услуга ([Backend as a service](#), Baas).

2.3. ТРЕТО НИВО – ИНТЕРНЕТ СВЪРЗАНИ УСТРОЙСТВА

Устройства свързани с Интернет (Internet of Things) е днешна реалност, а не е научна фантастика. Електронните датчици са вече навсякъде: в нашия смарт

телефон; в колата; в къщата, управляват различни електрически системи, устройства за здравеопазване, фитнес монитори и работни места.



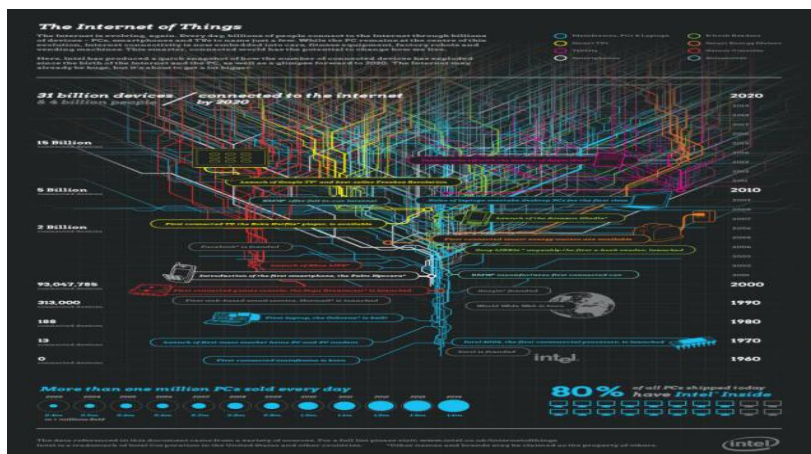
Фиг. 3. Интернет свързани устройства

Развитието на Internet of Things се описва с:

- Сензорите свързани с Интернет стартират през 70-те години на миналия век;
- Преди няколко години – увеличение;
- Последните две години – революция;
- Много устройства от различен тип;
- Много индустриални устройства.

Брой на сензорните устройства свързани с Internet по години (фиг. 4.):

- 1970 = 13;
- 1980 = 188;
- 1990 = 313,000;
- 2000 = 93,000,000;
- 2010 = 5,000,000,000;
- 2020 = 31,000,000,000 (прогноза).



Фиг. 4. Брой Интернет свързани устройства по години

2.4. ЧЕТВЪРТО НИВО – МОБИЛНИ ПРИЛОЖЕНИЯ

Мобилно приложение е компютърна програма, предназначена да работи на смартфони, таблетни компютри и други мобилни устройства. Приложенията, обикновено са достъпни чрез платформи за разпространение на приложения, които започват да се появяват през 2008 г. Обикновено се експлоатират от собственика на мобилната операционна система, като например AppleStore, Google Play, Windows Phone Store и BlackBerry App World. Някои приложения са безплатни, а други трябва да бъдат закупени.



Фиг. 5. Мобилни приложения

Типове мобилни приложения

Основните типове Мобилни приложения, в зависимост от предназначението им са:

- Комуникации (Communications);
- Търсене (Search based on location);
- Свързани с местоположението (Location based Apps);
- Резервни копия в Облака (Back up in the Cloud);
- Приложения базирани на сензори (Different sensors apps).

2.5. ПЕТО НИВО - ГОЛЕМИТЕ ДАННИ

В областта на информационните технологии, големи данни е една колекция от множества данни, толкова голяма и сложна, че става трудно да се обработи с използване на ръчни или конвенционални средства за управление на бази данни. Предизвикателствата включват обобщаване, консервация, съхранение, търсене, споделяне, анализ и визуализация. Тенденцията към обработката на по-големи масиви от данни се дължи на необходимостта допълнителната информация да се извлича чрез анализ на един голям набор от данни, свързани помежду си, за сравнението данните да се разделят на малки групи с общ размер, което позволява да се намери корелацията за бизнес тенденциите, да определи качеството на научните изследвания, превенция на заболяванията, връзката юридически цитати, борба с престъпността и т.н.



Фиг. 6. Големите данни

3. ОСНОВНИ (БАЗОВИ) ПРИНЦИПИ (BASE PRINCIPLES)

Няколко са базовите принципи, върху които се осъществяват дейностите свързани с неприкосновеността и защита на данните:

- Неприкосновеност (Privacy);
- Видимост и прозрачност (Visibility and Transparency);
- Отчетност (Accountability).

3.1. НЕПРИКОСНОВЕНОСТ

Новите моменти включват:

- Неприкосновеност при проектиране (Privacy by Design)
- Неприкосновеност при препроектиране (Privacy by Redesign)
- Неприкосновеност по подразбиране (Privacy by Default).

Неприкосновеност при проектиране

Неприкосновеността при проектиране се базира и се реализира в седем основни направления:

- Превенция, а не реакция (Proactive not Reactive; Preventative not Remedial);
- Неприкосновеността като параметри по подразбиране (Privacy as the Default Setting);
- Неприкосновеност, вградена в проекта (идеята) (Privacy Embedded into Design);
- Пълна функционалност (Full Functionality: Positive-Sum, not Zero-Sum);
- Сигурност от край до край - Защита през целия жизнен цикъл (End-to-End Security — Full Life cycle Protection);
- Видимост и прозрачност (Visibility and Transparency — Keep it Open);
- Зачитане (уважение) към неприкосновеността на потребителя (Respect for User Privacy — Keep it User-Centric).

Неприкосновеност при препроектиране

Как да се осигурят защитата на данните и неприкосновеността в работещи системи, които не са проектирани и реализирани с цел защита? – това е един от основните въпроси за разрешаване в съвременното информационно общество.

Неприкосновеност по подразбиране

Необходимо е защитата на данните и неприкосновеността да бъдат заложени в Правилата по подразбиране. С това се осигурява автоматична защита във всяка ИТ система или бизнес процес или практика. Не се изискват допълнителни усилия (действия) за защита на неприкосновеността и данните – всичко това е по подразбиране. *„Ако си в системата – ти си защитен“*.

3.2. ВИДИМОСТ И ПРОЗРАЧНОСТ

„Вярвай, но проверявай“. Необходимо е да се осигури пълна прозрачност и достъпност за множество въпроси, сред които:

- Какви лични данни се обработват;
- На какво правно основание;
- Къде и как се съхраняват;
- Кой има достъп до тях;
- На кого, защо и как се предоставят;
- Кога и как се унищожават;
- Как се осъществяват контрола и наблюдението.

3.3. ОТЧЕТНОСТ

Последните разработки в областта на глобалната политика и законовата уредба за осигуряването на неприкосновеността на личността обхващат:

- Нови модели за отчетност на действията;
- Как ще се оцени и изпита отчетността;
- Какви са критериите и опциите за отчетност.

Отчетността е един от основните принцип е едно от решенията за защита на данните в цифровия свят. Отчетността може да бъде разгледана в тринадесет основни направления, както следва:

- Поддържане на управленската структура;
- Поддържане на описите с данни;
- Поддържане на политиката за неприкосновеност и защита на личните данни;
- Поддържане на операционната политики и процедури;
- Повишаваща се тренираност и съзнание (убеждение);
- Поддържане на контролите за сигурност;
- Поддържане на договорите;
- Поддържане на бележките;
- Управление на въпросите, оплакванията и дискусиите;
- Мониторинг (непрекъснато наблюдение) за новите операционни (оперативни) практики
- Мониторинг (непрекъснато наблюдение) за нарушенията на личните данни;
- Мониторинг (непрекъснато наблюдение) на практиките за управление на личните данни;
- Следене на външните критерии.

4. ЗАКЛЮЧЕНИЕ

Новите взаимодействия (политически и икономически), новите информационни технологии и новите заплахи за неприкосновеността и личните данни са новите предизвикателства пред научните изследвания. За намиране на адекватни отговори и правилни решения е необходимо постигането на пълна интеграция и добро взаимодействие в усилията на:

- Държавните структури;
- Университетите и научните организации;
- Структурите на бизнеса;
- Неправителствените организации и медиите.
- Основните насоки на взаимодействията са както следва:
- Координация и кооперация;
- Идентифициране на усилията;
- Дефиниране (определяне) на насоките за развитие.

Представените в доклада проблеми свързани със сигурността и защита на данните в условията на бум на новите информационни технологии са резултат от изследванията и лекциите проведени в Университета по библиотекознание и информационни технологии в рамките на програмите за „Национална сигурност“ и

„Бизнес и Административна Сигурност”. Възможно е предложените разсъждения и твърдения да бъдат развити и прецизирани в бъдещи изследвания. Огразен е и опитът на автора, придобит от работата му в различните структури на Република България, НАТО и ЕС, занимаващи се с проблемите на сигурността на данните.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Конвенцията на Съвета на Европа за защита на гражданите по отношение на автоматичната обработка на личните данни
2. Директива 95/46/ЕО за защита на гражданите във връзка с обработката на личните данни и свободното движение на такива данни
3. Препоръка № R (87) 15 на комитета на съвета на министрите към страните-членки на Съвета на Европа
4. Денчев, С. Публичност и тероризъм, Публичност и тероризъм, „За буквите – о писменехъ”, София, 2005, ISBN 954-8887-07-X
5. Целков, В., Сигурността и защита на личните данни в процеса на глобализация, СВУБИТ, Научна конференция „Глобализация и сигурност”, 6 юни 2009 г.
6. Целков, В., Информационната цивилизация, глобализацията и неприкосновеността на личността, сп. Фонд за Научни изследвания, 2012 г.
7. Thomas, Richard, Data Protection in the European Union - Promising Themes for Reform, European Privacy and Data Protection Commissioners’ conference, Edinburgh, 24 April 2009.
8. 32-та Международна конференция на комисарите по защита на данните и неприкосновеността на личния живот, 27 - 29 октомври 2010 г., Йерусалим, Израел
9. 33-та Международна конференция на комисарите за защита на личните данни и неприкосновеността на личния живот, 1 - 3 ноември 2011 г., Мексико сити, Мексико.
10. 35-та Международна конференция на комисарите за защита на личните данни и неприкосновеността на личния живот, 2014 г., Мавриций.
11. Целков, В., Бумът на информационните технологии и новите предизвикателства за защита на личните данни и неприкосновеността на личността, Информационен бюлетин на Комисията за защита на личните данни, брой 6 (39), ноември 2012, стр. 118 - 126
12. Целков В., Работа в облака, големите данни и защита на личните данни, , Информационен бюлетин на Комисията за защита на личните данни, брой 3 (42), ноември 2013, стр. 125 - 131
13. Tselkov V., Cloud Computing, Big Data, Accountability and New Challenges for Protection of Personal Data, 16th meeting, Central Eastern Europe Data Protection Authority (CEDPA) , 2-3 April 2014, Skopje, Macedonia
14. Tselkov V., New Challenges for Privacy and Personal Data Protection in Digital World, Regional Conference “Privacy in Digital Age”, 27-28 January 2015, Pristina, Kosovo
15. Nymity Accountability Framework
16. Nymity Privacy Management Accountability Framework

BINARY INTRAPULSE MODULATIONS FOR RADAR PULSE COMPRESSION

MARIÁN BABJAK, ZDENĚK MATOUŠEK, JÁN OCHODNICKÝ

*Department of Electronics, Armed Forces Academy of M. R. Stefanik, Liptovský Mikuláš,
e-mail:marian.babjak@aos.sk, zdenek.matousek@aos.sk, jan.ochodnický@aos.sk*

ABSTRACT: *In the paper the performance of Walsh-Hadamard sequences (WHS) for binary encoding of radar signals is described. It is shown that between WHS with length 8, 16 and 32 it is possible to find a set of orthogonal sequences with good properties. Probability of correct range detection of selected WHS in presence of active noise jamming is described and it is compared with cases when Barker code and linear frequency modulation inside pulse duration are used.*

KEY WORDS: *Pulse compression methods; Radar signal processing; Spread spectrum radar.*

I. INTRODUCTION

Generally, the radar needs a large peak signal power to average noise power ratio (signal-to-noise ratio - SNR) at the time of the target return signal for good detection performance. The maximal achievable SNR depends on the total transmitted energy, but not on the presence of any modulation. Thus for good detection, many radars seek to transmit long-duration pulses to achieve high energy, because transmitters typically operates near their peak power limitation [1]. The use of a constant-frequency waveform imposes the two serious restrictions on the shape of the ambiguity function: the product of delay and Doppler resolution remains near to unity, and the pulse energy is directly proportional to the width of the resolution element in delay. To obtain adequate SNR on small targets, it may be necessary to extend the pulse width beyond the separation delay of the nearest target, preventing them from being resolved. If phase modulation of transmitted pulse is permitted, both these restrictions can be bypassed, and the resulting process is called pulse compression [2].

Pulse compression is a radar signal processing technique to increase the range resolution as well as to improve the SNR. This is achieved by modulating the transmitted pulse (spectrum spreading) and then correlating the received signal with the transmitted pulse. Rapid evolution of digital technologies brings also new approaches to the field of radar signal's designing and processing.

The resistance against active jamming in military radar applications is the most important factor when one compares their performance. It can be achieved by spread spectrum techniques which can be classified according to the method of spectrum spreading to Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) and Linear or Non-Linear Frequency Modulation inside pulse duration (LFM or NLFM). New types of radar signals were developed by applying spread spectrum techniques into the pulse radar technology. They are known as signals with intra-pulse modulation (IM). In this case a radar pulse is divided into multiple subpulses and frequency or phase modulation is applied inside of each subpulse. From this point of

view, it is possible to classify radar signals with intra-pulse modulation into the following groups [3], [4], [5]:

- Signals with continuous (linear or nonlinear) frequency modulation,
- Signals with discrete frequency modulation,
- Signals with binary phase modulation.

The using of these signals in radar technology enables to decrease transmitted power of radar, to improve range resolution and resistance against various kinds of active jamming. Binary coded signals have been widely used as radar pulse compression signals to achieve high-range resolution and to maintain the long-range detection capability. The main problem when using binary coded signals is finding sequences with proper autocorrelation properties. Binary sequences with low aperiodic side lobes of autocorrelation and small mutual cross correlation are required. Using of Barker codes of different length for binary encoded radar signals was proposed in [6], because they have good autocorrelation properties. Their disadvantage is that for defined length (7, 11, 13) there is only one sequence.

In this paper performance of Walsh-Hadamard sequences (WHS) for binary encoding of radar signals is described. It is shown that between WHS with length 8, 16 and 32 it is possible to find a set of orthogonal sequences with good properties. Probability of correct range detection of selected WHS in presence of active noise jamming is described and it is compared with cases when Barker code is used for binary encoding of radar signals and when widely used linear frequency modulation inside pulse duration is used to spread spectrum of radar signals.

II. WALSH-HADAMARD SEQUENCES FOR BINARY ENCODED RADAR SIGNALS

A. WALSH-HADAMARD SEQUENCES

The paper proposes to use Walsh-Hadamard sequences to binary coding of radar signal - spreading the spectrum of radar pulse with BPSK intra-pulse modulation (BPSK-IM). Walsh-Hadamard sequences are easy to generate, and orthogonal [8] in the case of perfect synchronization.

The Walsh-Hadamard sequences of the length N ; $N = 2^n$, $n = 1, 2, \dots$, are often defined using Hadamard matrices H_N [8], with

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (1)$$

and

$$H_{2N} = \begin{bmatrix} H_N & H_N \\ H_N & -H_N \end{bmatrix}. \quad (2)$$

The resulting matrices H_N are orthogonal matrices, i.e. for every N we have:

$$H_N H_N^T = N I_N, \quad (3)$$

where H_N^T is the transposed Hadamard matrix of order N , and I_N is the $N \times N$ unity matrix.

In such way we can generate N ; $N = 2^n$, $n = 1, 2, \dots$, orthogonal sequences $WHS(i, N)$, $i=1, 2, \dots, N$, with length N , each representing the i^{th} row of Hadamard matrix H_N .

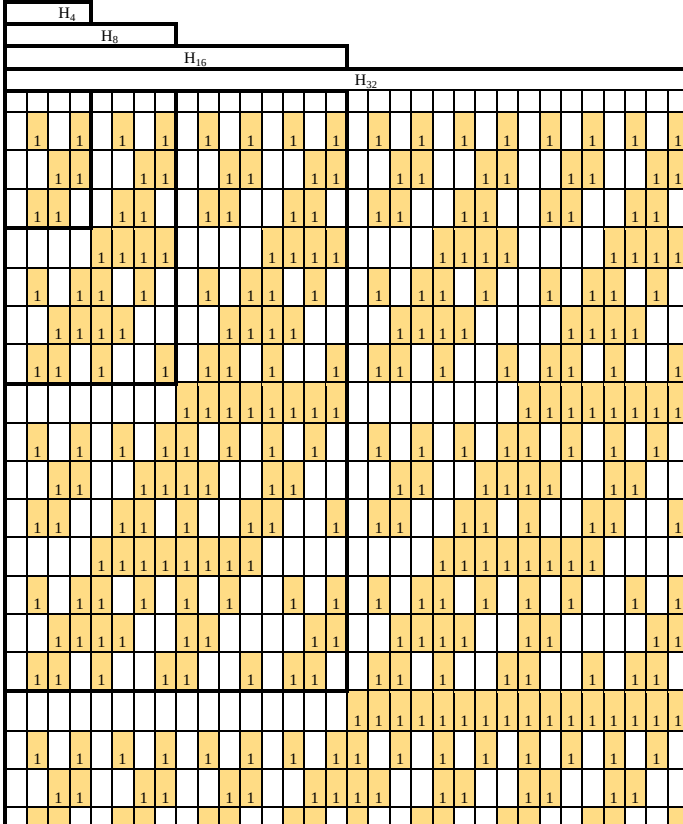
In this paper H_8 , H_{16} and H_{32} are used for binary coding of radar signal and to produce BPSK-IM inside radar pulse. Walsh-Hadamard sequences (WHS) for various N are shown in Fig. 1.

B. BINARY ENCODED RADAR SIGNALS

To apply the WHS for binary coding of radar pulse, we divide the transmitted pulse of duration PW into N subpulses of duration $PW_m = PW/N$. These subpulses are used to modulate carrier frequency by BPSK modulation. Resultant signal create BPSK-IM. Generally, the radar signal with BPSK-IM in time domain may be described as [10]

$$s(t) = \begin{cases} A \sin[\omega t + \Delta\psi_m] & \text{for } t \in \langle i.PRI, i.PRI + PW \rangle, \\ 0 & \text{for } t \in \langle i.PRI + PW, i.PRI + PW + DT \rangle \end{cases} \quad (4)$$

where ω is a signal frequency, t is time, $\Delta\psi_n$ is a phase deviation in the m^{th} subpulse (value 0 when the m^{th} bit in WHS equals +1 and value π when it equals -1), PRI is the pulse repetition interval and DT is dwell time. BPSK-IM signal in time domain is shown in Fig.2.



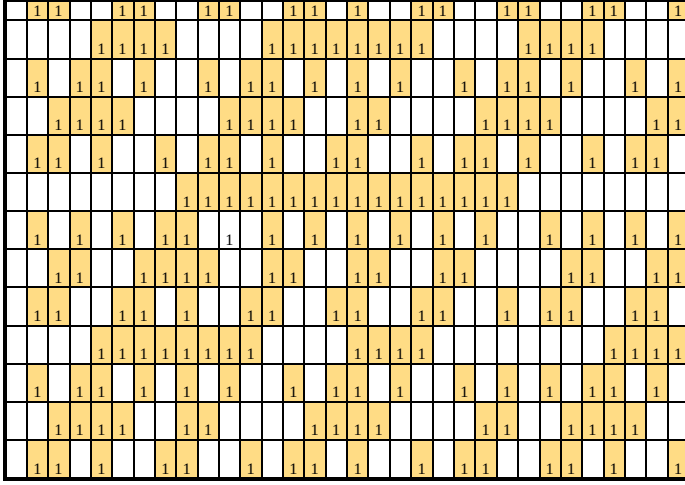


Figure 1. Walsh-Hadamard sequences for $N=4, 8, 16$ and 32

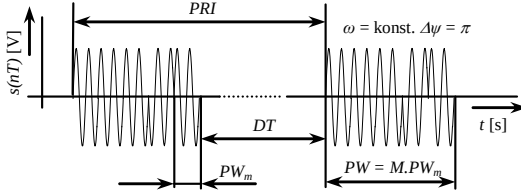


Figure 2. BPSK intra-pulse modulated signal in time domain

The effect of applying BPSK intra-pulse modulation with N subpulses to radar pulse is spreading its spectrum N times in frequency domain and can be represented as direct sequence spread spectrum system. At the receiver side during reception, signals which are coherent with used binary sequence are de-spread while all other signals not coherent with it are spread. So we can achieve broadband gain which is proportional to the pulse and the shortest subpulse run (PW_s) duration ratio

$$G_{BB} = 10 \log \frac{PW}{PW_s} \quad (5)$$

together with pulse compression.

C. PERFORMANCE OF WALSH-HADAMARD SEQUENCES

If we use the WHS from Fig. 1, each row of this matrix represents WHS for binary encoding of radar pulse during its pulse duration (PW). Because of WHS orthogonality it is possible to separate two radar pulses spread by two different WHSs from received signal, or in other words, to extract from received signal only that part which was spread by the certain WHS. But not all WHSs provide the same performance from the resistance to active noise jamming point of view.

Aperiodic autocorrelation function, very low or none side lobes in autocorrelation function and small mutual cross correlation are the most crucial parameters required from sequence for binary encoding of radar signals. Due to orthogonality of WHS they provide zero mutual cross correlation under condition of perfect synchronization. But not all of

them provide sufficiently low side lobes in autocorrelation function. By analysis of autocorrelation functions of WHSs, the following conclusions for selection of “good sequences” can be formulated:

- Good sequence should contain so many state transition as possible;
- Good sequence should has difference between the autocorrelation function maximum and the nearest side lobes in autocorrelation function big enough; the bigger difference will produce better performance.
- Good sequence should not contain periodic pattern;
- If there is periodic pattern, sequences with longer period will provide better performance.

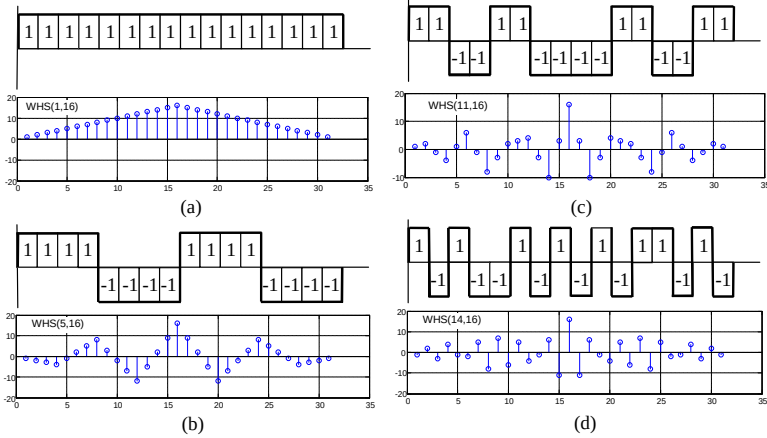


Figure 3. Walsh-Hadamard sequences and their autocorrelation functions for $N=16$, (a) $i=1$, (b) $i=5$, (c) $i=11$, (d) $i=14$

Walsh-Hadamard sequences with length 16 together with their autocorrelation functions are shown on Fig. 3. First sequence (Fig. 3a) WHS(1,16) contains all ones. There if no state transition in the sequence and its autocorrelation function is the same as autocorrelation function of radar pulse without intra-pulse modulation. First WHS for any N has these properties and it is not suitable for binary coding of radar signal. The 5th sequence (Fig.3b) WHS(5,16) has only three state transitions and the shortest subpulse run is 4, so $GBB=6$ dB. The 11th sequence (Fig.3c) WHS(11,16) has six state transitions the shortest subpulse run is 2, so $GBB=9$ dB. The 14th sequence (Fig.3d) WHS(14,16) has the best performance from the all above mentioned. It has thirteen state transitions and the shortest subpulse run is 1, so $GBB=12$ dB.

As the result of WHS property analysis for $N=8, 16$ and 32 we can observe following conclusions:

- The first sequence (all ones) cannot be used for binary encoding of radar signals;
- Other sequences can be divided into 3 groups – the worst, good, the best - according to above mentioned rules;
- All sequences in the group provide approximately the same performance.

III. MODEL FOR WHS ENCODED BPSK-IM RADAR SIGNALS IN PRESENCE OF ACTIVE JAMMING

For an analysis of using WHS encoded BPSK-IM radar signals in the case of active noise jamming, a radar model was designed and encoded in Matlab environment. This model simulates the generating and processing of the radar signals with the different jamming-to-signal ratio (JSR). The basic parameters of the proposed model are defined in Table I.

TABLE I. *Basic Parameters for Modelling*

PW_m	0.2 μ s
PRI	30 μ s
IF carrier frequency	30 MHz
Sampling period	$1/10 f_{max}$
Barker encoded BPSK-IM	Barker code with length of 13
WHS encoded BPSK-IM	WHS with length 8, 16 and 32
Jamming signal	Gaussian noise

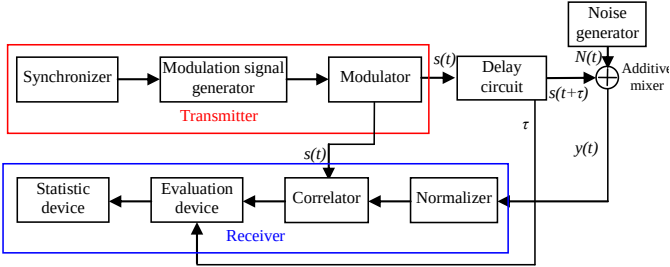


Figure 4. *The model for the binary encoded BPSK-IM signals and jamming generation and processing*

The model of radar system with BPSK-IM modulation, active noise jamming and the signal processing is presented in Fig.4. The synchronizer provides timing for the pulse and subpulse triggering. The modulation signal generator generates bipolar binary sequence which is used for BPSK modulation of carrier frequency. The delay circuit randomly generates delay τ of echo signal within the range from 5 to 25 μ s. Delayed signal $s(t+\tau)$ is mixed in additive mixer with noise $N(t)$ that is generated in the noise jamming generator. The result of mixer is an additive mix of delayed signal and noise given by

$$y(t) = s(t + \tau) + N(t). \quad (6)$$

The average power of active noise jamming $N(t)$ was modified during simulation in order to reach power ratio of JSR within the range from -3 to 9 dB. The JSR ratio is expressed by

$$JSR = 10 \log \frac{N(t)}{s(t+\tau)}. \quad (7)$$

In the next step, the delayed additive mix signal (echo) with noise $y(t)$ is normed and the correlation function with modulated signal $s(t)$ is computed in a correlator as

$$cor(m) = \sum_{n=0}^{N-m-1} (s_{[(n+1)T_1]} \cdot (y_{[(n+m+1)T_1]})^*, \quad (8)$$

where T is a sampling period, n is a number of signal samples, $m = 0, 1, 2, \dots, N-1$ and $*$ represents the complex conjugate.

A target range is evaluated (in the evaluation device) from the correlation function $\text{cor}(m)$ and it is compared with random delay of modulated signal that is adjusted in the delay circuit. A number of correct detection N_{COR} for given JSR is evaluated in the statistic device and after that is computed the probability of detection P_D which is defined as

$$P_D = \frac{N_{\text{COR}}}{N_{\text{PRI}}}, \quad (9)$$

where $N_{\text{PRI}} = 10\,000$ is the number of periods in which the statistical evaluation for given JSR was repeated.

IV. SIMULATION RESULTS

The simulations were performed to evaluate performance of WHS encoded BPSK-IM radar signals in presence of active noise jamming. Decompositions of WHS for $N=8, 16$ and 32 are shown in Table II, Table III and Table IV respectively together with required JSR for $P_D=0,8$. Decomposition was performed according to the rules described in section II.C and according to required JSR to achieve $P_D=0,8$ from simulation results. For each N , $N-1$ sequences (without 1st sequence) were divided into 3 groups – the best group (BG), the good group (GG) and the worst group (WG).

TABLE II. *Decomposition of WHS for $N=8$ into groups (JSR for $P_D=0,8$)*

The best group			The good group			The worst group	
Row	6	8	2	4	3	7	5
JSR	9,25	9,13	8,74	8,6	8,19	7,57	5,94

TABLE III. *Decomposition of WHS for $N=16$ into groups (JSR for $P_D=0,8$)*

The best group						The worst group		
Row	14	6	10	16	8			
JSR	12,58	12,43	12,41	12,41	12,39	12,25		
The good group						The worst group		
Row	11	15	4	3	2	7	5	13
JSR	11,6	11,22	11,11	10,91	10,74	10,32	9,55	8,31

TABLE IV. *Decomposition of WHS for $N=32$ into Groups (JSR for $P_D=0,8$)*

The best group										
Row	30	22	32	24	14	26	10	28	16	12
JSR	15,59	15,57	15,52	15,46	15,38	15,19	15,18	15,13	15,11	15,09
The good group										
Row	6	8	20	27	18	19	11	15	31	23
JSR	14,69	14,67	14,63	14,57	14,56	14,37	14,21	14,02	13,98	13,65
The worst group										
Row	4	3	7	5; 21	2	29	13	9	25	17
JSR	12,89	12,88	12,55	12,34	11,85	11,7	10,99	9,83	8,36	6,13

For WSH with $N=8$ there are 2, 3 and 2 sequences in BG, GG and WG respectively. So we have only 2 sequences with the best performance. To achieve more sequences with the best performance, we have to use WHS with $N=16$ or 32 . For WSH with $N=16$ there are 6, 6 and 3 sequences in BG, GG and WG respectively. Moreover, for WSH with $N=32$ there are 10, 10 and 11 sequences in BG, GG and WG respectively. We can see for the tables below that with using longer sequence length we gain not only more sequences in BG but also better resistance against to the active noise jamming. By increasing length of sequence by 2 we can achieve improvement about 3 dB from the JSR point of view for given P_D .

Relations between probability of correct range detection and JSR for the best sequences from each group (BG, GG, WG) for WHS with length $N=8, 16$ and 32 are shown in Fig.5. In the figures there is also shown the dependence for radar signal without IM. We can see that even using of sequences from WG for all N provides the significant gain with comparison to system without IM.

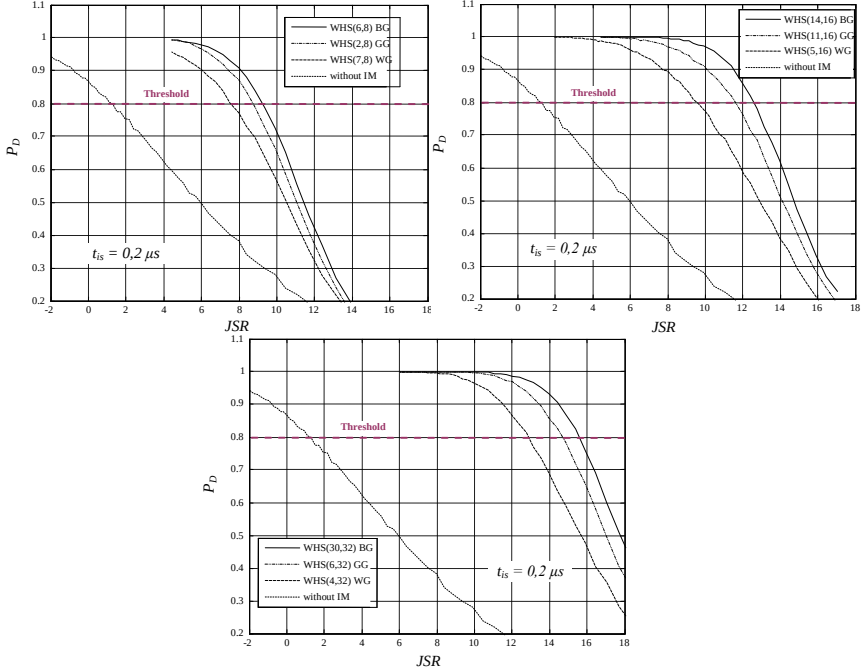


Figure 5. Probability of correct range detection versus JSR for WHS with length 8 ,16 and 32

Comparison of proposed binary encoding of radar signals with using WHS with cases when Barker code of length 13 is used for binary encoding of radar signals and when widely used linear frequency modulation inside pulse duration is used to spread spectrum of radar signals is shown in Fig.6. The better performance than the Barker 13 binary encoded and linear frequency modulation inside pulse duration radar signals can be achieved only by binary encoding by WHS with length 16 or longer. When using WHS with length 16, even by using of sequences from GG we can achieve approximately the same performance as with Barker 13 encoding. Moreover, for WHS with length 32, most of sequences from WG provide approximately the same performance as with Barker 13 encoding.

V. CONCLUSIONS

The aim of this article was to make an analysis of Walsh-Hadamard sequences for binary encoding of radar signals in presence of the active noise jamming. The decomposition of WHS with length 8, 16 and 32 into 3 groups with approximately the same performance was proposed. According to simulation results the best groups for $N=16$ and 32 will always provide the significantly better performance than systems with

Barker 13 binary encoded or linear frequency modulation inside pulse duration radar signals. When using WHS with length 16, even by using of sequences from the good group or WHS with length 32, most of sequences from the worst group provide approximately the same performance as with Barker 13 encoded or linear frequency modulation inside pulse duration radar signals.

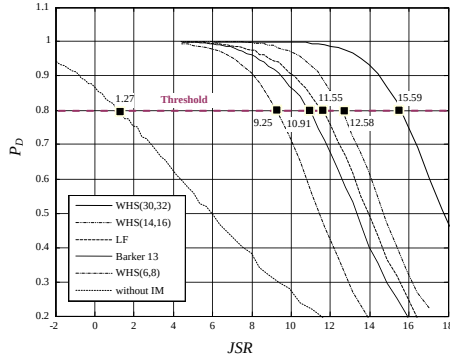


Figure 6. Comparison for the best sequence from the best group of WHS with length 8, 16 and 32 with the Barker 13 binary encoded and linear frequency modulation inside pulse duration

The big advantage of using of WHS for binary encoding of radar signals is that we have a set of orthogonal sequences for binary encoding instead of only one sequence in the case of Barker 13. Thus, we can randomly use various sequences in subsequent PRI and to make the system resistant also against the active response jamming, because only echo signals which are coherent with used orthogonal sequence will be processed in receiver. Another advantage of using WHS for binary coding is possibility to avoid mutual interferences of own radar systems. For each radar system only one sequence will be assigned this case.

REFERENCES

- [1] P. Z. Peebles, "Radar principles," John Wiley & Sons, Inc., New York, 1998.
- [2] D. K. Barton, "Radar system analysis and modeling," Artech House, Inc., Norwood, 2005.
- [3] O. A. Dobre, A. Abdi, and Y. Bar-Ness, W. Su, "Survey of automatic modulation classification techniques: classical approaches and new trends," IET Communications, vol. 1, (2), 2007, pp. 137-156.
- [4] Z. Yu, Y. Q. Shi, and W. Su, "A Practical classification algorithm for M-ary frequency shift keying signals," Proceedings of the IEEE Military Communications Conference MILCOM 2004, Monterey, 2004, pp. 1123-1128.
- [5] Y. Yao, J. Chen, and Z. Huang, "Recognition of frequency modulation signal using parameter invariant filter," Journal of Shanghai University, vol. 9, (5), Shanghai, 2005, pp. 415-418.
- [6] M. I. Skolnik, "Radar handbook. Chapter 10.," McGraw-Hill, New York 1990.
- [7] H. Deng, "Effective CLEAN algorithms for performance-enhanced detection of binary coding radar signals," IEEE Transactions on Signal Processing, Vol. 52, No. 1, January, 2004.
- [8] G. M. O. Silva, J. C. A. Santos, and M. H. C. Dias, "RF jamming coverage prediction at mixed-path urban scenarios," SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC), Belem, 2009.
- [9] O. Svenson, "Topics in Theoretical Computer Science," EPFL-IC, Lausanne, Switzerland, 2014.

[10]P. Prasanthi, P. R. Kumar, and A. K. Singh, "FPGA implementation of time frequency algorithm for intrapulse modulation recognition of radar signals," International Journal of Emerging trends in Engineering and Development, Issue 2, Vol. 7, November 2012, pp. 571-578.

APPLICATIONS OF SOFTWARE DEFINED RADIOS IN WIRELESS SENSOR NETWORKS

ROMAN BEREŠÍK

*Department of Electronics, Armed Forces Academy of M. R. Štefánik, Liptovský Mikuláš,
e-mail:roman.beresik@aos.sk*

ABSTRACT: *Wireless sensor networks become widely used not only in industry sector but also in military and security applications. In many cases, these sensor applications require to use the data rate and waveforms which ZigBee based wireless sensor networks are not able to employ. Software defined radios have a potential to replace the low power wireless technology in sensor systems and at the same time to provide effective frequency management within wireless sensor network.*

KEY WORDS: *Wireless sensor network, software defined radio, sensor system.*

I. INTRODUCTION

There is significantly increased effort in design of a new integrated circuit technology and its incorporation into computing and communication systems. These systems enabled us to monitor and control processes via analog and digital signal processing means and sensors. Sensor systems can be found in automotive industry, environmental monitoring applications and also in military and security systems. Many of these systems are networked in order to enhance control mechanisms of monitored physical processes. Due to the fact that the connection of sensor systems into hierarchical higher layers is realized via wireless technology, there are many problems to overcome before the data will be available on the Internet.

The technology of Wireless Sensor Networks (WSNs) is widely used in applications where other sensor systems could be hardly exercised due to limited access to the communication backbone. As it was mentioned previously, WSNs can be used in military environment as part of Unattended Ground Sensor (UGS) systems. UGS systems are used for the monitoring of remote areas where systems act as permanent or temporal surveillance. WSNs can also be deployed in urban environment where is necessity to share the frequency band with other wireless technologies. The typical example is when the WSN operates in unlicensed ISM (Industrial Scientific and Medical) frequency band. There are several wireless technologies which operate in ISM frequency band, like WiFi, Bluetooth and also ZigBee and IEEE 802.15.4 technology. Basic element of WSN, which employ ZigBee standard, consists of sensing subsystem, low power radio frequency communication subsystem and computation unit (e.g. MCU) integrated into one platform called sensor node. An on-board computation unit allows sensor node to process gathered data internally, if it is necessary, before transmitting backwards to the gateway (GW) and

subsequently to monitoring and control system (e.g. personal computer) for further processing. In the real situation, the deployment of WSN which contains several tens wireless sensor nodes; can cause huge demand for communication channels within used frequency band. The ZigBee and IEEE 802.15.4 based WSNs have their own limitation in terms of frequency channel number and data rate available for reliable data transfer within WSN. The radio frequency spectrum is considered the most expensive and scarce resource among all wireless network resources, and it is closely followed by the energy consumption, especially in low energy, battery powered sensor network devices [1]. The operation of WSN in ISM frequency band become challenge not only because of coexistence issues of WSN with other wireless technologies, but also because of necessity to guarantee the sufficient data rate for transmitting sensed data over the given radio channel. One of solutions how to solve frequency management tasks in WSNs is to use software defined radios (SDRs).

II. WIRELESS SENSOR NETWORKS AND UGS SYSTEMS

The UGS systems are capable to monitor remote areas and provide data for detection, identification and classification of events in monitored area [2]. They can be designed as low power sensor systems with low data rate or as high performance sensor systems when guaranteeing sufficient data rate is main issue. In general, WSNs can contain hundreds of sensor nodes equipped with the sensing, computing and communications subsystems. The basic structure of WSN and its integration into hierarchical higher layers is shown in Fig 1.

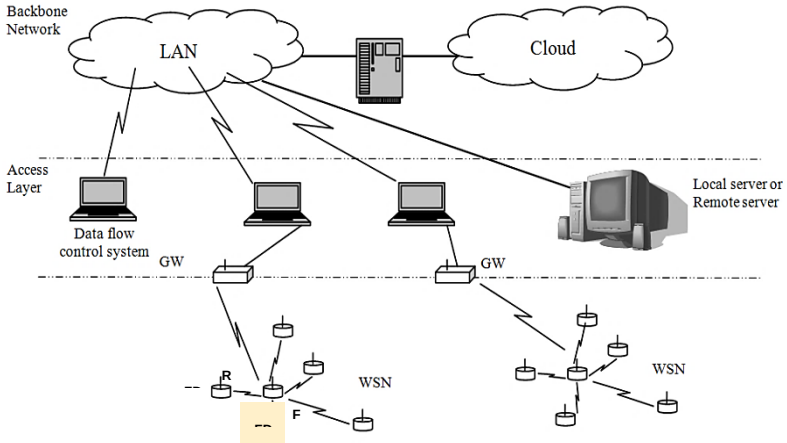


Figure 1. Structure WSN and its interconnection into hierarchical higher layers [2]

The lower part of the structure, shown in Fig. 1 consists of two WSNs arranged in star topology. In this case, sensor nodes which act as reduced-function devices (RFD) are connected to the fully-function devices (FFD) and create the cluster. The RFD can only talk to the FFD which acts as router. The data transmission in cluster and on the way to the gateway (GW) is realized in certain frequency channel. The GW can also act as sensor node, similar to other sensor nodes of WSN in cluster, or it may be entirely different, performing, e.g., extra signal processing and communications tasks and having

no sensors [1]. Next layer, access layer, can perform the data transfer sensor data servers and/or cloud if available. One of problems which must be considered during the WSN deployment is the electromagnetic coexistence among other wireless technologies used in monitored area. The TABLE I represents the comparison of parameters ZigBee wireless technology from the physical layer of ISO/OSI model point of view. From the TABLE I. implies that when 2.4 GHz frequency band is used, one of 16 frequency channels can be used for data transmission with data rate 250 kbps. When WSNs with several tens or hundreds of sensor nodes operate in same monitored area, the frequency channels used by WSNs must be properly planed in order to avoid mutual jamming among WSNs. Mutual jamming of the WSNs can cause data transfer latency or data transmission failure [3].

TABLE V. *Physical layer of ISO/OSI model of ZigBee [1]*

Frequency (MHz)	Number of channels	Data rate (kbps)	Modulation	Country
868-868,6	1	20	BPSK	Europe
902-928	10	40	BPSK	USA
2400-2483,5	16	250	O-QPSK	World Wide

The Fig. 2 represents typical situation when several wireless networks share the same frequency band, in this case 2.4 GHz ISM frequency band. It can be clearly identifiable the presence of WiFi 802.11g (6th channel), Bluetooth 802.15.1 and ZigBee wireless node tuned on its 26th frequency channel (2437 MHz). In this scenario, the ZigBee based WSN, WiFi and Bluetooth wireless networks can coexist side by side without degradation of ZigBee WSN performance. However, this assumption is not valid when several WiFi and Bluetooth networks operate in same area and ZigBee WSN uses another frequency channel other than 26th one.

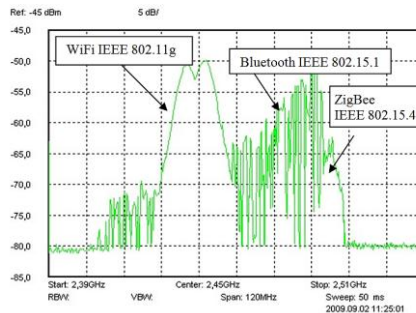


Figure 2. *Utilization of 2.4 GHz ISM frequency band [3]*

Outcomes of experiments presented in [3] showed that when the ZigBee WSN operated in 18th frequency channel (2440 MHz), which was already occupied by WiFi network (e.g. 6th channel), the successful data transfer was decreased to 79 % (distance of ZigBee sensor node from WiFi AP was 15 m).

III. SOFTWARE DEFINED RADIO IN WIRELESS SENSOR NETWORK

As it was mentioned previously, the typical ZigBee wireless sensor node consists of the low power, low data rate RF transceiver and 8 bit MCU (e.g. MicaZ). This configuration of sensor node is suitable for application like event driven sensor systems, when the data transfer is initialized only when certain event or events occur and subsequently confirmed. However, the situation is different when it is necessary to carry out data transfer from high performance sensor systems which consist of seismic, acoustic, magnetic and image sensors. The signatures of events described based on data from seismic, acoustic, magnetic and image sensors are represented by high amount of data. For instance, the seismic signal is typically sampled by 2500 Hz and one sample of seismic signal is represented by 24 bits. The duration of one second signal consists of 7500 byte of data. The amount of data from rest of sensors is same or higher. The transfer of such amount of data requires using different wireless standards in different frequency bands. Current advances in design of SDRs show that they will be able replace low power radio frequency transmitters of wireless sensor nodes and subsequently to change the approach how to ensure the reliable data transfer, electromagnetic coexistence and frequency management in given frequency band. Some described problems can be solved via cognitive radio (CR) approach which has ability to sense the spectrum and determine vacant frequency band [4, 5]. The structure of wireless sensor node which consists of the SDR differs from ZigBee one. The main function of the SDR based sensor node is to perform not only sensing of physical quantities in monitored area but also sensing on the frequency band at same time [5]. Similarly to ZigBee sensor node, the SDR based sensor node also consists of the signal processing unit, circuitry able to interface with analog and/or digital sensors and power supply unit. One of possible architectures of SDR wireless sensor node is shown in Fig. 3. Due to the fact that upper mentioned tasks dedicated to SDR wireless sensor node require high performance CPU, the computation core can contain the ARM processor based evaluation board, like Raspberry Pi 3 or ODROID C2. These two platforms have several things in common and one of them is that they use Linux like OS, the Ubuntu and Raspbian OS. Moreover, these platforms provide not only sufficient computation power, but also means to connect the SDR with outside world via Gigabit Ethernet and USB interfaces, or interface sensors system via standard SPI and I2C interfaces.

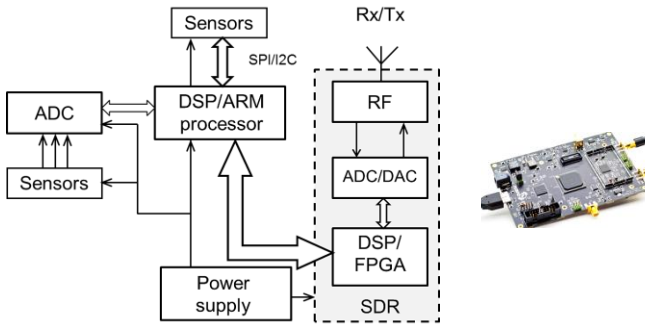


Figure 3. Possible architecture of SDR wireless sensor node

From the wireless data transfer and spectrum sensing point of view, the key part of architecture is created by the SDR. There are several requirements which should be

considered. The SDR should be battery powered, self-contained, portable and easily integrable into sensor node from hardware and software side. Several SDR platforms are suitable to fulfil these requirements. One of them is portable SDR named bladeRF x40 [6]. The SDR bladeRF x40 has following basic parameters:

- 300 MHz - 3.8 GHz RF frequency range,
- Independent RX/TX 12-bit 40 MSPS quadrature sampling,
- Capable of achieving full-duplex 28 MHz channels,
- On-board 200 MHz ARM9 with 512 kB embedded SRAM,
- 2x2 MIMO configurable with SMB cable, expandable up to 4x4,
- Stable Linux, Windows, Mac and GNU Radio software support.

The support of the Linux and GNU Radio environment, together with ARM based computation unit provides the possibility to design portable embedded SDR wireless sensor node as a part of modern WSN.



Figure 4. Interfacing of bladeRF and Raspberry Pi [6]

IV. CONCLUSIONS

The aim of paper was to provide the basic analysis of usage SDR in wireless sensor network as a part of the UGS systems. The key point for successful data transfer within WSN is effective utilization of operational frequency band. It is done via spectrum sensing, frequency channel allocation and waveform generation. When high performance sensor systems are used in military applications, like seismic and acoustic sensor systems, high data rate is required to be provided by radio communication means. In embedded sensor systems it can be done via implementation of software defined radios.

References

- [1] G. Pottie and W. Kaiser, "Principles of Embedded Networked Systems Design," Cambridge University Press, Cambridge, 2005.
- [2] A. Sabo, R. Beresik, J. Puttera, "Design of usage of the Intelligent Wireless Sensor Networks for protection and early warning purposes ," [in Slovak], In. International Conference of the New Trends in Signal Processing IX, Liptovský Mikuláš, 2008, pp. 258-261.
- [3] R. Beresik, J. Puttera, "Immunity of Wireless Sensor Networks ZigBee against interference," [in Slovak], In: International Conference of Communication and Information Technology 2009, Liptovský Mikuláš, 2009, pp. 1-5.
- [4] O. B. Akan, O. B. Karli and O. Ergul, "Cognitive Radio Sensor Networks," Journal of IEEE Network, vol. 23, (4), 2009, pp. 34-40.
- [5] S. Anusha and V. Mohanraj, "Dynamic Spectrum Access in Cognitive Radio Wireless Sensor Networks Using Different Spectrum Sensing Techniques," International Journal of Applied Engineering Research, vol. 11, (6), 2016, pp. 4044-4048.

- [6] Nuand, “bladeRF-the USB 3.0 Superspeed Software Defined Radio”, available online: <http://nuand.com/>, 2016.

BEST PRACTICES IN BUILDING PRIVATE CLOUD

Anatoly T. Peshev

peshev@outlook.com

ABSTRACT

This paper (1) outlines security issues and considerations in cloud computing and (2) provides an overview of the best practices in cloud computing security. Many organizations today are implementing cloud-based solutions. The regulatory environment within which they operate may generate particular issues with cloud-based data storage, such as legislation on data access.

KEY WORDS

Cloud Computing, Security, Private Cloud

Security is one of the major concerns in cloud computing. To mitigate security risks while still gaining benefits from cloud computing, organizations can choose to focus on on-premises solutions (private cloud). Moving to a cloud-based platform requires a change in mindset for IT security professionals. Traditional security models include, among an essentially limitless array of security systems, physical security, firewalls, anti-virus software, identity and authorization systems and perimeter networks (DMZs). They can also be applied in the private cloud model.

By taking a fresh look at security when moving to a cloud-based model, security practices will evolve to include the unique requirements imposed by the cloud, which do not map precisely with traditional on-premises approaches. In spite of the differences in approach, it should still target security levels which are at least as high existing on-premises solutions, as the opportunity for architecting security into the cloud-based solution is optimal when changing the core of your IT architecture from traditional on-premises to either Private Cloud or Hybrid Cloud.

In a cloud-based platform, regardless of whether it is private or public, organization is working in an abstracted and virtualized environment. The platform or software may run on top of a shared physical infrastructure managed internally (as in the case of Private Cloud) or by the service provider (as in the case of Public Cloud). The security architecture used by the applications will need to move up from the platform infrastructure to the application layers. For example, if Software as a Service (SaaS) application is provided by a public cloud vendor, there is no control over the software development platform or infrastructure and it is needed to consider and apply all available and necessary security controls at the application level.

Because of what seems like excessive reliance on the CSP to provide robust security

controls, Private Cloud might be seen to have an advantage since perimeter defense security mechanisms are available and are under the control of the organization. However, this advantage may be more apparent than real, since the highest impact security breaches occur internally, behind the firewall and other network-centric security devices and therefore a cloud-based architecture should be seen as an opportunity to protect against all threats (not just attacks by outsiders) by assessing and architecting a security design that places emphasis not only on traditional perimeter security, but throughout the entire stack. If you take the approach that *all* networks are untrusted, then the security you put in place in your newly architected cloud solution will be more robust than your current design and align itself more closely with the threat landscape we see today.

Whether the cloud architecture is public, private, or hybrid, applications must be designed so that they:

- Expose a reduced attack surface
- Run with least privileges
- Validate inputs
- Require user authentication
- Enforce authorization policies
- Encrypt data on disk
- Encrypt data over the network
- Encrypt data at the client application

This process describes a methodology for how applications should be written before any move to a cloud-based infrastructure and, if these practices have already been implemented, the risks in adapting to a cloud deployment model are reduced.

Security issues

The Private Cloud model requires total control over all layers of the stack, which includes any traditional network perimeter security you might want to have in place. In a private cloud model, the cloud services are not typically exposed general Internet users (although they can be) and remote access to private cloud hosted resources is enabled through mechanisms used in traditional data centres (although a private cloud can host perimeter security devices hosted on a cloud infrastructure).

In this scenario organization could rely on traditional enterprise security architectures and methodologies; however there are a number of reasons to consider a redesign of the security architecture when moving to a Private Cloud:

- A well architected and designed Private Cloud infrastructure would be prepared for an evolution to hybrid or public cloud computing in the future. This is the most compelling reason for adopting a private cloud infrastructure, since it enables a stepping-stone to a hybrid cloud solution.
- Private Cloud computing typically uses virtualization technologies to increase hardware utilization and to abstract compute, memory, network and storage component from Private Cloud consumers. Organization should be particularly aware of any vulnerabilities to the hypervisor and the patches needed to fix these. There have been hypervisor vulnerabilities that have allowed a guest operating system to run processes on other guests or the host.

- While traditional perimeter security provides protection from the Internet, it is often not configured to protect resources against attacks sourcing from within the organization. It is extremely unlikely that every piece of information should be available to every department and at every level in the hierarchy.
- The most deleterious security breaches come from inside the organization and therefore treatment of the traffic inside the Internet perimeter with as much security as the traffic outside is required.
- In a Private Cloud environment, it is possible that virtual machines will be able to communicate with each other from within the virtual environment and not send traffic over a physical Ethernet connection. To ensure that virtual machines only communicate with virtual machines that they should communicate with, network level authentication and encryption mechanisms should be used, such as those provided by IPsec.
- The host operating system should be isolated from all virtual machines contained within it. There should be no back-channels that enable guest virtual machines from communicating with the host operating system over either virtual or physical network connections.
- The host operating system must be free from malware, and mechanisms, such as anti-malware software, must be in place to detect potential compromise. The host operating system should not have Internet connectivity, and any updates required for the host operating system should be obtained from a trusted source on the intranet, which has had the opportunity for scanning all updates prior to delivery to the host operating systems.
- In a Private Cloud environment, guest virtual machines belonging to different security zones should not be hosted on the same virtual server. For example, if the Private Cloud virtual server is hosting Internet facing resources, such as virtual firewalls, or Internet-facing front-end applications, these Internet-facing guest virtual machines should not be hosted on the same virtual server as non-Internet facing guest virtual machines, such as those hosting internal database and collaboration information.

Security Considerations

With Software as a Service (SaaS) solutions as the most common nowadays, the security options that organization can control may be only at the application level. In a Public Cloud scenario, this requires a high degree of trust in the cloud vendor because they have complete control of the infrastructure and platform layers. While network security is not typically considered a part of SaaS, there is no reason it cannot be implemented in addition to application specific controls included in the SaaS solution.

Storage and Data

Although SaaS is not concerned directly with storage, you should ensure that data is encrypted as it travels across the Internet and if the data is stored at a Public Cloud vendor facility you should investigate their storage encryption mechanisms and their overall storage architecture. Specialist storage vendors typically store all of the data from all customers together and therefore the risks of data being accessed by another customer from the same cloud vendor can be high.

Client Security

As well as the SaaS software itself, it should also be considered browser vulnerabilities and compatibility. Browser updates should be implemented quickly, but should also be tested to ensure they are fully functional with the SaaS software. Processes should be put in place to test, evaluate, and deploy updates for critical browser updates.

Cloud Security Compliance

Privacy Compliance

Depending upon which country the organization is in, people have varying rights regarding the data that it holds about them. Typically, an individual can ask to see this data or have this data destroyed and this data must be treated as confidential and not shared with other parties without the express permission of the individual.

Geographic Compliance

There are risks which come with international storage and these should be assessed and mitigated through contracts. There are also regulations that require the disclosure of private data to government agencies. Regulations which require privacy in one country are often contradictory to regulations which require disclosure in another. Geographic considerations mostly affect data storage, but may also affect data processing. Therefore it should be considered:

- whether regulations are enforced based on where the data is stored,
- where the data is processed, or
- where the individual resides that the data concerns.

Industry Compliance

Industry compliance considerations are typically seen as an area where many cloud migrations flounder. Organizations such as financial and medical institutions typically operate under strict compliance regulations, so these bodies are always particularly aware of any issue that can have a regulatory implication.

With Private Cloud implementations, there are significant advantages to be realized from this type of environment. One major advantage of implementing a Private Cloud is the possibility that data is no longer stored on the individual computers. With this fundamental shift in storage location should be enough to interest compliance officers that Private Cloud systems can make their lives simpler by centralizing data in one area where it can be tracked and audited more effectively.

Compliance Factors

There are many areas that have to be considered when seeking to look at migrating to cloud architecture from a compliance perspective. Compliance factors in cloud-based environments include:

- Platform integrity and security. It must be considered what possible vulnerabilities might arrive from adopting a cloud-based environment and the risks that those vulnerabilities might bring. With SaaS and PaaS, there is an element of shared responsibility for ensuring platform integrity and security that is shared with the service provider but with IaaS, the responsibility for this integrity and security falls entirely on the hosted organization.

- Who has access to the applications and the data that those applications process? Just as on a local area network, it should be guaranteed that only authorized people have access to applications and data.
- What access rights do privileged users have? The administrative staff of the organization providing the cloud service will need rights to the applications that run within the cloud service in order to manage the service.
- Where is the data stored? Certain compliance regulations specify that data must reside within a particular country or region
- What facilities are there for federated reporting and auditing? Auditing and reporting forms a central part of compliance checking and it is vital that any cloud service that is selected provides federated reports across the entire environment and can also generate and supply adequate auditing information for any likely investigation of your computing environment.

Best Practices to Secure Cloud Deployment

The most important task in securing the cloud deployment is the centralization of the data, application and identity management.

Centralized Data Management

It is not rational to manage access at every server, because many deployments contain hundreds or even thousands of servers. IT can not really determine data rights and access rules. IT can, however, establish a role-management system with which business owners can permit or deny access relevant to business objectives. The regulatory environment has become increasingly stringent both for data modification and data access. This requires a new paradigm: one that will allow data to migrate to whichever server is best able to service access requests, while ensuring compliance at reasonable cost. Some of the requirements to consider for data management in a cloud environment are:

- Fast access to data for which the user is authorized, and when and where it is required
- Access not compromised by a natural or business catastrophe
- Data discovery by legal governmental requests, assuming the enterprise can provide the data needed
- Data Loss Prevention (DLP) is an integral part of the service offering
- A service-oriented architecture (SOA) should enable easy data migration back and forth to the cloud
- Identity of data must not include its physical location, so that the data can easily be moved
- Location tags for data should be the logical country of origin, not the data's physical location
- Data backup and recovery operations need to be based on the data identity, not its location
- Data-access rules can be created and maintained by the business owner of the data
- Access permissions can be viewed by compliance auditors

- Sensitive data can have audit controls for both modification and access
- Separation of duties prevents the same administrator from modifying data and audit logs
- Service Level Agreements (SLAs) need to spell out everyone's expectations and responsibilities

As an example, organization can use Microsoft SharePoint Server as critical communications channel through which people can get current information, with the ability to search quickly for the information that they need when they need it. Availability and reliability can be tracked with Microsoft System Center Operations Manager (SCOM) and other analytic tools.

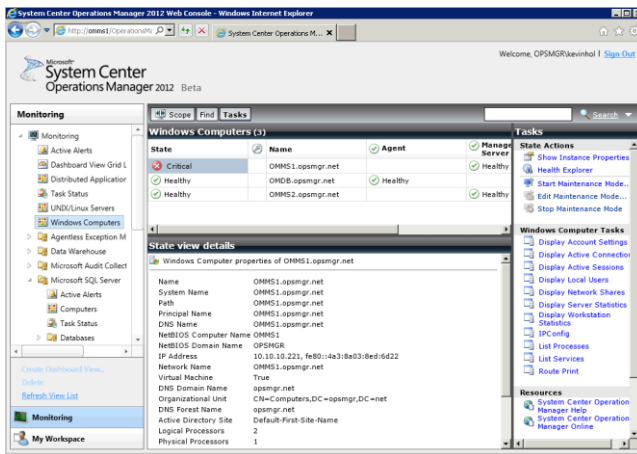


Fig. 1. System Center Operations Manager 2012

Because SharePoint supports both internal and external network connections, the server locations can adapt to suit the current network topology without concern for local, cloud or mixed environments. This deployment can realize the following benefits:

- Supporting store growth and capacity needs by improving system stability with effective monitoring and reporting tools
- Allowing store partners to work more efficiently and effectively with an intuitive portal interface and easy access to information across the enterprise
- Maintaining data security with enhanced document management and privacy functionality
- Aligning store priorities with company objectives by integrating trends and growth reports with partner communications

Centralized Application Management

Web-based applications have steadily grown in importance, to the point where a new name seemed necessary for the combination of service-orientation and standardized Internet service interfaces – hence the term “cloud computing.” What is new and different today from 10 years ago is the attention given to the value that’s available at reasonable marginal cost. A company no longer needs to develop Exchange expertise to have the

benefit of Exchange services, as there are a number of vendors competing to provide that service.

For a service to migrate easily from a local location to the cloud and back again, the application needs to provide a standard service-oriented set of interfaces for use both locally and in the cloud. This is why a cloud application was initially called software as a service. When a business application is undergoing a revision, it is a good time to include time to review the application-interface specifications to see if they can fit one of the existing Web services standards.

All authorization claims and authentication identity need to be shared by all resources, whether local or cloud-based. Over time, all applications will become able to migrate to the most efficient locale to meet their organization's expectations. At that point, moving an application is a simple matter of changing a directory entry for the application. Provisioning resources is just a base functionality of the services provider selected. The cloud provides a virtualized view of the resources that looks like a single computer, one that is never down for services, but could in reality be hosted on many machines or shared on a single machine, as demand requires.

Identity Management

Every organization should have its own identity-management system to control access to information and computing resources. That identity should have the same weight for getting authorization to run applications in the cloud.

External identity providers will typically only verify customers or other casual users. Therefore, the cloud identity system needs to track the owner of each identity and the level of assurance that is given to that identity. Coexistence of services in local and cloud environments is only possible when the same standard service identity interface is used for authorization in both environments.

Only a few organizations will be interested in creating their own private cloud service. For those doing so, the cloud identity solution will need to work across all divisions and acquisitions. While it is possible for a cloud service to create its own identity provider, such a proprietary solution would take it outside of our definition of a true cloud service.

These cases would need a federation gateway from each cloud service to link the external identity to an internal identity manager, such as Forefront Identity Manager (FIM), to provide a clean and quick authorization provider for each cloud resource completely independent of the original identity provider. Identity providers must create a list of all known sources of identity used to authorize access to resources to be sure that any cloud services provider can accommodate all of them.

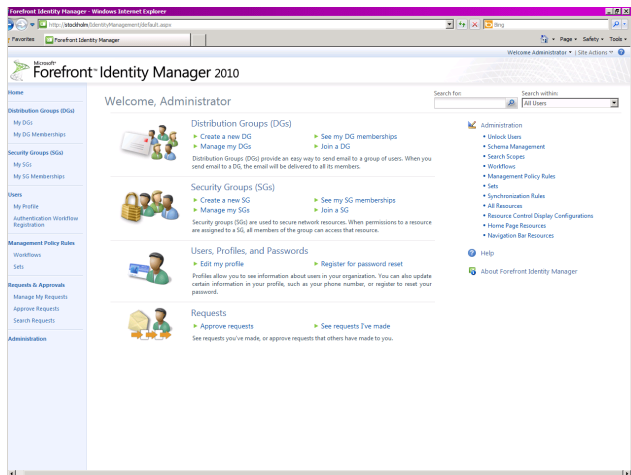


Fig. 2. Forefront Identity Manager 2010

The end-point application and data servers will need to be aware of the origin and reliability of the identity presented in such heterogeneous environments before authorizing access. Thus, for example, critical information can be protected with the organization's own Active Directory while the external identity provider can be used for tracking customer behaviour over an extended period.

Conclusion

Private cloud-based systems introduce new challenges in authentication and authorization, as organizations must be able to identify users with confidence without generating excessive overhead related to account provisioning. Security decisions must be well-defined and very granular, particularly in multi-tenant environments.

References

1. Shoikova, E, Peshev, A. (2012). Managing Private Cloud Computing Infrastructure
2. Shoikova, E, Peshev, A. (2011). Research of Cloud Computing Driven Knowledge Management
3. Shinder, T. (2011). Cloud Computing Security Architecture
4. Shinder, T. (2011). Security Implications of Cloud Service and Deployment Models
5. Griffin, D. (2010). Cloud Security: Safely Sharing IT Solutions

ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ И НОВИТЕ ЕВРОПЕЙСКИ РЕГУЛАЦИИ

Цанко Цолов

Комисия за защита на личните данни

София бул. „Проф. Цветан Лазаров“ 2

I. ВЪВЕДЕНИЕ

На 25 януари 2012 г. Комисията предложи всеобхватен пакет за защита на данните, състоящ се от:

— посоченото по-горе предложение за общ регламент относно защитата на данните, което е преназначено да замени Директивата за защита на данните от 1995 г. (бивш първи стълб);

— предложение за директива относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции и относно свободното движение на такива данни, което е предназначено да замени Рамковото решение за защита на данните от 2008 г. (бивш трети стълб).

На 12 март 2014 г. Европейският парламент прие позицията си относно предложението за общ регламент относно защитата на данните и предложението за директива (док. 7427/14).

На 15 юни 2015 г. Съветът постигна съгласие по общ подход, като по този начин предостави на председателството мандат за водене на преговори, за да встъпи в тристранни разговори с Европейския парламент (док. 9565/15).

Европейският парламент и Съветът, на равнището на Комисията по граждански свободи, правосъдие и вътрешни работи и Комитета на постоянните представители, потвърдиха съответно на 17 и 18 декември 2015 г. съгласието си по компромисния текст, изготвен в резултат на тристранните преговори.

На заседанието си от 12 февруари 2016 г. Съветът постигна политическо споразумение по проекта за регламент (док. 5455/15). На заседанието си от 21 април 2016 г. Съветът прие позицията си, която е изцяло в съответствие с компромисния текст на регламента, договорен по време на неформалните преговори между Съвета и Европейския парламент.

Европейският икономически и социален комитет даде становище по регламента през 2012 г. (док. 12388/12).

Европейският надзорен орган по защита на данните беше консултиран и даде първо становище през 2012 г. (ОВ С 192, 30.6.2012 г., стр. 7) и второ становище през 2015 г. (ОВ С 301, 12.9.2015 г., стр. 1-8).

Агенцията за основните права даде становището си на 1 октомври 2012 г.

II. ЦЕЛ

В общия регламент относно защитата на данните се хармонизират правилата за защита на данните в Европейския съюз. Целите на регламента са да се укрепят

правата на физическите лица в областта на защитата на данните, да се улесни свободното движение на лични данни на единния пазар и да се намали административната тежест.

III. ПРАВЕН АНАЛИЗ

A. Общи бележки

В контекста на целта на Европейския съвет за постигане на споразумение относно реформата в областта на защитата на данните до края на 2015 г., Европейският парламент и Съветът проведоха неофициални преговори за сближаване на позициите си. Текстът отразява компромиса, постигнат между двамата съзаконотатели със съдействието на Европейската комисия.

Запазват се целите на Директива 95/46/ЕО: защита на правата на защита на данните и свободното движение на данните. Същевременно тя се стреми да адаптира действащите правила за защита на данните в светлината на нарастващия обем на обработваните лични данни в резултат на технологичните промени и глобализацията. С оглед на това регламентът да бъде адекватен спрямо бъдещето, правилата за защита на данните са технологично неутрални.

За да се гарантира съгласувано ниво на защита на физическите лица в целия Съюз и за да се предотвратят различията, възпрепятстващи свободното движение на лични данни в рамките на вътрешния пазар, до голяма степен се предвижда единен набор от правила, които са пряко приложими на територията на целия Съюз. Това хармонизиране ще сложи край на фрагментарността, произтичаща от различните закони на държавите членки, прилагащи Директива 95/46. Все пак, за да се вземат под внимание изискванията, свързани с особени ситуации на обработване на данни, включително за публичния сектор, се дава възможност на държавите членки да уточнят допълнително как ще прилагат в националното си право предвидените в регламента правила за защита на данните.

Защитата на личните данни е основно право, заложено в член 8, параграф 1 от Хартата на основните права на Европейския съюз. Член 16 от Договора за функционирането на Европейския съюз постановява, че всеки има право на защита на личните си данни, независимо от националността или местопребиваването си, и че за тази цел и за целта на свободното движение на лични данни следва да се определят правила. Въз основа на това се определят принципите и правилата относно защитата на физическите лица по отношение на обработването на техните лични данни.

За да се постигнат целите на регламента, се предвиждат по-строги изисквания за отчетност на администраторите (отговарящи за определянето на целите и средствата за обработването на личните данни) и обработващите данните (отговарящи за обработването на личните данни от името на администраторите), което създава истинска култура на защита на данните. В този контекст в целия регламент се въвежда основан на риска подход, който дава възможност за адаптиране на задълженията на администратора и обработващия данни в зависимост от риска, свързан с извършването от тях обработване на данни. Наред с това, за спазването на правилата за защита на данните допринасят кодекси за поведение и механизми за сертифициране. Този подход предотвратява въвеждането на прекалено ограничителни правила и намалява административната тежест, без това да засяга съответствието. Нещо повече, възпиращият характер на

потенциалните санкции, които могат да бъдат наложени, създава стимули за администраторите да спазват регламента.

Наред с това новите правила за защита на данните, водят и до засилени и приложими права за гражданите. Това дава възможност на физическите лица да упражняват по-добър контрол върху личните си данни, което води до по-голямо доверие в онлайн услугите в трансграничен мащаб, което пък ще активизира цифровия единен пазар. За децата следва да се осигури специална защита, тъй като може те да са по-слабо осведомени за рисковете, свързани с обработването на лични данни, както и за правата си.

Освен това, се укрепва независимостта на надзорните органи, като същевременно се хармонизират техните задачи и правомощия. Правилата за сътрудничество между надзорните органи и когато е подходящо, Комисията при трансгранични случаи (механизъм за съгласуваност) ще допринесат за последователното прилагане на регламента в целия Европейски съюз. Това ще предостави по-голяма правна сигурност и ще намали административната тежест. Наред с това механизмът за обслужване на едно гише ще доведе до наличието на един-единствен партньор за администраторите и обработващите лични данни във водените от тях трансгранични производства, включително обвързващи решения по спорове, постановени от новосъздадения Европейски комитет по защита на данните. Благодарение на този механизъм регламентът ще се прилага по-съгласувано. Наред с това той ще предостави по-голяма правна сигурност и ще намали административната тежест.

Установява всеобхватна рамка за предаване на лични данни от Европейския съюз на получатели в трети държави или в международни организации, с което предоставя нови инструменти в сравнение с Директива 95/46/ЕО.

Б. Ключови въпроси

Съветът и Европейският парламент, със съдействието на Европейската комисия, съгласуваха чрез неформални преговори позициите си, определени съответно в общия подход на Съвета и в позицията на Европейския парламент. Позицията на Съвета по общия регламент относно защитата на данните изцяло отразява постигнатия компромис. Основните елементи на са изложени по-долу.

1. Обхват

1.1. Материален обхват на регламента и разграничаване с директивата в областта на правоприлагането

Общият регламент относно защитата на данните се прилага за обработването на лични данни, извършвано изцяло или частично с автоматизирани средства, както и за обработването с други средства на лични данни, които са част от структуриран набор от лични данни, достъпни съгласно определени критерии, или които са предназначени да съставляват част от такъв структуриран набор. Материалният обхват на общия регламент относно защитата на данните и обхватът на Директивата за защита на данните в областта на правоприлагането са взаимно изключващи се. В регламента е посочено, че той не се прилага по отношение на обработването на лични данни от компетентните органи за цели на предотвратяването, разследването, разкриването или наказателното преследване на престъпления, изпълнението на наказателни санкции, включително предпазването от и предотвратяването на заплахи за обществената сигурност. Това ограничение дава възможност на правоприлагащите органи, и по-специално на полицията, принципно да прилагат

предвидения в директивата режим на защита на данните, като същевременно гарантира съгласувана защита на високо равнище на личните данни на физическите лица — обект на операции по правоприлагане.

1.2. Институции и органи на ЕС

За да се осигури единна и съгласувана защита на субектите на данни по отношение на обработването на техните лични данни, се посочва, че необходимите изменения на Регламент (ЕО) № 45/2001, който се прилага за институциите, органите, службите и агенциите на ЕС, следва да се осъществят след приемането на общия регламент относно защитата на данните, за да може той да е приложим едновременно с общия регламент относно защитата на данните.

1.3. Изключение във връзка с домашни дейности

За да се избегне установяването на нормативна уредба, която ще създаде ненужна тежест за физическите лица, се предвижда, че регламентът не се прилага за обработването на лични данни от физическо лице в рамките на изцяло лични или домашни дейности, които следователно нямат връзка с професионална или търговска дейност.

1.4. Териториален обхват

Създава равни условия за администраторите и обработващите лични данни от гледна точка на териториалния обхват, като обхваща всички администратори и обработващи данни, независимо дали са установени в Съюза или не.

На първо място, в регламента се предвижда, че правилата за защита на данните се прилагат за обработването на лични данни в контекста на дейностите на администратор или обработващ лични данни на дадено място на установяване в Съюза, независимо дали обработването се извършва в Съюза или не. На второ място, за да се гарантира, че физическите лица не са лишени от защита на своите данни, регламентът се прилага за обработването на лични данни на субекти на данни, които са в рамките на Съюза, дори ако администраторът или обработващият лични данни не е установен в Съюза, но неговите дейности по обработване на данни са свързани с предлагането на стоки или услуги на такива субекти на данни в Съюза, както и с наблюдението на тяхното поведение, доколкото това поведение се проявява в рамките на Европейския съюз. Освен това определянето на обхвата по такъв начин увеличава правната сигурност за администраторите и субектите на данни (физическите лица, чиито лични данни се обработват).

Също така се гарантира, че субектите на данни и надзорните органи разполагат с точка за контакт в ЕС, в случай че администраторите или обработващите лични данни не са установени в Съюза, но попадат под обхвата на действие на регламента: те трябва писмено да определят представител в Съюза. С цел да се избегне ненужната административна тежест, това задължение не се прилага за обработването на данни, което е малко вероятно да доведе до риск за правата и свободите на физическите лица, и за обработването от публичен орган или структура на третата държава.

2. Принципи, свързани с обработването на лични данни

Принципите за защита на данните се прилагат за всяка информация, отнасяща се до физически лица, които са идентифицирани или могат да бъдат идентифицирани, включително информация, което не може повече да бъде свързвана с конкретен субект на данни, без да се използва допълнителна информация, доколкото тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се

гарантира невъзможността да се направи връзка с физическо лице, което е идентифицирано или което може да бъде идентифицирано (псевдонимизация). Спрямо Директива 95/46 регламентът до голяма степен осигурява приемственост по отношение на принципите, на които се основава обработването на лични данни. Същевременно принципът на „минимизиране на данните“ беше коригиран, за да се вземе под внимание цифровата реалност и с оглед на установяването на баланс между защитата на данните на физическите лица, от една страна, и възможностите за администраторите да обработват данни, от друга страна.

3. Законосъобразност на обработването

3.1. Условия за законосъобразност

С цел осигуряване на правна сигурност се основава на Директива 95/46, като посочва, че обработването на лични данни е законосъобразно само ако е изпълнено най-малко едно от следните условия:

- съгласие на субекта на данни за една или повече конкретни цели;
- договор;
- правно задължение;
- защита на жизненоважни интереси на субекта на данни или на друго физическо лице;
- задача, изпълнявана в обществен интерес или при упражняването на официалните правомощия, които са предоставени на администратора;
- законни интереси, преследвани от администратор или от трета страна.

Две от условията е необходимо да бъдат допълнително уточнени: съгласие и законен интерес, преследван от администратор или от трета страна.

3.1.1. Съгласие

За да позволи обработването на личните си данни, субектът на данни може да даде съгласието си за това чрез ясно утвърдително действие, с което да се изразява свободно дадено, конкретно, информирано и недвусмислено заявление за съгласието му свързаните с него лични данни да бъдат обработвани. Такова съгласие следва да обхваща всички дейности по обработване, извършвани за една и съща цел или цели. Когато обработването преследва повече цели, за всички тях трябва да бъде дадено съгласие. Освен това администраторът трябва да може да докаже, че субектът на данни е дал съгласието си за операцията по обработване. Поради това мълчанието, предварително отменатите полета или липсата на действие не представляват съгласие. Формулирането на понятието „съгласие“ осигурява приемственост спрямо достиженията на правото на ЕС по отношение на използването на това понятие въз основа на Директива 95/46/ЕО, като същевременно допринася за общото му разбиране и прилагане в целия Европейски съюз.

Наред с това, с оглед на защитата на правата за защита на данните на субекта на данни се уточнява, че ако той е дал съгласието си в контекста на писмена декларация, която се отнася и до други въпроси, никоя част от тази декларация, която представлява нарушение на регламента, не е обвързваща. Нещо повече, при преценката доколко съгласието е дадено свободно, трябва в най-голяма степен да се отчита дали, наред с другото, изпълнението на даден договор е обусловено от наличието на съгласие за обработване, което не е необходимо за изпълнението на договора.

Накрая, за да се даде възможност за дерогации от общата забрана за обработване на специални категории лични данни, се предвижда по-висок праг, отколкото

за други видове обработване, тъй като субектът на данни трябва да даде изричното си съгласие за обработването на такива чувствителни лични данни.

Що се отнася до децата, се предвижда специален режим на защита за даването на съгласие от деца във връзка с предлагането на услуги на информационното общество. Обработването на личните данни на дете под максималната възраст от 16 години е законосъобразно, ако може с достоверност да се провери, като се вземат предвид наличните технологии, че такова съгласие е дадено или разрешено от носещия родителска отговорност за детето. Държавите членки, които считат, че е по-уместно да се предвиди по-ниска възрастова граница, имат право да определят по-малка максимална възраст, при условие че тя не е под 13 години.

3.1.2. Законен интерес на администратора

Обработването на лични данни може да бъде законосъобразно ако е необходимо за целите на законните интереси, преследвани от администратор или от трета страна. Тези законни интереси обаче не са достатъчно основание за законосъобразно обработване, когато преимущество пред тях имат интересите или основните права и свободи на субекта на данни, които изискват защита на личните данни, по-специално когато субектът на данни е дете.

За установяването на законен интерес е необходима преценка, в т.ч. дали субектът на данни може по времето и в контекста на събирането на лични данни основателно да очаква, че може да се осъществи обработване за тази цел. Обработването на лични данни за целите на директния маркетинг може да се разглежда като осъществявано поради законен интерес. Като се има предвид, че е задължение на законодателя да уреди със закон правното основание за обработването на лични данни от публичните органи, това правно основание не се прилага спрямо обработването на лични данни от публичните органи при изпълнението на техните задачи.

3.2. Специфични правила на държавите членки, чрез които да се адаптира прилагането на регламента

Дава възможност на държавите членки да запазят или да въведат по-конкретни разпоредби, които адаптират прилагането на заложените в регламента правила, ако личните данни се обработват с цел спазване на правно задължение или ако обработването е необходимо за задача, изпълнявана в обществен интерес или при упражняването на официалните правомощия, предоставени на администратора. Наред с това са предвидени дерогации, специфични изисквания и други мерки относно специални операции по обработване, чрез които държавите членки съчетават правото на защита на личните данни с правото на свобода на изразяване и на информация, публичен достъп до официални документи, обработване на национални идентификационни номера, обработване в контекста на заетостта и обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели.

3.3. Допълнително обработване

Обработването за друга цел, освен тази, за която личните данни са били събрани първоначално, е законосъобразно само ако това допълнително обработване е съвместимо с целите, за които личните данните са били първоначално обработани. Когато обаче субектът на данни е дал съгласието си или когато обработването се основава на правото на Съюза или на държава членка, което представлява необходима и пропорционална мярка в едно демократично общество, за да се гарантират по-специално важни цели от широк обществен интерес, администраторът има

право да обработва допълнително личните данни, независимо от съвместимостта на целите. Предвидени са повече права на субекта на данни в случай на допълнително обработване, по-специално по отношение на правото на информация и правото на възражение срещу по-нататъшното обработване, когато това не е необходимо за изпълнението на задача, осъществявана от съображения от обществен интерес.

За да установи дали дадена цел на допълнително обработване е съвместима с целта, за която първоначално са събрани данните, администраторът трябва да отчете, наред с другото, всички връзки между първоначалните цели и целите на предвиденото допълнително обработване, в какъв контекст са събрани личните данни, по-специално основателните очаквания на субекта на данни въз основа на неговите взаимоотношения с администратора по отношение на по-нататъшно използване на личните данни, естеството им, последствията от предвиденото допълнително обработване на данни за субекта на данни и наличието на подходящи гаранции при операциите по първоначалното и предвиденото допълнително обработване.

3.4. Обработване на специални категории лични данни

На личните данни, които по своето естество са особено чувствителни, се полага специална защита, тъй като контекстът на тяхното обработване може да създаде значителни рискове за основните права и свободи на лицата. Поради тази причина принципно запазва подхода на Директива 95/46 за забрана на обработването на специални категории лични данни.

Чрез дерогация от това правило в някои изчерпателно изброени случаи обработването на чувствителни данни е разрешено, например когато субектът на данни е дал изрично съгласие, когато обработването е необходимо по съображения, свързани със значим обществен интерес или когато обработването е необходимо за други цели, наред с другото, в областта на здравеопазването.

И накрая, се предвижда, че държавите членки могат да въведат допълнителни условия, включително ограничения, във връзка с обработването на генетични данни, биометрични данни или данни за здравословното състояние. Въпреки това тези допълнителни условия не трябва да възпрепятстват свободното движение на данни в Съюза.

4. Допълнителни права на субектите на данни

4.1. Въведение

Оправомощава в още по-голяма степен субектите на данни, като им предоставя засилени права за защита на данните и въвежда задължения за администраторите. Сред правата на субектите на данни са правото на информация; на достъп до лични данни; на коригиране; на заличаване на личните данни, включително правото „да бъдеш забравен“; на ограничение на обработването; на преносимост на данните; на възражение, както и да не подлежат на решения, основани единствено на автоматизирано обработване, включително профилиране. Правата, които са претърпели важни промени в сравнение с Директива 95/46, са по-подробно обяснени по-долу.

Администраторите са задължени да улесняват упражняването на правата на субектите на данни и да обработват лични данни в съответствие с принципа на прозрачност, по-специално като предоставят информация за обработването на лични данни, което извършват.

Ако обработваните от администратора лични данни не му позволяват да идентифицира даден субект на данни, администраторът на данни не е задължен да се сдобие с допълнителна информация, за да идентифицира субекта на данни единствено с цел спазване на някоя от разпоредбите на настоящия регламент.

Независимо от тези права на субектите на данни и задължения на администраторите, запазва подхода на Директива 95/46, като дава възможност за ограничения на общите принципи и на правата на лицето, ако въпросните ограничения се основават на правото на Съюза или на държава членка. Тези ограничения трябва да зачитат същността на основните права и свободи и да са необходими и пропорционални в едно демократично общество с оглед на защитата на определени обществени интереси.

4.2. Прозрачност

В съответствие с принципа на прозрачност администраторите трябва да предоставят информация и съобщения, свързани с обработването на лични данни, в сбита, прозрачна, разбираема и лесно достъпна форма, като използват ясни и недвусмислени формулировки, по-специално при всяка информация, адресирана до дете. Информацията се предоставя писмено или по друг начин, а когато е целесъобразно в електронна форма.

Определят се още срокове за искания за информация, съобщения или други действия на администратора, които по принцип трябва да се извършват безплатно. Когато исканията от даден субект на данни обаче са очевидно неоснователни или прекомерни, по-специално поради своята повтораемост, администраторът може да начисли такса в разумен размер, като взема предвид административните разходи за предоставяне на информацията или съобщението или предприемане на исканото действие, или може да откаже да предприеме действия по искането. В тези случаи администраторът носи тежестта на доказване на очевидно неоснователния или прекомерен характер на искането.

4.3. Информация и съобщения, които трябва да бъдат предоставени от администратора

С цел постигане на баланс между предоставянето на достатъчно информация на субектите на данни относно обработването на личните им данни, от една страна, и избягването на обременителните задължения за предоставяне на информация от страна на администраторите, от друга страна, предвижда двуетапен подход, за да се гарантира, че субектите на данни са подходящо информирани както в случаите, когато личните данни са получени от субекта на данни, така и в случаите, когато те не са получени от него. Като първа стъпка, администраторът е длъжен в момента на получаване на личните данни да предостави на субекта на данни посочената в регламента информация. Като втора стъпка, администраторът трябва да предостави допълнителната информация, която е посочена в регламента и е необходима за осигуряване на добросъвестно и ефикасно обработване. Също така администраторите информират субектите на данни, когато възнамеряват да извършат допълнително обработване за цел, различна от целта, за която личните данни са събрани първоначално.

Администраторът не е длъжен да предоставя информацията, посочена в първата или втората стъпка, когато субектът на данни вече разполага с тази информация. Когато личните данни не са получени от субекта на данни, администраторът не дава никаква информация на субекта на данни, в случай че записването или разк-

риането на лични данни на други страни е изрично предвидено със закон или ако предоставянето на информация на субекта на данни се окаже невъзможно или изисква непропорционално големи усилия.

И накрая, администраторите са длъжни да съобщават за всяка корекция, заличаване или ограничаване на обработването на данни на всеки получател, на когото са били разкрити личните данни, освен ако това е невъзможно или изисква непропорционално големи усилия. Освен това администраторът трябва да информира субекта на данни относно тези получатели, ако субектът на данни поиска това.

4.4. Икони

Принципът на прозрачно обработване изисква субектът на данни да бъде информиран за осъществяването на обработването и за неговите цели. В този контекст предвижда, че предоставянето на информация на субекта на данни може да бъде придружено със стандартизирани икони. Администраторите могат да решават на доброволна основа дали използването на тези стандартизирани икони би било полезно за извършването от тях обработване на лични данни. Иконите следва да представят по лесно видим, разбираем и ясно четим начин смислен обзор на планираното обработване. Иконите трябва да се предоставят едновременно с информацията. Ако иконите се представят в електронен вид, те трябва да бъдат машинночетими. За да се допринесе за стандартизираното използване на икони в ЕС, регламентът дава правомощия на Комисията да приема делегирани актове за определяне на информацията, която следва да представят иконите, както и на процедурите за предоставянето на стандартизирани икони. Европейският комитет по защита на данните трябва да даде становище относно предложените от Комисията икони. Възможността за приемане на делегирани актове не възпрепятства Европейския комитет по защита на данните да издава насоки, становища и добри практики относно иконите.

4.5. Право на достъп

Субектът на данни има право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако такива лични данни се обработват, да получи достъп до посочената в регламента информация. Във връзка с това в регламента се посочва, че администраторът трябва безплатно да предостави копие от личните данни, които се обработват. За допълнителни копия, поискани от субекта на данни, администраторът може да наложи разумна такса въз основа на административните разходи. Правото на получаване на копие не влияе неблагоприятно върху правата и свободите на други лица.

4.6. Право на заличаване (право „да бъдеш забравен“)

Дава право на субектите на данни свързаните с тях лични данни да бъдат заличени, когато обработването на тези данни не е в съответствие с настоящия регламент или с правото на Съюза или на държава членка, което се прилага спрямо администратора.

„Правото да бъдеш забравен“ се споменава с оглед на необходимостта от адаптиране на правото на заличаване, по-специално в контекста на цифровизацията. Администратори, които са оповестили публично лични данни, които субектът на данни желае да бъдат забравени, е длъжен да предприеме разумни мерки, включително от технически характер, за да информира администраторите, които обработват личните данни за искането на субекта на данни за заличаване на връзките към такива данни или на копията или репликите на тези данни, като се вземат предвид

наличните технологии и разходите за прилагане. Европейският комитет по защита на данните може да издава насоки, препоръки и добри практики относно процедурите за заличаването на връзки, копия или реплики на личните данни от обществено достъпни съобщителни услуги.

Правото на заличаване и задължението на администратора да информира другите администратори за искането за заличаване не се прилага, доколкото обработването на лични данни е необходимо за целите, които са изчерпателно изброени в регламента, като правото на свобода на изразяване и на информация.

4.7. Право на преносимост на данните

Посочва се, че когато обработването на личните данни се извършва с автоматизирани средства, субектите на данни имат право да получат отнасящите се до тях лични данни, които са предоставили на администратора, в структуриран, широко използван, оперативен съвместим и машинночитем формат, и да ги предадат на друг администратор. Освен това следва да се уточни, че когато това е технически осъществимо, субектите на данни имат право личните им данни да бъдат предавани пряко от един администратор на друг. Това допълнително засилва контрола на субектите на данни върху техните данни. Освен това по този начин се насърчава конкуренцията между администраторите.

Правото на преносимост на данните обаче не се отнася до обработването, необходимо за задача, изпълнявана в обществен интерес или при упражняването на официалните правомощия, които са предоставени на администратора. Освен това когато в определен набор от лични данни участва повече от един субект на данни, правото на субекта на данни да получи личните данни не засяга правата и свободите на останалите.

4.8. Право на възражение

В случаите, когато личните данни биха могли да се обработват законно, тъй като обработването е необходимо за задача, изпълнявана в обществен интерес или при упражняването на официално правомощие, предоставено на администратора, или по съображения, свързани със законните интереси на администратора или на трета страна, субектът на данни има право на възражение срещу обработването на лични данни, свързани с неговото конкретно положение. В този случай администраторът вече няма право да обработва личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

В този контекст следва да се уточни, че когато се обработват лични данни за целите на директния маркетинг, субектът на данни има право по всяко време на възражение срещу обработването на отнасящите се до него лични данни. Това включва профилиране, доколкото то е свързано с такъв директен маркетинг. „Профилиране“ означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използване на тези данни за оценяване на някои лични аспекти, свързани с дадено физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения, икономическото състояние, здравето, личните предпочитания, интересите, надеждността, поведението, местоположението или движението на това физическо лице. Когато субектът на данни възрази срещу обработването на данните за целите на директния маркетинг, обработването на личните данни за тези цели вече не е поз-

волено. Нещо повече, това право трябва да бъде изрично и ясно представено на вниманието на субекта на данни най-късно при осъществяване на първия контакт на администратора на лични данни със субекта на данни.

Освен това се споменава онлайн функцията „не ме проследявай“, като се уточнява, че в контекста на използването на услугите на информационното общество субектът на данни може да упражнява правото си на възразение чрез автоматизирани средства посредством използване на тези технически спецификации.

4.9. Автоматизирано вземане на индивидуални решения, включително профилиране

Субектът на данни има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, което оценява свързани с него лични аспекти и поражда правни последици за него или по подобен начин го засяга в значителна степен. Примери за това са автоматичен отказ на онлайн искания за кредит или практики за електронно набиране на персонал без човешка намеса. Това автоматизирано обработване на данни може да включва профилиране. Правото да не бъде обект на такова автоматизирано обработване обаче не се прилага, когато то е необходимо за:

- сключването или изпълнението на договор между субекта на данни и администратора;

- когато е разрешено от правото на Съюза или на държава членка, което се прилага спрямо администратора и в което се предвиждат също подходящи мерки за защита на правата и свободите и законните интереси на субекта на данни, като наблюдението на измамите и на укриването на данъци; или

- когато се основава на изричното съгласие на субекта на данни.

- Освен във втория случай, отнасящ се до обработка, разрешена съгласно правото на Съюза или на държава членка, администраторът, който извършва обработването с автоматизирани средства, трябва да осигури подходящи гаранции по отношение на правата и свободите на субектите на данни, както и на законните им интереси. Тези гаранции трябва да включват най-малко правото на получаване на човешка намеса от страна на администратора и възможността субектът на данни да изрази гледната си точка и да оспори решението. Освен това, за да се гарантира добросъвестно и прозрачно обработване, администраторите следва да използват подходящи математически и статистически процедури за профилирането и мерки, които да сведат до минимум потенциалните рискове за интересите на субектите на данни.

Субектът на данни разполага с допълнителни права, тъй като администраторът е длъжен да му предостави, когато е необходимо, за да се гарантира добросъвестно и прозрачно обработване, информация за наличието на автоматизирано вземане на решения, включително профилиране, и поне в тези случаи съдържателна информация относно приложената логика, както и значението и очакваните последици от това обработване за субекта на данни.

И накрая, автоматизираното вземане на решения и профилирането на базата на специални категории лични данни се разрешава само при специфични условия, включително правото на субекта на данни на възразение срещу такова обработване, когато тези лични данни се обработват за научни и исторически изследвания или за статистически цели, освен ако обработването е необходимо за изпълнението на задача, която се осъществява в обществен интерес.

Европейският комитет по защита на данните може да издава насоки, препоръки и добри практики с цел по-подробно уточняване на критериите и условията за решенията, основани на профилиране.

5. Администратор и обработващ лични данни

5.1. Въведение

Определя правната рамка за отговорностите и задълженията във връзка с всяко обработване на лични данни, извършено от администратор или от негово име от обработващ лични данни. В съответствие с принципа за отчетност администраторът е длъжен да прилага подходящи технически и организационни мерки и да бъде в състояние да докаже, че извършваните от него операции по обработване са в съответствие с регламента. В този контекст регламентът определя правила относно отговорностите на администратора във връзка с оценките на въздействието, воденето на документация за обработването, нарушенията на сигурността на данните, определянето на длъжностно лице по защита на данните и кодексите за поведение и механизмите за сертифициране.

5.2. Оценки на въздействието

Администраторът отговаря за извършването на оценка на въздействието върху защитата на данните, за да прецени дали има вероятност обработването да доведе до висок риск за правата и свободите на лицата. Определят се случаите, когато се изисква по-конкретно оценка на въздействието върху защитата на данните, например за някои специфични мащабни операции по обработване. Когато в такава оценка на въздействието е указано, че операциите по обработването водят до висок риск, който администраторът не може да ограничи с подходящи мерки от гледна точка на наличните технологии и разходите за прилагане, преди обработването трябва да се осъществи консултация с надзорния орган. След това надзорният орган може да даде съвети на администратора и използва правомощията си.

Европейският комитет по защита на данните може да издава насоки относно операции по обработване, които е вероятно да доведат до висок риск за правата и свободите на физическите лица, и да дава указания какви мерки могат да бъдат достатъчни в такива случаи за преодоляването на потенциален риск.

5.3. Регистри на дейности по обработване на данни

С цел да се даде възможност за последващ контрол от страна на надзорния орган, администраторът или, ако има такъв, представителят на администратора, или обработващият лични данни трябва да водят документация за дейностите по обработване, за които отговарят, включително относно нарушенията на сигурността на личните данни. С оглед намаляване на административната тежест, задължението за регистриране не се прилага за предприятия или организации с по-малко от 250 служители, освен ако съществува вероятност извършването от тях обработване да доведе до риск за правата и свободите на субектите на данни, ако обработването не е спорадично или включва чувствителни данни или данни, свързани с наказателни присъди и престъпления.

5.4. Нарушения на сигурността на данните

Нарушаването на сигурността на личните данни може да доведе до физически, материални или нематериални вреди за физическите лица, като загуба на контрол върху личните им данни или ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизацията, накръняване на репутацията, нарушаване

на поверителността на данни, защитени от професионална тайна, или някакви други икономически или социални неблагоприятни последици за засегнатите лица. Администраторите трябва да уведомяват надзорните органи за нарушения на сигурността на данните, освен ако няма вероятност нарушението на сигурността на данните да доведе до риск за правата и свободите на лицата. Освен това те са длъжни да информират съответните субекти на данни относно нарушения, които могат да представляват висок риск. Уведомяването на надзорните органи ще им даде възможност за намеса, ако такава е необходима. Нещо повече, информирането на съответните субекти на данни ще им даде възможност да вземат предпазни мерки.

С цел да се намали административната тежест, се прилагат различни прагове за уведомяване на надзорния орган и за информиране на съответните субекти на данните, като прагове за информиране са по-високи от тези за уведомяване. Администраторите са задължени, веднага след като установят нарушение на сигурността на лични данни, да уведомят компетентния надзорен орган без ненужно забавяне и, когато е осъществимо, не по-късно от 72 часа след установяване на нарушението. Независимо от това администраторите могат да не пристъпят към уведомяване ако са в състояние да докажат, че не съществува вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на лицата. Освен в някои изключения, администраторите са задължени без ненужно забавяне да съобщят на съответните субекти на данни за нарушението на сигурността на личните данни, когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на тези субекти на данните.

Европейският комитет по защита на данните може да дава насоки, препоръки и добри практики за установяване на нарушения на сигурността на данните и определянето на понятието за ненужно забавяне, след като администраторът е узнал за нарушението, за конкретните обстоятелства, при които се изисква администраторът да уведомява за нарушение на сигурността на личните данни, както и за обстоятелствата, при които дадено нарушение на сигурността на личните данни има вероятност да породи висок риск за правата и свободите на съответните лица.

5.5. Длъжностно лице по защита на данните

Целта на определянето на длъжностно лице по защита на данните е да се подобри спазването на регламента. Следователно длъжностното лице по защита на данните трябва да бъде лице с експертни познания в правото и практиките в областта на защитата на данните и трябва да подпомага администратора или обработващия лични данни да наблюдават вътрешното съответствие с настоящия регламент. Длъжностното лице по защита на данните може да бъде член на персонала на администратора или на обработващия лични данни или да изпълнява задачите въз основа на договор за услуги. Предвидена е възможност за определяне на едно длъжностно лице по защита на данните за група от предприятия или когато администраторът или обработващият данни е публичен орган. Предвижда се задължение за определяне на длъжностно лице защита на данните, когато:

- обработването се извършва от публичен орган, освен когато става въпрос за съдилища или независими съдебни органи, изпълняващи съдебните си функции;
- основните дейности на администратора или обработващия лични данни се състоят в операции по обработване, които поради своето естество, обхват и/или

цели изискват редовно и систематично мащабно наблюдение на субектите на данни; или

— основните дейности на администратора или обработващия лични данни се състоят в мащабно обработване на чувствителни данни и на данни, свързани с наказателни присъди и престъпления.

5.6. Кодекси за поведение и механизми за сертифициране

Съдържат се стимули за прилагането на кодекси за поведение и насърчава по-широкото използване на механизми за сертифициране за защита на данните и печати и маркировки за защита на данните. Тези инициативи допринасят за спазването на правилата за защита на данните и същевременно избягват задаването на прекалено ограничителни правила и водят до намаляване на разходите за публичните органи, отговарящи за прилагането. Освен това кодексите за поведение могат да бъдат съобразени със специфичните характеристики на обработването, което се извършва в определени сектори, както и с потребностите на микропредприятията и на малките и средните предприятия. Механизмите за сертифициране, както и печатите и маркировките за защита на данните, от своя страна допринасят за спазването на регламента, тъй като субектите на данни могат лесно да оценяват нивото на защита на данните на съответните продукти и услуги.

Включеният сложен набор от правила по отношение на кодексите за поведение и механизмите за сертифициране, печатите и маркировките за защита на данните, дават възможност за частна инициатива, като същевременно се защитават стандартите за защита на данните чрез участието на надзорните органи.

5.6.1. Кодекси за поведение

Надзорният орган може да одобрява кодекси за поведение, техни изменения или допълнения. Когато проектът на кодекс за поведение е свързан с дейности по обработване в няколко държави членки, компетентният надзорен орган трябва преди одобряването да представи проект на изменения или допълнен кодекс на Европейският комитет по защита на данните за становище.

Комисията може да приема актове за изпълнение, за да реши дали новите кодекси за поведение и измененията или допълненията към съществуващи кодекси за поведение, одобрени от компетентния надзорен орган, са общовалидни в рамките на Съюза.

Европейският комитет по защита на данните следва да насърчава изготвянето на кодекси за поведение. Освен това той трябва да събира всички одобрени кодекси за поведение и измененията към тях в регистър и да ги прави обществено достъпни чрез всички подходящи средства.

5.6.2. Механизми за сертифициране и печати и маркировки за защита на данните

Посочва се, че всяка държава членка трябва да предвиди дали сертифициращите органи се акредитират от надзорния орган или от националния орган по акредитация. Акредитираните органи за сертификация могат да сертифицират администраторите и обработващите лични данни въз основа на критериите, одобрени от компетентния надзорен орган или — в съответствие с механизма за съгласуваност — от Европейския комитет по защита на данните. В последния случай, критериите, одобрени от Европейския комитет по защита на данните, могат да доведат до единно сертифициране — „Европейски печат за защита на данните“. Сертификатите се издават на администраторите и обработващите лични данни за срок, не по-

дълъг от 3 години, с възможност за удължаване. Сертифициращият орган трябва да предостави на надзорния орган мотивите за издаване или отнемане на искания сертификат. Впоследствие надзорният орган може да отхвърли въпросния сертификат или да го обяви за невалиден.

Комисията е компетентна да приема делегирани актове за прецизиране на изискванията, които трябва да се отчитат по отношение на механизмите за сертифициране за защита на данните. Европейският комитет по защита на данните трябва да даде становище относно тези изисквания. Комисията може да приема и актове за изпълнение относно техническите стандарти за механизмите за сертифициране и за печатите и маркировките за защита на данните, както и за механизми за насърчаване и признаване на механизмите за сертифициране и на печатите и маркировките за защита на данните.

Европейският комитет по защита на данните следва още да насърчава създаването на механизми за сертифициране за защита на данните и на печати и маркировки за защита на данните.

6. Предаване на лични данни на трети държави или международни организации

6.1. Въведение

Трансграничните потоци от лични данни към и от държави извън Съюза и международни организации са от решаващо значение в контекста на глобалната търговия и трансграничната цифрова икономика. Нивото на защита, гарантирано от Съюза, не трябва да бъде засегнато, ако личните данни на гражданите на ЕС се предават извън Съюза. Като общо правило всяко предаване на лични данни на трета държава или международна организация може да се осъществява само ако администраторите и обработващите лични данни спазват разпоредбите на регламента. Съобразена е изцяло със съдебната практика на Съда на Европейския съюз, в т.ч. неговото решение от 6 октомври 2015 г. по дело C-362/14. Запазени са различни начини за разрешаване на трансгранично предаване на лични данни, като същевременно се засилват гаранциите, че правата на защита на данните се спазват. Тези различни начини за предаване на данни са решенията относно адекватността, подходящите гаранции и дерогациите.

Всяко решение на съд или трибунал и решение на административен орган на трета държава, което изисква администратор или обработващ лични данни да предаде или разкрие лични данни, може да бъде признато или изпълнено по какъвто и да е начин само ако се основава на международно споразумение, което е в сила между молещата трета държава и Съюза или държава членка. Нещо повече, изрично се посочва, че такива международни споразумения не засягат други предвидени в регламента основания за трансгранично предаване.

6.2. Решения относно адекватността

Предаването на данни в международен мащаб може да се осъществява въз основа на решение на Комисията относно адекватността, съгласно което въпросната трета държава, или територия или един или повече конкретни сектори в рамките на тази трета държава, или въпросната международна организация гарантират ниво на защита, което по своята същност е равностойно на гарантираното в рамките на Съюза. По този начин се осигуряват правна сигурност и еднообразно прилагане навсякъде в Съюза.

Комисията може да реши да отмени решение относно адекватността, след като е отправила предизвестие и е предоставила пълна обосновка на третата държава или международно организация. Комисията приема решения относно адекватността и решения за оттегляне на такива решения под формата на актове за изпълнение. Актовете за изпълнение трябва да предвиждат механизъм за периодичен преглед най-малко на всеки четири години. Комисията трябва да следи събитията в трети държави и международни организации, които могат да имат отражение върху функционирането на решенията относно адекватността. За целите на наблюдението и извършването на периодичните прегледи Комисията следва да вземе предвид становищата и констатациите на Европейския парламент и Съвета, както и на други релевантни органи и източници. В рамките на оценката и прегледа на регламента Комисията трябва също периодично да докладва на Съвета и на Европейския парламент. Накрая, Европейският комитет по защита на данните трябва да предоставя на Комисията становище за оценка на адекватността на нивото на защита в трета държава или международна организация, включително за оценка на това дали повече не може да бъде гарантирано адекватно ниво на защита.

Решенията, приети от Комисията въз основа на член 25, параграф 6 от Директива 95/46/ЕО, остават в сила, докато не бъдат изменени, заменени или отменени от решение на Комисията. В същия дух, разрешенията, издадени от държава членка или надзорен орган въз основа на член 26, параграф 2 от Директива 95/46/ЕО, и решенията, приети от Комисията въз основа на член 26, параграф 4 от Директива 95/46/ЕО, остават валидни, докато не бъдат изменени, заменени или отменени, ако е необходимо, съответно от този надзорен орган или посредством решение на Комисията. Като гарантира приемственост, създава правна сигурност.

6.3. Подходящи гаранции

В допълнение към решенията относно адекватността, трансграничното предаване на данни може също да се извършва ако администраторът или обработващият лични данни са осигурили подходящи гаранции за компенсиране на липсата на защита на данните в третата държава или международната организация. Такива подходящи гаранции могат да се изразяват в приемането на правнообвързващи и подлежащи на изпълнение инструменти между публичните органи, задължителни фирмени правила, използването на стандартни клаузи за защита на данните, приети от Комисията, стандартни клаузи за защита на данните, приети от надзорен орган, или договорни клаузи, разрешени от надзорен орган. Администратори или обработващият лични данни в дадена трета държава също могат да осигурят подходящи гаранции за предаването на лични данни на трети държави или международни организации. Те могат да направят това чрез одобрен кодекс за поведение заедно с обвързващи и подлежащи на изпълнение ангажменти за прилагане на подходящи гаранции чрез договорен или друг правнообвързващ инструмент, включително що се отнася до правата на субектите на данни. Това може да се направи и посредством механизъм за сертифициране, одобрен от компетентния надзорен орган, заедно със задължителни и изпълними ангажменти на администратора или обработващия лични данни в третата държава да прилагат подходящите гаранции, включително по отношение на правата на субектите на данни.

6.4. Дерогации

При липсата на решение относно адекватността или на подходящи гаранции предаването или съвкупността от предавания на лични данни на трета държава или

международна организация могат да се извършат въз основа на дерогациите, които са упоменати в изчерпателния списък в регламента. Една от тези дерогации се отнася за законните интереси, преследвани от администратора, при положение че интересите или правата и свободите на субекта на данните нямат предимство пред тези интереси. С оглед на предоставянето на достатъчно гаранции при трансграничното предаване на лични данни, законните интереси на администратора са строго ограничени и позоваване на тях може да се прави само в краен случай (като „*ultimum remedium*“). С цел да се гарантира последователното прилагане на регламента, Европейският комитет по защита на данните трябва, по своя инициатива или по искане на Комисията, да изготвя и преразглежда насоки, препоръки и добри практики с цел допълнително уточняване на критериите и изискванията за предаването на данни при отсъствие на решение относно адекватността или на подходящи гаранции.

7. Надзорни органи

7.1. Независимост

Всяка държава членка трябва да предвиди един или повече независими публични органи да отговарят за наблюдението на прилагането на регламента на нейна територия, с цел да се защитят основните права и свободи на лицата във връзка с обработването на личните им данни и да се улесни свободното движение на личните данни в рамките на Съюза. Всеки надзорен орган и неговите членове трябва да действат при пълна независимост, включително с интегритет, при изпълнението на задачите и упражняването на правомощията, които са им възложени.

Всеки надзорен орган трябва да допринася за последователното прилагане на настоящия регламент в рамките на Съюза. За тази цел надзорните органи трябва да си сътрудничат помежду си, с Европейския комитет по защита на данните и с Комисията. Последователното прилагане на регламента се осигурява също чрез установяване на правомощията на надзорните органи и чрез определяне на задачите и на минималните правомощията за разследване и даване на разрешение и корективните и консултативни правомощия, които надзорните органи трябва да притежават

7.2. Професионална тайна

Регламентът определя правилата за професионална тайна на надзорните органи и на техните членове. На първо място, както по време на мандата си, така и след неговото приключване, членът или членовете и персоналът на всеки надзорен орган, в съответствие с правото на Съюза или на държава членка, трябва да бъдат обвързани от задължението за опазване на професионалната тайна по отношение на всяка поверителна информация, която е стигнала до тяхното знание при изпълнението на техните задачи или упражняването на техните правомощия. Уточнява се още, че по време на техния мандат това задължение за опазване на професионалната тайна се прилага по-специално по отношение на подаването на сигнали от физически лица за нарушения на регламента. Освен това Европейският комитет по защита на данните има за задача да издава насоки, препоръки и добри практики за установяване на общи процедури за докладване от страна на физическите лица за нарушения на регламента.

8. Сътрудничество и съгласуваност

8.1. Европейски комитет по защита на данните

С регламента се създава Европейски комитет по защита на данните, който е орган на Съюза, притежаващ юридическа правосубектност, с цел да се гарантира

правилното и съгласувано прилагане на регламента. Намесата на Комитета се изразява по-конкретно в предоставяне на становища, приемане на обвързващи решения в контекста на уреждане на спорове между надзорни органи или изготвяне на насоки по въпроси, отнасящи се до прилагането на регламента, за да се гарантира последователното му прилагане.

Европейският комитет по защита на данните е съставен от ръководителите на по един надзорен орган от всяка държава членка и Европейския надзорен орган по защита на данните, или от съответните им представители. Комисията има право да участва в дейностите и заседанията на Европейския комитет по защита на данните без право на глас. Обсъжданията на Европейския комитет по защита на данните са поверителни, когато Комитетът счита това за необходимо, както е посочено в процедурния му правилник.

В случай че Европейският комитет по защита на данните приема решение със задължителен характер във връзка с разрешаване на спорове, Европейският надзорен орган по защита на данните има право на глас само за решения, които засягат принципи и правила, приложими за институциите, органите, службите и агенциите на Съюза, които по същество съответстват на тези на регламента.

8.2. Механизъм за съгласуваност

В случаи на трансгранично обработване на лични данни с участието на повече от един надзорен орган, механизмът за съгласуваност гарантира, че се взема едноединствено решение, което ще бъде приложимо на цялата територия на Европейския съюз, като се взема под внимание становището на различните засегнати надзорни органи. Следователно механизмът за съгласуваност засилва „близостта“ между субектите на данни и надзорния орган, който взема решение, чрез привличане на „местните“ надзорни органи в процеса на вземане на решение. Нещо повече, при възникването на спорове между надзорните органи от различни държави членки, новосъздаденият Европейски комитет по защита на данните е компетентен да взема обвързващи решения.

Правилата на механизма за съгласуване не се прилагат, когато обработването се извършва от публични органи или от частни структури в обществен интерес. В такива случаи единственият надзорен орган, който е компетентен, е надзорният орган на държавата членка, в която е установен публичният орган или частната структура.

Предвижда се, че в контекста на оценката на регламента, която Комисията извършва, ще бъде разгледано прилагането на механизма за сътрудничество и съгласуваност.

9. Средства за правна защита, отговорност за причинени вреди и санкции

Предвижда се подробен набор от правила, който дава на субектите на данни няколко възможности за правна защита, включително предявяването на иск за обезщетение при причинени вреди в резултат на нарушение на регламента.

9.1. Право на подаване на жалба и право на съдебна защита

Всеки субект на данни има правото да подаде жалба пред надзорния орган, ако счита, че отнасящото се до него обработване на лични данни не спазва настоящия регламент. Нещо повече, всеки субект на данни има право на ефективни средства за съдебна защита срещу правнообвързващо решение на надзорен орган, което се отнася до него. Субектът на данни има също правото на ефективна съдебна защита,

в случаите когато надзорният орган не предприема действия във връзка с жалбата или не предоставя информация относно развитието по жалбата или резултата от нея.

Всеки субект на данни има също правото на ефективна съдебна защита, ако счита, че неговите права по този регламент са били нарушени в резултат на обработването на негови лични данни в нарушение на регламента.

Гарантирана е близостта между субекта на данни и националния съд, тъй като субектът на данни има право да поиска от националния съд преразглеждане на решението на неговия орган по защита на данните, независимо от това в коя държава членка е установен администраторът или обработващият лични данни. Производствата срещу даден администратор или обработващ лични данни трябва да се образуват пред съдилищата на държавата членка, в която администраторът или обработващият лични данни има място на установяване. Като алтернативен вариант такива производства могат да се образуват пред съдилищата на държавата членка, в която субектът на данните има обичайно местопребиваване, освен ако администраторът или обработващият лични данни е публичен орган на държава членка, действащ в изпълнение на публичните си правомощия.

Наред с това, всяко физическо или юридическо лице има правото да внася иск за отмяна на решения на Европейския комитет по защита на данните пред Съда на Европейския съюз при условията, предвидени в член 263 от ДФЕС.

9.2. Представителство на субектите на данни

Субектът на данни има право да възложи на органи, организации или сдружения, които отговарят на специфични критерии, като работещи с нестопанска цел или развиващи дейност в областта на защитата на данните, да подадат жалба от негово име, да упражнят правото на съдебна защита от негово име и да упражнят правото на обезщетение от негово име, ако това е предвидено в правото на държавата членка. Въпросните специфични критерии имат за цел да се избегне утвърждаването на култура на търговски искове в сферата на защитата на данните. В допълнение държавите членки могат да предвидят, че всеки такъв орган, организация или сдружение, независимо от възложения от субекта на данни мандат, има право да подаде в съответната държава членка жалба до компетентния надзорен орган и да упражни правото на съдебна защита, ако счита, че правата на субект на данни са били нарушени в резултат на обработване на лични данни, което не съответства на регламента.

9.3. Спиране на производство

С оглед да се избегне разглеждането от различни съдилища на един и същи въпрос във връзка с обработване от един и същ администратор или обработващ лични данни, всеки компетентен съд, освен първия сезиран съд, може да спре производството или, по молба на една от страните, да се откаже от компетентност.

9.4. Право на обезщетение и отговорност за причинени вреди

Всеки субект на данни, който е претърпял материални или нематериални вреди в резултат на нарушение на регламента, има право да получи обезщетение от администратора или обработващия лични данни. С цел на субектите на данни да се предостави възможност да предявяват иск за обезщетение в случай на вреди, а на администраторите и обработващите лични данни да се предостави правна сигурност, в регламента се определят техните отговорности за причинени вреди. Всеки администратор, който участва в обработването, носи отговорност за причинените

от него вреди. Обработващият лични данни носи отговорност само когато не е спазил задълженията по регламента, които са изрично насочени към обработващите лични данни, или е действал извън законосъобразните указания на администратора или в противоречие с тях. Независимо от това администраторът или обработващият лични данни се освобождава от отговорност, ако докаже, че по никакъв начин не е отговорен за събитието, причинило вредата.

Когато в една и съща операция по обработване участват повече от един администратор или обработващ лични данни или участват и администратор, и обработващ лични данни, и когато те са отговорни за някаква вреда във връзка с обработването, всеки администратор или обработващ лични данни носи отговорност за цялата вреда, за да се гарантира действително обезщетение на субекта на данни. Независимо от това, когато администратор или обработващ лични данни е изплатил пълното обезщетение за причинената вреда, той има право да поиска от другите администратори или обработващи лични данни, участвали в същата операция по обработване, да му възстановят част от платеното обезщетение, съответстваща на тяхната част от отговорността за причинената вреда.

9.5. Санкции

С цел да се гарантира спазването на регламента, се предвижда, че надзорните органи могат да налагат административни глоби. Тези глоби трябва да бъдат ефективни, пропорционални и възпиращи. Държавите членка могат да предвидят правила относно това дали и до каква степен могат да бъдат налагани административни глоби на публични органи и структури, установени в тази държава членка. Освен налагането на административни глоби надзорните органи могат да използват и други корективни правомощия, например предупреждения или порицания. С оглед повишаване на хармонизацията Европейският комитет по защита на данните трябва да изготви насоки за надзорните органи относно прилагането на корективните правомощия на надзорните органи и определянето на административни глоби.

Регламентът съдържа списък с критерии за надзорния орган при вземането на решение дали да наложи административна санкция и, ако да, какъв следва да бъде размерът на глобата. Тези критерии са свързани наред с другото с естеството, тежестта и продължителността на нарушението на регламента, както и с това дали то е било извършено умишлено или по небрежност. В регламента се изброяват както нарушенията, така и съответстващите им максимални административни глоби. В рамките на тези максимални административни глоби надзорният орган трябва да определи целесъобразен размер в зависимост от обстоятелствата по всяко отделно нарушение. С оглед на допълнителното предоставяне на правна сигурност за администраторите и обработващите лични данни, както и по-голямо хармонизиране на административните глоби в рамките на Съюза, като същевременно се запази известна свобода на преценка за надзорните органи, тези нарушения са разделени в три категории. Нарушенията в първата категория, които се отнасят до задълженията на администраторите и обработващите лични данни, подлежат на глоби в размер до 10 000 000 EUR или, ако става дума за предприятие — до 2% от общия му годишен оборот в целия свят за предходната финансова година, като се взема по-високата от двете суми. За втората категория нарушения, свързани с правата на субектите на данни и общите принципи, максималният размер е 20 000 000 EUR или 4% от оборота. Третата категория нарушения се отнася до неспазването на разпореждане

на надзорен орган и също се санкционира с максимален размер на глобата от 20 000 000 EUR или 4 % от оборота.

10. Специфични ситуации във връзка с обработването на данни

10.1. Обработване на лични данни и свобода на изразяване и информация

Държавите членки са длъжни да предвидят със закон съчетаването на правото на защита на личните данни с правото на свобода на изразяване и информация, включително обработването на лични данни за журналистически цели и за целите на академичното, художественото или литературното изразяване. С цел да се осигури прозрачност във връзка със съчетаването на тези права, всяка държава членка е длъжна да нотифицира Комисията за съответните разпоредби в своето право и за измененията на тези разпоредби, както и за съответни нови разпоредби.

10.2. Обработване в контекста на трудово правоотношение

Държавите членки могат със закон или с колективни споразумения да предвидят по-конкретни правила, за да гарантират защитата на правата и свободите по отношение на обработването на личните данни на наетите лица в контекста на трудово правоотношение.

Тези правила трябва да включват подходящи и конкретни мерки за защита на човешкото достойнство, законните интереси и основните права на субекта на данните. Всяка държава членка трябва да нотифицира Комисията за съответните разпоредби в своето право и за измененията на тези разпоредби, както и за съответни нови разпоредби.

10.3. Гаранции и дерогации за обработването на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели

Регламентът определя специфични правила за обработването на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели. Целта на тези правила е да бъдат съчетани от една страна интересът от наличието на лични данни за поддържане на архиви, предоставяне на статистически данни или провеждане на изследвания и от друга страна, правата за защита на данните.

Обработването за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели подлежи на подходящи гаранции за правата и свободите на субекта на данни. Тези гаранции предвиждат, че трябва да са налице технически и организационни мерки, по-специално с цел да се гарантира, че е спазен принципът за свеждане до минимум на данните в случай на обработка за тези конкретни цели. Мерките могат да включват псевдонимизация, доколкото посочените цели могат да бъдат постигнати по този начин. Когато тези цели могат да бъдат постигнати чрез по-нататъшно обработване на лични данни, което не позволява или повече не позволява идентифицирането на субектите на данни, целите трябва да бъдат постигнати по този начин. При задължение за изпълнение на тези гаранции и доколкото такива права има вероятност да направят невъзможно или сериозно да навредят на обработването за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, администраторите имат право да направят дерогации от някои права за защита на данните, съдържащи се в регламента, при условие че тези дерогации са необходими за изпълнението на конкретните цели. Тези дерогации са диференцирани в зависимост от целта на обработването. Независимо от дерогациите, които вече са

предвидени в регламента относно правото на информация и правото на заличаване, правото „да бъдеш забравен“, правото на Съюза или на държавите членки може да предвижда при определени условия и при спазване на съответните предпазни мерки дерогации от правото на достъп, правото на поправка, правото на ограничаване на обработването, задължението за уведомяване, правото на преносимост на данните и правото на възражение при обработването на лични данни за целите на архивирането в обществен интерес, както и дерогации от правото на достъп, правото на поправка, правото на ограничаване на обработването и правото на възражение при обработването на лични данни за научни или исторически изследвания или за статистически цели. Правото на Съюза или на държава членка следва да предвижда подходящи гаранции при такова обработване на лични данни.

Предвижда се и дерогация от забраната за обработване на чувствителни лични данни при обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели. Такава дерогация се позволява, когато въпросното обработване се основава на правото на Съюза или на държава членка, което трябва да е пропорционално на преследваната цел, да зачита същността на правото на защита на данните и да предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данни.

11. По-рано сключени споразумения

Международните споразумения, включващи предаване на лични данни на трети държави или международни организации, които са сключени от държавите членки преди влизането в сила на този регламент и са в съответствие с правото на Съюза, приложимо преди влизането в сила на регламента, остават в сила, докато не бъдат изменени, заменени или отменени. По този начин се гарантира правна сигурност за администраторите и се избягва ненужна административна тежест за държавите членки. В позицията се отчита също, че за изменянето на съществуващи споразумения, държавите членки са зависими от сътрудничеството на третата държава или международната организация.

IV. ЗАКЛЮЧЕНИЕ

Регламентът отразява компромиса, постигнат при неофициалните преговори между Съвета и Европейския парламент със съдействието на Комисията. Съветът приканва Европейския парламент официално да одобри позицията на Съвета без изменения, така че да може да бъде създадена новата законодателна рамка на ЕС за защита на данните, която ще укрепи правата за защита на данните, като същевременно ще улесни движението на лични данни на цифровия пазар.

ЛИТЕРАТУРА

1. Закон за защита на личните данни, ДВ. бр.1 от 4 януари 2002.
2. Регламент (ЕС) 2016/679, на Европейския парламент и Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на личните данни и относно свободното движение на такива данни и за отмяната на Директива 95/46/ЕО, Официален вестник на европейския съюз L119 от 4 май 2016.

АНАЛИЗ НА АРХИТЕКТУРИ ЗА ОБЛАЧНИ УСЛУГИ

Иван П. Иванов¹, Николай Т. Стоянов²

¹Р България, София 1592, бул. "Цв. Лазаров" № 2,
Институт по отбрана „Професор Цветан Лазаров”
Тел. +359 0221822, E-mail: i.p.ivanov@di.mod.bg

²Р България, София 1592, бул. "Цв. Лазаров" № 2,
Институт по отбрана „Професор Цветан Лазаров”
Тел. +359 0221827, E-mail: n.stoianov@di.mod.bg

ANALYSIS OF ARCHITECTURES FOR CLOUD SERVICES

Ivan P. Ivanov, Nikolai T. Stoianov

ABSTRACT: *The classic architecture of cloud computation is ubiquitous reality. The development of mobile computing and modern needs of service require search and analysis of new models of cloud computing. Of particular interest is finding suitable solutions for military operations. Based on the analysis of classical and specialized architectures is proposed hybrid model of cloud computing that takes into account the dynamics of the modern battlefield.*

KEY WORDS: *cloud computing, architectures.*

Въведение

През последните няколко години изчисленията в облака или облачните изчисления придобиха голяма популярност. Те се превърнаха от една изследователска област в реалност използвана от милиони потребители. Днес от тези подходи започват да се възползват и т.нар. Internet of Things (IoT). Достъпът до информация е възможен навсякъде, по всяко време и с различно устройство благодарение на концепцията и технологиите за облачни услуги или т.нар. “облаци”. Предимствата които предоставя облака са: ефективна цена, архивиране и възстановяване, лесен достъп до информация, бързо развърщане и стартиране на услуги, автоматична интеграция на различните софтуерни приложения и др., но също така има и няколко недостатъка: свързаност на потребители с облака и междублачна комуникация, въпросите за сигурността не са решени цялостно, ограничен контрол и намалена гъвкавост, зависимост от доставчика и увеличаване на уязвимостите. В същото време значителното развитието на мобилните компютри създава условия за цял нов свят, в който тези устройства безпроблемно увеличават познавателните способности на потребителите на основата на интензивни изчисления като: разпознаване на глас, обработка на говор, компютърно зрение, машинно обучение, добавена реалност, планиране и подпомагане вземането на решение и др. 9. Всичко това налага развитие и анализ на архитектурите за облачни услуги.

I. Облачни услуги – основни елементи

Съгласно препоръка SP800-145 на Националния институт по стандартизация и технологии (NIST) на САЩ, облачните услуги (cloud computing) или облака за краткост е “модел за осигуряване на повсеместен, удобен и при поискване мрежови достъп до общ набор от конфигурируеми изчислителни ресурси (например мрежи, сървъри, масиви за съхранение, приложения и услуги), които могат да бъдат бързо предоставени за ползване и освободени с минимални усилия по управлението или взаимодействието с доставчик на услуги” 11. Определението на NIST характеризира важни аспекти на облака и е предназначено да служи като средство за сравнения на облачните услуги и стратегиите по внедряването, както и да се осигури основа за обсъждане на широк кръг от въпроси - от това какво е облачни изчисления, до това как най-добре да се използва облака. Дефинираните модели на услугите и внедряването(развързването) образуват проста таксономия, която не е предназначена да предписва или ограничава всеки конкретен метод на внедряване, предоставяне на услуги или бизнес дейност.

Предложеният в 11 възглед се състои от пет съществени характеристики, три модела на услугите и четири модела за внедряване (развързване). Визуално това определение е представено на фиг. 1.



Фиг. 1. Обобщен модел на облачните изчисления.

Облачните изчисления се характеризират с пет **съществени характеристики**:

1. **Самообслужване при поискване.** Потребителите могат едностранно да изискват предоставяне на изчислителни възможности, като например сървърно време или мрежово хранилище, при възникнала необходимост автоматично, без нужда от човешкото взаимодействие с всеки доставчик на услуга.

2. **Широк (набор за) достъп до мрежата.** Способностите са налични в мрежата и достъпни чрез стандартни механизми, които насърчават използването от разнородни стандартни или тънка клиентски платформи (например, мобилни телефони, таблети, лаптопи и работни станции).

3. **Избираем набор от ресурси.** Изчислителните ресурси на доставчика са събрани в набор и по начин да обслужва множество потребители, използвайки модела на мулти-наемател, с различни физически и виртуални ресурси динамично назначени и преназначени според потребителското търсене. Съществува чувство за

независимост от местоположението в това, че клиентът обикновено няма контрол или познания върху точното местоположение на предоставяните ресурси, но може да бъде в състояние да определи местоположението на по-високо ниво на абстракция (например, страна, състояние, или центровете за данни). Примери за ресурси включват съхраняване, обработка, памет и мрежови трафик.

4. **Бърза еластичност.** Ресурсите могат да бъде еластично осигурени и освободени и автоматично мащабирани, в съответствието с потребността. От гледна точка на потребителя, ресурсите са на разположение за предоставяне, като често изглежда, че са неограничени и могат да бъдат придобити във всякакви количества и по всяко време.

5. **Измеримост на услугата.** Облачните системи автоматично контролират и оптимизират използването на ресурсите, чрез измервания на приложено ниво на абстракция, подходящо за конкретната услуга (напр. съхранение, обработка, честотна лента и активни потребителски акаунти). Използване на ресурсите може да се наблюдава, контролира и докладва, осигуряващо прозрачност както за доставчика, така и за потребителя на използваната услуга.

Облачните изчисления предлагат три **модела на услугите**:

1. **Софтуер като услуга (SaaS).** Тази услуга предоставя способност на потребителя да използва приложения на доставчика, работещи на облачната инфраструктура чрез различни клиентски устройства(програми) - от тънки клиенти като например уеб браузър (например уеб-базирана поща) до програмни интерфейси. Потребителят не управлява или контролира използваната облачна инфраструктура - мрежа, сървъри, операционни системи, съхранение и др.

2. **Платформата като услуга (PaaS).** Тази услуга предоставя способност на потребителя да разположи върху облачната инфраструктура приложения, създадени с помощта на езиците за програмиране, библиотеки, услуги и инструменти, осигурени от доставчика. Потребителят не управлява или контролира основната облачна инфраструктура, включително мрежа, сървъри, операционни системи или устройства за съхранение, но има контрол върху приложенията и евентуално конфигурационни настройки за обкръжението на хоста.

3. **Инфраструктура като услуга (IaaS).** Тази услуга предоставя способност на потребителя да използва изчислителни ресурси, дискови усторойсва за съхранение, мрежи и други основни компютърни ресурси, на които потребителят е в състояние да разположи и стартира произволен софтуер - операционни системи и приложения. Потребителят не управлява или контролира базовата облачна инфраструктура, но има контрол върху операционни системи, устройства за съхранение и приложения и евентуално ограничен контрол на избрани мрежови компоненти (например защитната стена на хоста).

Облакът предлага четири основни **модела за внедряване** (развърщане):

1. **Частен облак.** Инфраструктурата на облак е предвидена за използване само от една организация, включваща множество потребители (например бизнес единици). Тя може да бъде притежавана, управлявана и поддържана от организацията, от трета страна или някаква друга комбинация и да е разположена както вътре, така и извън сградата на бизнес организацията.

2. **Облак на общност.** Инфраструктурата на облак е предвидена за използване само от специфична общност на потребители от различни организации, които споделят общо начинание (мисия, изисквания за сигурност, политика за съот-

ветствие и др.). Инфраструктурата може да бъде притежавана, управлявана и поддържана от един или повече от организациите в общността, от трета страна, или някаква друга комбинация и да бъде разположена както вътре, така и извън сградите на организациите.

3. Публичен облак. Инфраструктурата на облак е предвидена за ползване от широката общественост. Тя може да бъде притежавана, управлявана и експлоатирана от бизнес, академична или държавна организация, или някаква комбинация от тях. Разположена е в помещенията на доставчика на облака.

4. Хибриден облак. Инфраструктурата на облака е композиция от две или повече различни облачни инфраструктури (частен, общностен или публичен), които остават уникални образувания, но са свързани помежду си чрез стандартизирана или патентована технология, която позволява на преносимост на данните и приложенията (например поточен облак за балансиране на натоварването между облаци).

II. Някои ограничения и предизвикателства пред облачните изчисления

В сравнение с предишните традиционните изчислителни подходи, изчислителните облаци предоставя различни предимства и за двете страни - доставчици на услуги и потребители, но има и някои ограничения и предизвикателства 1, 10, 12.

Сигурност и поверителност: Сигурността на данните е основен въпрос, свързан със защита на личните данни и конфиденциална информация на организациите. Потребителят напълно е зависим от доставчика на облачни услуги, за това как се съхраняват и опазват неговите лични данни и корпоративна информация.

Технически предизвикателства: Високата скорост изисква добра комуникационна свързаност. За осигуряване на това изискване съществуват няколко ограничения. За всички е ясно, че мобилните устройства имат доста ограничения – захранване, памет, изчислителна мощ, място за съхранение, скорост на предаване/приемане и др.

Едно от очевидните решения за преодоляване на тези ограничения е да се използват изчисления в облака и облачни услуги. Използвайки концепцията за тънък клиент, мобилното устройство може да изпълни заявка за сложни изчисления върху отдалечен сървър с висока производителност използвайки Интернет свързаност. За съжаление обаче забавянето на WAN (long WAN latencies) комуникацията е един от основните проблеми.

Закъснения при WAN комуникацията - Закъсненията при WAN комуникацията са един от основните проблеми при използването на мобилни компютри, разчитащи на изчислителната мощ на облака. Потребителите са много чувствителни и нетърпеливи към закъснения и накъсвания, а това доста трудно може да се контролира във WAN комуникацията. Пряката зависимост е, че когато се увеличава латентността на връзката, то отговора се забавя. И докато малко ресурсоемки задачи, като сърфиране в мрежата, все още могат да се изпълняват, то задачи изискващи по-голям ресурс (напр. добавена реалност) се забавят неимоверно или дори спират своето изпълнение.

Ограниченията в честотната лента - Друг елемент влияещ върху използването на облачните изчисления и услуги с помощта на мобилните компютри е ограничението, което налага честотната лента на безжичната комуникация. Например при

обработка на графични или видеоизображения е необходимо както много процесорна (изчислителна) мощ така и прехвърляне на голямо количество данни от облачната среда в крайното устройство. Поради естеството на безжичната комуникация тези прехвърлянето на голям обем от данни ще доведе до забавяне на взаимодействието с потребителя. В този случай ефектът е двоен: забавяне от времето за изчисление и забавяне от прехвърлянето на голям обем от данни.

Data lock-in (заклучване от производителите): Към настоящия момент множество компании предлагат решения за облачни услуги и облачни изчисления, но всички те са частни т.нар. proprietary. Липсата на стандартни интерфейси ограничава възможността за миграция на данните от едно приложение към друга, а също така и от един облак към друг. С увеличаване на използваемостта на облака се очаква проблемите, свързани с преносимост на данните, миграция и зависимост от доставчика на услуга/изчисления да се задълбочат.

Сегрегация на данните: Проблемът със сегрегация на данните възниква при режим на многопотребителско използване на даден ресурс, където виртуалните машини на различни потребители са разположени върху едни и същи твърди дискове или сървъри. В този случай рисковете се крият в начина на разделение, използване и управление на паметта и твърдите дискове между различните потребители на системата.

Географско местоположение на данните: Географското разположение на данните е също много важен елемент за осигуряване на сигурност на данните на потребителите. Правилата и регулациите за определени типове данни е различно в различните страни. Възможно е потребителя да бъде въввлечен в различни правни аспекти на сигурността на данните без дори да бъде информиран.

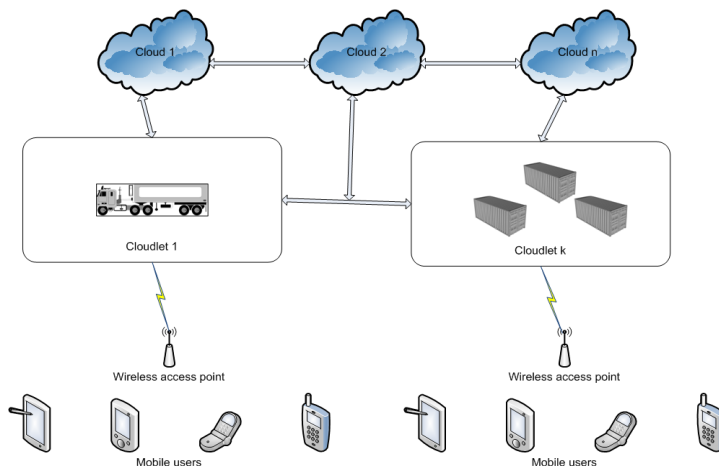
Архивиране и възстановяване: Един от основните въпроси за сигурността и надеждността на една система е начина на създаване и управление на резервните копия на информация. При облачните услуги този въпрос е предоставен за решаване от доставчика на услуга и потребителите няма възможност да оказват влияние върху него. Възможно е след срив в системата (физически, природен и т.н.) данните да се възстановят много бавно или дори да не могат да бъдат възстановени.

III. Специализирани архитектури за облачни услуги Мобилни облачни центрове (Cloudlets)

Въпросът който логично следва е може ли да използваме новостите и предимствата на облачните услуги без да сме ограничени от WAN средата?

Едно от решенията е разгледамо на много различни източници и е известно като Mobile Cloud Computing (MCC) или Cloudlet (облаче) 5, 6, архитектурата на което е показана на фиг.2. При този тип решение основният акцент се поставя върху това да не се използват отдалечени облачни центрове, комуникацията до които е бавна, а да се изградят и използват малки облачни центрове (cloudlets), които се намират близко до потребителите и в същото време са мобилни. Необходимостта от бърз отговор и изчисления почти в реално време обуславят изискванията които могат да бъдат постигнати чрез услуги и ресурси намиращи се на т.нар. един хоп, ниска латентност и високо пропусклива безжична мрежа до облачната инфраструктура. Физическата близост на “облачето” е от съществено значение: времето за отговор от точка до точка, трябва да бъде от порядъка на няколко милисекунди и също така да бъде предсказуемо. Ако няма наличен Cloudlet в близост или всички негови

ресурси са заети, то тогава мобилното приложение може да изиска достъп и потърси услуга от наличен класически център за облачни изчисления, като по този начин скоростта на обработка и комуникация ще се намали значително. Пълната функционалност ще се възстанови по-късно когато Cloudlet е наличен или са освободени ресурси в съществуващ такъв 5.



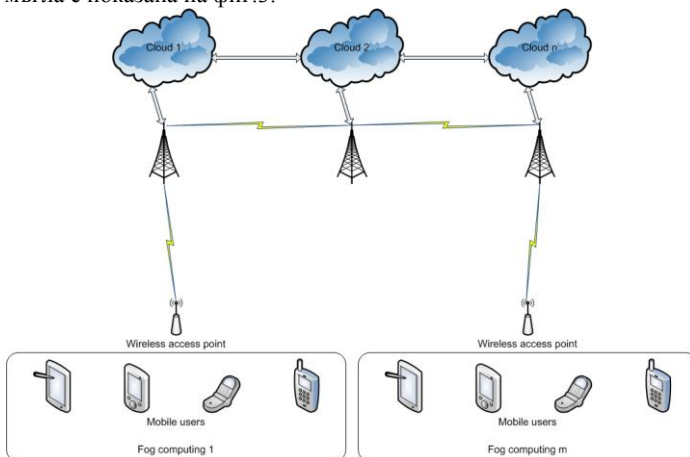
Фиг. 2. Мобилни изчислителни центрове за данни (Cloudlets).

От гледна точка на архитектурата на подобна система, то “облачетата” са децентрализирани, и широко разпръснати, като техните изчислителни ресурси и капацитет за съхранение на данни са в интерес на най-близките мобилни устройства. От друга гледна точка Cloudlet може да бъде разглеждан като мобилен център за данни или като data center in the box. Той има собствено управление и настройки, контрол на достъпа до основните системи за управление и разбира се свързаност както с мобилните устройства около него, така и с един или няколко центъра за данни предоставящи облачни услуги. По своята същност Cloudlet не трябва да се разглежда като самостоятелно решение, а като един от елементите (междинен) при изграждане на единна облачна инфраструктура. Тази негова функционалност го прави удобен за разполагане на различни места близко до мобилните потребители – в лекарски кабинет, в ресторант или кафе, но също така и в бойна машина, кораб или самолет. Основната характеристика която обуславя неговото използване е, че данните съхранени в Cloudlet-a са копие на данни вече съхранени в основните центрове за данни, следователно унищожаването на такъв мобилен център за данни ще има ефект върху скоростта на обработка и разпространение на информация в близките мобилни устройства, но няма да има загуба на информация 5, 9.

Fog Computing (изчислителна мъгла)

Преди 2 години фирмата Cisco Systems предложи ново понятие “fog computing” (изчислителна мъгла) 2, 3. Целта на предложението е лесен трансфер на данни от

центровете за данни в безжична и разпределена среда. Архитектурата на изчислителната мъгла е показана на фиг.3.



Фиг. 3. Примерна архитектура на fog computing

Някои автори тълкуват понятието с аналогията, че мъглата е облак който е по близо до земята. Според авторите на доклада може да се каже, че изчислителната мъгла е разпределена система за облачни изчисления използваща предимно крайните потребителски устройства. Следователно това са изчисления и услуги базирани на облачни технологии, които се извършват в непосредствена близост до потребителите, чрез използване на техните крайни мобилни устройства може да се дефинира като изчислителна мъгла. Fog computing като концепция предоставя по-добро качество на услугата, от гледна точка на консумация на енергия, забавяне, и намаляване на трафика на данни по комуникационните канали 4, 7, 8.

Основните предимства на fog computing са свързани със 10:

Поддържане на данните близо до потребителя: С цел намаляване на забавянето на трансфера на данни fog computing позволява запазване на данните, в близост до потребителя. По този начин само основните данни се прехвърлят в центровете за данни.

Добро (наситено) географско разпределение: Fog computing създава базова мрежа (edge networks) която се намира в множество точки и позволява предоставяне на облачни услуги в изолирани географски райони. По този начин е възможно да се анализират големи обеми от данни по-бързо без да е необходимо данните да се трансферират до основните отдалечени центрове за данни.

Подкрепа на мобилността: В последните години има огромно увеличение в размер на данните и броя на мобилните устройства. Fog computing концепцията позволява да се обработват тези големи обеми от данни и информация и предоставя по-добър и по-бърз начин за достъп и анализ до данните и информацията.

Запазване (намаляване) на мястото за съхранение на данни: Чрез прилагане на концепцията за изчисления в мъглата ще се намали необходимостта от трансфер и съхранение на неподходящи данни и информация по този начин ще се

спести място за съхранение на данни и ще се намали трафика на данни в комуникационната мрежа.

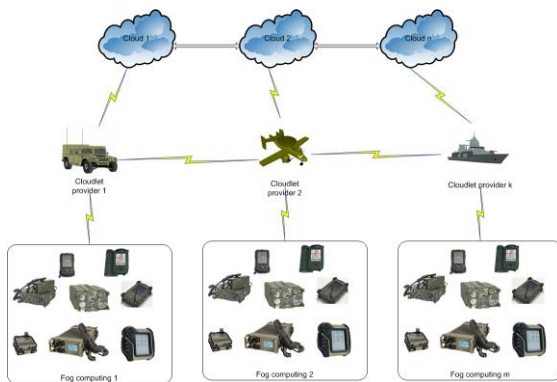
Парадигмата Fog computing е приложима в различни области където Интернет (мрежата) от неща вече съществува или започва да се развива като: светофарни уредби (т.нар. smart светофари), автомобили, интелигентни мрежи (електроснабдяване, водоснабдяване и др.) умни градове, използване на различни средства в бойните машини или войника като система от сензори и разпределени изчисления. По своята същност fog computing не трябва да се счита за замяна на облака, а като продължаване на тези услуги, но филтрирани и с по-бърз достъп на потребителите.

IV. Хибридна архитектура при изграждане на облачни решения с военно предназначение

Изграждането на различни информационни и комуникационни решения е в пряка зависимост от целите и задачите които даденото формирование трябва да изпълнява. От една страна се поставят необходимите качество, навременност, надеждност на изискваните услуги, а от друга възможността да се осигурят с налични сили и средства.

Съществуващите към момента подходи разчитат на класически архитектури при които имаме централизирана клиент-сървър среда или разпределена среда с равнопоставени възли. Към дадения момент все още не са изследвани напълно възможностите на класическа облачна инфраструктура в контекста на военни операции. Повечето от съвременните схващания са, че облачна инфраструктура с изразени центрове за данни е приложима в ежедневната работа на оперативно и тактическо ниво, но без отчитане на елемента възможна криза или бедствие. Разбира се изграждането на инфраструктура и услуги на основата на облачни технологии е приложима и с отчитане на възможности за създаване на т.нар. планове за възстановяване след бедствия и аварии.

Принципна схема на комбинираното използване на различните архитектури с отчитане на аспектите и изискванията към комуникационните и информационните услуги в контекста на военни задачи е представен на фиг. 4.



Фиг. 4. Подход за използване на облачни технологии във военен контекст

Все повече се налага модела при който силите и средствата които се разполагат в дадена област идват със свои собствени комуникационни и информационни услуги и развърщат свои собствени малки/мобилни центрове за данни. Погледнато от гледна точка на разновидността на облачните архитектури това е класически начин за създаване на cloudlets архитектури и услуги които са близо до потребителя, създават своя собствена комуникационна инфраструктура и мобилните военни и цивилни средства използват тази инфраструктура за изчисления, анализи и съхранение на данни. Тези центрове (облачета) могат да бъдат разположени в самолети, кораби или бойни машини. Те са мобилни, близо до потребителите, предоставят допълнителни ресурси, но също така мога лесно да бъдат идентифицирани и повредени. Тези мобилни облачни центрове препредават данните до стационарните защитени центрове за данни с дефинирани и стартирани облачни услуги.

От друга страна използваните от войника средства на полето или в машината разполагат с достатъчно изчислителна мощ, захранване и място за съхранение за изпълнение на конкретни задачи, а част от тези ресурси могат да бъдат предоставени за общо ползване от други мобилни устройства в непосредствена близост. По този начин се формира слой за първични, близки до реално време изчисления които използват всички близки ресурси и предоставят непосредствена информация на потребителя. На базата на подхода разгледан по-горе това е т.нар. изчисления в мъглата (fog computing).

Заклучение

Класическата облачна архитектура, с присъщите си ограничения, не е адекватна на динамиката и многообразието на съвременната реалност като цяло и бойното поле в частност. Развитието на изчислителните технологии от една страна и съвременните функционални потребности от друга водят до нови архитектури в облачните услуги като облачета (Cloudlet) и изчисления в мъглата (fog computing). Предложената хибридна архитектура, базирана на комбинираното им използване, съвместно с класическия модел, е подходяща за прилагане в широк кръг военни операции.

Литература

1. Archer, Jerry, et al. "Top threats to cloud computing v1.0." Cloud Security Alliance (2010).
2. Cisco, "Cisco delivers vision of fog computing to accelerate value from billions of connected devices," Cisco, Tech. Rep., Jan. 2014.
3. Cisco, Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are
4. Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli, Fog Computing and Its Role in the Internet of Things, MCC '12 Proceedings of the first edition of the MCC workshop on Mobile cloud computing, ACM New York, NY, USA ©2012 ISBN: 978-1-4503-1519-7 doi: 10.1145/2342509.2342513
5. Graham Kirby, Alan Dearle, Angus Macdonald, Alvaro Fernandes, An Approach to Ad hoc Cloud Computing, arXiv:1002.4738v1 [cs.DC]
6. Gülfem Işıklar Alptekin, A Resource Trading Framework for Cloudlets, Proceedings of the World Congress on Engineering and Computer Science 2015 Vol II WCECS 2015, October 21-23, 2015, San Francisco, USA, ISBN: 978-988-14047-2-5

7. K.P.Saharan, Anuj Kumar, Fog in Comparison to Cloud: A Survey, International Journal of Computer Applications (0975 – 8887), Volume 122 – No.3, July 2015
8. Kanghyo Lee, Donghyun Kim, Dongsoo Ha, Ubaidullah Rajput, Heekuck Oh, On Security and Privacy Issues of Fog Computing supported Internet of Things Environment, IEEE Network of the Future (NOF), DOI: 10.1109/NOF.2015.7333287
9. Mahadev Satyanarayanan, Paramvir Bahl, Ramon Caceres, Nigel Davies, The Case for VM-based Cloudlets in Mobile Computing, IEEE Pervasive Computing (Volume:8 , Issue: 4), Page(s): 14 - 23, ISSN :1536-1268, DOI:10.1109/MPRV.2009.82
10. S. Yi, Z. Qin and Q. Li, "Security and privacy issues of fog computing: A survey", International Conference on Wireless Algorithms, Systems and Applications (WASA)
11. Special Publication 800-145. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology.
12. Желязков Д., Н. Стоянов, Проблеми при защита на информацията в решения от тип "cloud computing", Конференция „Военни технологии и системи 2011“, Институт по отбрана, София 2011.

ТЕНДЕНЦИИ В ДЕЙНОСТТА НА ИЗПЪЛНИТЕЛНА АГЕНЦИЯ ЕСМИС ЗА ПРИЛАГАНЕТО НА ОБЛАЧНИ ТЕХНОЛОГИИ В СФЕРАТА НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ

Добрин Ст. Караколев

Началник на отдел „Развитие на облачни технологии“, ИА ЕСМИС
гр. София, ул. Гурко №6, ПК 1000, ИА ЕСМИС

Гюлджан В. Ахмедова

Младши експерт, ИА ЕСМИС и докторант в Лесотехнически университет
гр. София, ул. Гурко №6, ПК 1000, ИА ЕСМИС

В публичното пространство непрекъснато се подчертава необходимостта от качествено информационно осигуряване, като предпоставка за гарантирано качество на управленските процеси. В наше време тяхното непрекъснато оптимизиране е функция на бързото развитие на информационните технологии и свободния обмен на информация. Прилагането на информационните технологии във всички сфери на обществения живот, доведе до преосмисляне на редица управленски теории и практики. Тези промени изискват, от своя страна, нови подходи и механизми в управлението на организациите и вземането на решения.

В тази връзка, вече не стои толкова въпросът дали да се използват съвременни технологии, а по-скоро как те правилно да се интегрират в съществуващата информационна инфраструктура, като същевременно са съобразени и адаптирани с изискванията на управленската среда. Разбира се, тази адаптация не трябва да бъде самоцел. Тя трябва да е в резултат на следването на избраната стратегия за разви-

тие на изградената информационна инфраструктура, анализ на управленските механизми и на възможността за участие в тях на заинтересованите страни (правителство, граждани и бизнес).

Широката популярност, която придоби Cloud Computing като технология, не е случайност или мода. Според експерти сформирането на единна разпределена изчислителна облачна среда ще позволи да бъдат постигнати икономии на бюджетни средства и да се осигури ново ниво на информационна сигурност.

В контекста на горното съвсем закономерно възниква въпросът – “Как облачните технологии могат ефективно да се използват в интерес на държавните институции и в сферата на електронното управление ?” В тази връзка е важно да се определят същността и елементите на двете понятия – „електронно управление“ и „облачни технологии“.

ЕЛЕКТРОННО УПРАВЛЕНИЕ И ЕЛЕКТРОННИ АДМИНИСТРАТИВНИ УСЛУГИ

Приема се, че терминът *електронно управление* обобщава употребата на информационни и комуникационни технологии (ИКТ) при предоставяне на публични **административни услуги на гражданите**. Като основни цели на електронното управление могат да се дефинират:

- повишаване удовлетвореността на гражданите и бизнеса;
- подобряване ефективността на работа и качеството на услугите, предоставяни от видовете власти;
- подобряване обмена на информация между отделните административни информационни системи.

Основен атрибут на електронното управление е електронната административна услуга (ЕАУ). В тази връзка ясно следва да се определят изискванията, на които ЕАУ трябва да отговаря, а именно: да е възможно в реално време (online) взаимодействието по **електронен път за всеки един от четирите** стадия от нейното реализиране:

- **Информиране** (предоставена е **информация** относно наличието на административната услуга, както и ясни указания за нейното използване и описание на крайния резултат при извършване на транзакция);
- **Едностранно взаимодействие** (осигурена е възможност за **зареждане** формите на документите, които са поискани от потребителите на ЕАУ);
- **Двустранно взаимодействие** (осигурена е възможност за **обработка** формите на документите, включително и автентификация от страна на потребителите на ЕАУ);
- **Провеждане на транзакция** (електронна реализация на исканата **операция**).

Тук следва да се отбележи, че ако дори една от описаните фази не е реализирана в реално време или тя е частично реализирана, то крайният резултат не би могъл да се приеме за положителен.

За по-детайлен анализ на множеството административни услуги те могат да се разделят на четири функционални групи:

- **Плащания** - услуги, при които финансовите потоци са насочени от гражданите и бизнеса към правителството (данък печалба, данък общ доход, обществено осигуряване и т.н.);

- **Регистрация** - услуги, свързани с оформяне обектни или персонални данни, като резултат на административни задължения (регистрация на фирма, регистрация на автомобил и т.н.);

- **Предоставяне на добавки** - услуги, позволяващи на гражданите да получават преимущество или печалба в замяна на това, че са изпълнили задълженията си към държавата (работа, социална защита, медицински услуги и т.н.);

- **Издаване на документи** - документи, издавани от държавните и общински органи (персонални документи, разрешения за строителство и т.н.).

Същевременно като **пета функционална група** ЕАУ могат да посочат гласуването в реално време – избори, референдуми и др., а защо не и машинното гласуване. Въпреки, че последното не е типична електронна административна услуга, при него ясно могат да се отличат посочените по-горе стадии на реализиране, а именно: информиране, взаимодействие и транзакция, които по същество се извършват в реално време.

ОБЛАЧНИ СРЕДИ И ОБЛАЧНИ УСЛУГИ

Много често, като основа при разглеждането на облачния модел, се приема формулировката на Националния институт по стандартите и технологиите на САЩ (National Institute of Standards and Technology – NIST [1]), публикувана в края на октомври 2010 година, а именно:

“Облачни изчисления – това е модел на осигуряване на повсеместен и удобен мрежови достъп по заявка до изчислителни ресурси (например мрежи, сървъри, системи за съхранение, приложения и услуги), които могат да бъдат бързо осигурени, използвани и освободени с минимални експлоатационни разходи и усилия по тяхното управление, чрез взаимодействие с доставчик на услуги”.

Пак в публикациите на NIST [1] детайлно са описани моделите на доставка на облачните услуги – Инфраструктура като услуга (IaaS), Платформа като услуга (PaaS) и Софтуер като услуга (SaaS). Предвид темата на доклада тези услуги няма да бъдат разглеждани в тяхната технологична същност. Следва да се подчертае, обаче че моделите на доставка на облачни услуги произтичат от съставните компоненти на самите информационни ресурси в своята цялост, а именно: инфраструктурен компонент (процесорна мощ, памет, дисково пространство и мрежи), компонент Платформа (различни среди за разработка, среди за тестване, среди за управление на ресурси и др.) и компонент Приложения (свкупността от приложения софтуер, който е инсталиран на сървърни платформи или на работните станции на крайните потребители).

Облачните структури имат пет ключови характеристики, които ги определят като такива, а именно: самообслужване по заявка, широк мрежов достъп, пул от ресурси, еластичност и измеряемост. Ако дори една от тези характеристики е пропусната, то структурата не може да се приеме за облачна.

ЦЕНТРОВЕ ЗА ДАННИ

Ако се приеме, че облачните структури могат да имат „физическо измерение“ то това са центровете за данни. Тези инженерно-технически съоръжения осигуряват информационни ресурси с високо ниво на достъпност и сигурност.

С развитието на облачните технологии и необходимостта от консолидация на услугите, съвременните центрове за данни придобиват все по-голямо значение и се очертават като основни ядра за обработка, съхранение и предоставяне на информа-

цията. Съвременният център за данни трябва да осигурява следните 3 важни условия:

- непрекъсваемост на информационните ресурси и достъпа до тях;
- висока консолидация, скалируемост и гъвкавост, базирани на прилагане на облачни технологии и виртуализация;
- надеждна защита и съхранение на информацията

Инфраструктурата на съвременния център за данни може да бъде условно разделена на физическа и информационна. Следва да се отбележи, че подобен поглед на инфраструктурата не е продиктувано от самите облачни технологии. През изминалите години, дори до края на 90-те на миналия век, в масова експлоатация бяха т.н. Изчислителни центрове. Предвид предназначението на тези съоръжения ще отбележим наличието в тях на повечето компоненти, характерни и за съвременните центрове за данни, а именно:

Физическа инфраструктура – която осигурява машинни зали гарантирано електрозахранване, климатизация, системи за пожароизвестяване и пожарогасене, структурно окабеляване, системи за контрол на достъпа, квалифициран технически персонал за експлоатация и поддръжка;

Информационна инфраструктура – която осигурява необходимата изчислителна мощ, изразена в процесорен ресурс, оперативна памет и дисково пространство.

Една от основните характеристики на изчислителните центрове, подобно и на съвременните центрове за данни, е високата концентрация на изчислителен ресурс. В същото време, обаче, инфраструктурата на съвременния център за данни притежава два съществени компонента, които не могат да бъдат открити в неговия стар аналог. Това са съвременните технологии за широк мрежов достъп и виртуализацията на ресурси.

Първата технология осигурява на потребителите отдалечени достъп до информационни ресурси практически без ограничения, което прави границите на облака променливи, така че тези граници да са там, където е самият потребител.

Виртуализацията, използвайки съвременни механизми и инструменти, позволява ефективното използване на изчислителния ресурс до 85% и повече.

От изложеното до тук може да се обобщи, че:

1. Основен компонент на електронното управление се явява широк набор от електронни административни услуги, които са насочени към гражданите и бизнеса.
2. Основен компонент на облачните инфраструктури се явяват облачните услуги. Ако говорим за облак на държавната администрация, то потребители на тези услуги с явяват държавните институции и органите за местно самоуправление. В този контекст същите се явяват точки на трансформация на изчислителни ресурси, предоставени от държавния облак в електронни административни услуги за гражданите и бизнеса.
3. Изчислителните ресурси на държавният облак са концентрирани в центрове за данни (основни, резервни и за възстановяване). Държавните институции и центрове за данни следва да са свързани в частна и контролирана Intranet среда.
4. От гледна точка на моделите на развържане (deployment model) на държавния облак, същият следва да се определи като Общностен (Community cloud). По дефиниция Общностният облак е вид частен облак, чиито ресурси се използват от няколко организации. Тези организации са обединени от различни признаци: еднакви цели и задачи, сродни бизнес модели, еднакви изисквания за сигурност и др.

Правата и задължението по поддръжката, развитието и управлението на облачната структура са делегирани на една от организациите, която се явява и доверен доставчик на облачни услуги на Общността. Целевата архитектура на Общностния държавен облак следва да дефинира участниците в процеса на управлението му и използване на ресурсите: доставчик на облачни услуги, потребители на облачни услуги, облачен брокер, облачен одитор и доставчик на външни (комуникационни) услуги, както и процедурите по които участниците си взаимодействат.

НАПРАВЛЕНИЯ ЗА РАБОТА В ИА ЕСМИС

Свързано с прилагането на облачните технологии в сферата на електронното управление, дейностите на Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи са“ са насочени в следните основни направления

- ✓ **Комуникационна и мрежова свързаност;**
- ✓ **Облачни технологии и облачни услуги;**
- ✓ **Поддръжка на центрове за данни**
- ✓ **Ко-локация на оборудване;**

В доклада са разгледани първите две направления

Комуникационна и мрежова свързаност

Една от основните задачи на ИА ЕСМИС е изграждане, поддържане, развитие, експлоатация и управление на **Единната електронна съобщителна мрежа на държавната администрация и за нуждите на националната сигурност (ЕЕС-МДАНС)**, която е част от Интегрираната комуникационно-информационна система за управление на страната и въоръжените сили. Тази среда осигурява комуникационни и мрежови мощности за:

- частни потребителски Intranet мрежи – осигуряват затворена свързаност между частни ресурси на отделните организации в т.ч. и между различни локации на територията на страната. Осигурява затворена свързаност на организациите към изградените центрове за данни;
- мрежи за публичен достъп (Интернет) – осигурява достъп на организациите до световната мрежа;
- мрежи на центрове за данни – осигурява затворена свързаност с необходимия капацитет и скорости между центрове за данни, необходима за извършване на репликации, резервиране на данните и осигуряване на висока наличност.

ЕЕСМДАНС е изградена на базата на L2/L3 инфраструктура с обща дължина на оптичните кабелни трасета над 7700км. Броят на възлите за достъп възлиза на 660. Ресурсите на мрежата се използват от всички държавни институции и областни центрове, а към 03.2016г. в нея са включени 78 общински центрове.

Агенцията разполага с инфраструктура подходяща за изграждане на защитени центрове за данни (място за сървъри зали, електричество, климатизация, контрол на достъпа и др.) В края на 2015 успешно беше финализиран проект за изграждане на център за данни, чиято физическа и информационна инфраструктура е събрана с изискванията към този тип съоръжения.

Облачни технологии и облачни услуги

През 2013 ИА ЕСМИС започна изграждането на прототипен център за данни, чиято първоначална цел беше да осигури необходимата среда за тестване на различни облачни решения и техники за виртуализация. В настоящият момент този

център разполага със значителен ресурс и въпреки името си е в състояние да осигури продукционна среда в следните направления:

- Облачни среди и среди за виртуализация;
- Системи за управление на облачни услуги;
- Многопотребителски (multi tenant) среди;
- Инфраструктура за виртуален десктоп;
- Хостинг;
- Прототипни среди за тестване.

Изградените среди използват решения на водещи производители каквито са Microsoft, Citrix, VMWare и Hewlett Packard. Сериозно внимание е отделено и на решения с използване на отворен код, които позволяват прилагането на KVM и Container виртуализация.

Независимо от използваното индустриалното решение, някои от средите в прототипния център за данни притежават необходимите характеристики, които ги определят като облак. От технологична гледна точка ясно могат да се различат важни компоненти като:

- Клъстерна организация и пул от ресурси;
- Логическо или физическо разделяне на мрежите: за управление, за дисковия капацитет, за потребителски достъп и др.
- Напълно функциониращи портали за самообслужване на потребителите (on-demand self service) и портали за администриране;
- Системи за управление на потребителите (дефиниране на права, дефиниране на квоти на ресурсите и др.)
- Пълно резервиране на физическата мрежова свързаност и конфигурирани системи за мрежов контрол на достъпа;
- Възможност за бързо добавяне на изчислителен ресурс;
- Инструменти за автоматизация и оркестрация на управлението.

При предоставянето на Инфраструктура като услуга (IaaS) платформите са в състояние да осигурят достъп до виртуалните ресурси по два основни сценария: използване на инфраструктура за предоставяне на публична услуга и използване на инфраструктура като част от локалните ресурси на потребителя. Вторият сценарий по същество дава възможност на потребителите да създадат собствен виртуален облак (virtual private cloud- VPC), който да управляват напълно самостоятелно.

През 2014г. в изпълнение на решение на Съвета по електронно управление и чрез използване на наличния изчислителен ресурс беше изградена многопотребителска (multi tenant) среда за обединени комуникации (МСОК) на базата на Microsoft Lync. Средата попада в полето на Платформа като услуга (PaaS) и дава възможност на държавните структури и на органите за местно самоуправление да използват възможностите ѝ без да правят каквито и да било инвестиции. Планира се до края на 2016г. в МСОК да се интегрира и пощенска услуга, след което да се въведе в редовна експлоатация.

Същевременно в процес на тестване са и решения за многопотребителски среди, които ще са в състояние да предоставят VoIP услуги. Значително внимание се отделя и на инфраструктурите за предоставяне на виртуален десктоп (VDI). Наред с другите предимства VDI са изключително полезни за достъп до приложения от мобилни клиенти. На този етап прототипът е оразмерен и лицензиран за около 100 потребителя.

ЗАКЛЮЧЕНИЕ

Очевидно е, че облачните технологии дават възможност на държавните структури да използват услуги на високо ниво, които да осигуряват необходимата изчислителна мощ при трансформирането им в електронни административни услуги. Същевременно технологията позволява виртуалните ресурси да са насочени и в интерес на самите държавни структури за обезпечаване на ежедневните бизнес процеси.

Същевременно следва да се подчертае, че технологичното изграждане на държавен изчислителен облак е само етап от процеса на прилагане на облачните технологии в интерес на държавното управление и елементите на електронното правителство. Като насоки за развитие могат да се дефинират следните основни направления:

1. Непрекъснат процес по наблюдение и оптимизиране на приложената целева архитектура.
2. Разработване и прилагане на методики за постепенно мигриране на информационните ресурси в облачната среда.
3. Разработване и прилагане политики и процедури за сигурност на данните.
4. Резервиране на инфраструктурата чрез резервни центрове за данни и център за възстановяване (Disaster Recovery Center).
5. Непрекъснат процес на поддръжка, управление, оптимизиране и развитие на изградената инфраструктура и запазване на инвестициите.

В редица от публикации по тематиката се изразява мнение, че облачните технологии ще определят технологичната и организационна рамка в сектора през следващите 15 и повече години. Ето защо от съществено значение е държавните стратегии и политики, които се изпълняват, да са съобразени с тази тенденция.

ЛИТЕРАТУРА:

1. Peter Mell, Timothy Grance, The, NIST Definition of Cloud Computing, Special Publication 800-145 -

АВТОМАТИЗИРАНО ПРОФИЛИРАНЕ В КОНТЕКСТА НА ГАРАНТИРАНЕ НА НАЦИОНАЛНАТА СИГУРНОСТ

Мартин В. Захариев

Десислава Е. Кръстева

*Адрес за кореспонденция: Фондация „Право и Интернет“, гр. София 1303, ул.
„Българска моравя“ № 54, ет. 7*

AUTOMATED DATA PROFILING IN THE CONTEXT OF GUARANTEEING THE NATIONAL SECURITY

Martin V. Zahariev

Desislava E. Krusteva

ABSTRACT: *The processing capacity of modern technologies can be used for protection of national security. The automated data profiling however raises many legal and ethical questions concerning the privacy and the balance between the interests of the individual and the society.*

KEY WORDS: *data profiling, data mining, national security, automated decisions taking, privacy*

1. Въведение – информационните и комуникационните технологии в контекста на националната сигурност

В контекста на усложнена международна обстановка и терористични атаки в редица точки по целия свят, съвременните държави са изправени пред сериозно предизвикателство в стремежа да гарантират своята национална сигурност. На този фон, развиващите се все по-бързо информационни и комуникационни технологии (ИКТ) са масово разпространени – на практика днес почти всеки има компютър, мобилен телефон, таблет и пр. Използвайки ИКТ в своето ежедневие, хората непрекъснато генерират огромен обем данни (в т.ч. и голямо количество лични данни) – разменена електронна кореспонденция под всякакви форми (имейли, социални мрежи, чатове, мобилни приложения и пр.), данни за търсения по ключови думи в различни търсачки, Джи-Пи-Ес данни и т.н [1]. В този поток от данни се съдържа изключително разнородна информация – както информация за личния, социалния, икономическия и т.н. живот на хората, както и информация, която може да бъде от ключово значение за откриването и предотвратяването на евентуални заплахи за националната сигурност. Навременното откриване на информация от втория вид е особено съществено за органите, призвани да гарантират националната сигурност. Следенето, записването, съхраняването и обработката на целия този огромен обем данни с помощта единствено на човешки потенциал е на практика невъзможно. За да се обработят такива обеми данни в разумни срокове, държавните служби за защита на националната сигурност могат да използват именно ИКТ. Единствено автоматизирани програми, работещи без човешка намеса, позволяват обработката на такива количества данни за относително кратки интервали от време, така че да се генерира полезна информация и да се предприемат мерки за противодействие на

планирани заплахи за националната сигурност. В същото време обаче възниква въпросът дали подобно обработване на лични данни е законосъобразно, доколко е оправдано навлизането в правната сфера на субектите, чиито данни се обработват и пр. Това отваря голямата тема за използването на автоматизираното профилиране за защита на националната сигурност и за пределите на неговата допустимост.

Настоящото изложение има за цел последователно да:

- Изясни същността на автоматизираното профилиране;
- Изясни предимствата на автоматизираното профилиране в сферата на сигурността и отбраната;
- Анализира някои правни аспекти на използването на автоматизирано за опазване на националната сигурност.

2. Същност на автоматизираното профилиране

Изясняването на това какво представлява автоматизирано профилиране предполага анализ на две други понятия, стоящи в основата на концепцията за него – „дейта майнинг“¹ и „профилиране“. Съществуват поне три концепции за същността на дейта майнинга – (i) метод за обработка на информацията, (ii) автоматизиран метод за откриване на знания в бази данни или (iii) един от етапите в откриването на знания в бази данни [2]. Независимо от теоретичните спорове относно същността на дейта майнинга, за целите на настоящото изложение ще се използва следната работна дефиниция: *„една или съвкупност от процедури, посредством които големи масиви от данни се обработват с алгоритми с цел откриване на повтарящи се образци или корелации между данни (на английски език “patterns”). Тези корелации указват наличието на определена връзка между данните, предмет на обработката, без обаче непременно да е необходимо тази връзка да е причинна“*. По този начин с помощта на автоматизирани методи за обработка на информацията от налични данни става възможно генерирането на нова информация, невидима за човека при обикновен преглед на данните. Използването на дейта майнинг е първата стъпка към осъществяването на автоматизираното профилиране.

Втората стъпка е използването на генерираната чрез дейта майнинга информация с цел профилиране на лицата, чиито данни са обработени. Думата „профилиране“ произлиза от „профил“ (от френски и италиански език *“profile”*). Едно от значенията на думата „профил“ е съвкупност от типичните черти на професия, специалност, на техни клонове и подобни [3]. Профилирането от своя страна може да се определи като дейност по групиране на отделни явления и/или обекти в отделни категории (профили) посредством една или повече техни общи черти/признаци/белези. Профилирането, осъществявано чрез ИКТ и зададени алгоритми, т.е. без човешка намеса, се нарича **автоматизирано профилиране**.

Автоматизираното профилиране се основава на дейта майнинга, но целта при този вид профилиране е генерирането на нова информация – прогноза или предположение, основана на предишно поведение, данните за което се съдържат в електронна среда. В този смисъл автоматизираното профилиране е способ за генериране на нови знания по индуктивен път [4]. Установените чрез него взаимовръзки и

¹ На английски език терминът се нарича *“data mining”*, докато в български език няма точен аналог. Използват се описателни понятия като „извличането на знания от данни“, „добив на данни“, „сондиране на данни“, „интелигентен анализ на данните“ и др. В настоящото изложение ще се използва транслитерация от английски език – „дейта майнинг“.

корелации указват наличието на вероятност за настъпване на определени обстоятелства, въз основа на вече генерирани данни. С оглед изложеното, за целите на настоящото изложение ще се използва следната работна дефиниция на автоматизираното профилиране: *„процес на (i) откриване на корелации между данни в масиви от данни, които са от естество да бъдат използвани за създаване на профил(и) въз основа на дадени характеристики на физическите лица, и/или (ii) прилагане на профилите, разбираани като вече обработена и генерирана нова информация, с цел индивидуализиране на лицата, чиито данни са обработени, и/или включването на лицата в дадена група или категория“.*

Профилирането навлиза в обществения живот много преди възникването на компютъра – създавани са профили на престъпници за целите на наказателната превенция и борбата с престъпността; профили на хора с психични заболявания в психиатрията и медицината; профили на клиенти и/или потребители, към които да се отправят търговски оферти и т.н. [4]. Въпреки това обаче никога досега не е било възможно обработването на толкова голямо количество данни за толкова кратки срокове. В този смисъл, използването на ИКТ за профилиране разкрива нови и неподозирани възможности за защита на националната сигурност.

3. Предимства на използването на автоматизираното профилиране в сферата на сигурността и отбраната

Условно може да се разграничат две групи предимства на използването на автоматизираното профилиране в сферата на сигурността: (i) предимства, произтичащи от автоматизирания му характер и (ii) предимства, произтичащи от самата същност на профилирането като дейност по групиране (систематизиране) на информацията.

3.1. Предимства, произтичащи от автоматизирания характер на профилирането. Те се дължат в голяма степен на ИКТ и техния капацитет за обработка на информацията. Чрез използването на сложни алгоритми, работещи без човешка намеса, става възможно:

- Обработката на изключително големи обеми данни;
- Постигането на много по-голяма бързина на процесите за обработка на данните в сравнение с обработката по неавтоматизиран път;
- Откриване на трудни (дори невъзможни) за установяване корелации.

В светлината на изложеното следва да се подчертае, че за да бъде автоматизираното профилиране ефективно е необходимо анализирането на **възможно най-голямо количество данни**, за да може да се изведе максимално достоверна структурирана информация. Иначе казано, колкото по-голям информационен масив се обработва, толкова по-голяма е вероятността да се открият достатъчно много повтарящи се белези на съответния обект на изследване, за да може той да бъде „профилиран“ – *„за да намериш игла в купа сено, първо трябва да създадеш купа сено“* [1].

Естествена последица от големия обем данни, които следва да се обработят, за да се приложи на практика автоматизираното профилиране, е **технологичното време**, необходимо за обработката. Ако профилирането не се осъществява по автоматизиран път, то някои обеми данни въобще не биха могли да се обработят от човека или биха изисквали ангажирането на огромен човешки ресурс, което би направило профилирането неефективно. Друг недостатък, който се преодолява с

помощта на ИКТ, е обстоятелството, че дори обработката да е възможна, повечето големи масиви от данни биха се обработили толкова бавно, че интересът от генериране на информацията вече не би бил налице или изходната информацията не би била актуална, т.к. в изходната база данни са постъпили нови и по-актуални данни. ИКТ правят възможно прилагането на сложни процедури за анализ в огромни масиви от данни, като резултатите могат да бъдат получени в разумни срокове и при оправдани разходи [5].

Най-ценното предимство на профилирането с автоматизирани алгоритми обаче е **генерираната нова информация**. С помощта на ИКТ става възможно откриването на нови, незабележими за човешкото око корелации и повтарящи се образци в масивите данни, които залягат в основата на създаването на отделните профили. ИКТ правят възможно преодоляването на едно от най-големите предизвикателства пред модерното общество – отсяването на релевантна информация от нерелевантна информация в рамките на непрестанния информационен обмен [4].

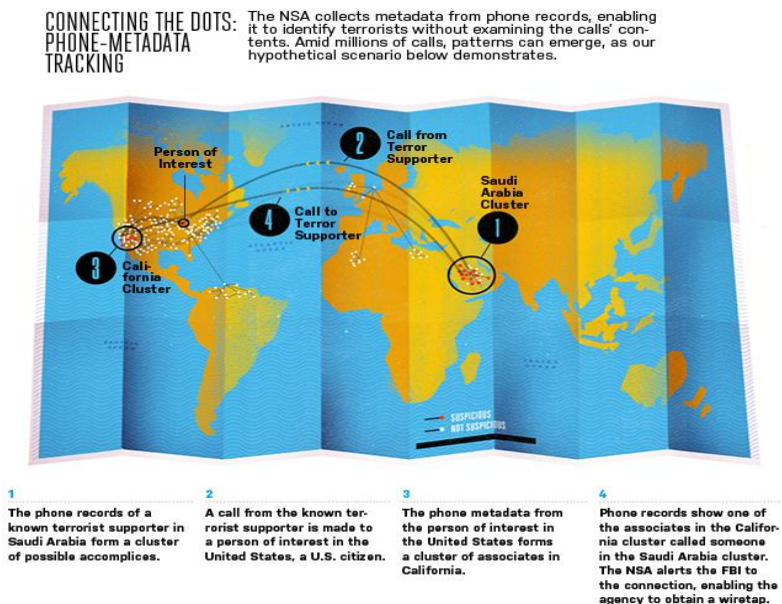
3.2. Предимства, произтичащи от същността на профилирането като дейност по систематизиране на получената информация. Те се свързват на първо място с **обобщаването на генерираната чрез дейта майнинга нова информация**, т.е. със създаването на профили на базата на откритите по автоматизиран път корелации. Систематизирането безспорно улеснява боравенето с получената в следствие на обработка на данните информация

Наред с това, създадените профили представляват прогноза за бъдещото поведение на субектите, чиито данни се обработват, или предположение за наличието на дадени факти. В този смисъл, чрез профилирането може да се направи **прогноза/предположение за наличието на бъдещи заплахи за националната сигурност**, което увеличава шансовете за тяхното разкриване и предотвратяване още на етап планиране. Доколкото откритите корелации са неоткриваеми за човека с традиционните неавтоматизирани методи за обработка на информацията, неимоверно се увеличава и вероятността за разкриване на внимателно планирани антидържавни действия, които се подготвят при много голяма секретност и в този смисъл са изключително трудни за разкриване само чрез използване на човешкия фактор. Пример как функционират профилиращите технологии чрез използването на дейта майнинг по отношение на метаданни от телефонни обаждания, т.е. без да се изследва съдържанието на самите обаждания, може да се види на фиг. 1 по-долу².

На фигурата под формата на хипотетичен модел в 4 действия е изобразено как Агенцията за национална сигурност на САЩ може да засече чрез дейта майнинг алгоритми потенциална заплаха за националната сигурност: 1) въз основа на записи на телефонни обаждания на известен терорист към дадени лица в Саудитска Арабия се формира клъстер с възможни съучастници; 2) обаждания от терориста към наблюдавано от Агенцията лице (на английски език “person of interest”); 3) въз основа на метаданните от телефонни обаждания на наблюдаваното лице се формира клъстер с възможни съучастници в САЩ; 4) обаждания от някой от клъстера възможни съучастници в САЩ към клъстера в Саудитска Арабия. Агенцията информира ФБР за установената връзка и може да започнат оперативно-издирвателни мероприятия – напр. пристъпване към процедура по получаване на

² Фигурата е възпроизведена от статията Pappalardo, J. – NSA Data Mining: How It Works, 2013, достъпна на интернет адрес <http://www.popularmechanics.com/military/a9465/nsa-data-mining-how-it-works-15910146/>, а като автор на фигурата е посочена Anderson, K.

разрешение за прилагане на специални разузнавателни средства (СРС) за подслушване на линията.



Фиг. 1

СРС в България не би следвало да допусне само въз основа на автоматизирано решение, макар да липсва изрична уредба по този въпрос. Прилагането на СРС по отношение на дейности, свързани със защитата на националната сигурност е възможно само въз основа на писмено мотивирано искане на административния ръководител на съответния орган, оправомощен да иска използването им (изчерпателно изброяване на тези органи се съдържа в чл. 13, ал. 1, т. 1-6 от Закона за специалните разузнавателни средства (ЗСРС), като от най-съществено значение в сферата на опазване на обществения ред и националната сигурност са Главна дирекция „Национална полиция“, Главна дирекция „Борба с организираната престъпност“, Главна дирекция „Гранична полиция“, дирекция „Вътрешна сигурност“, териториалните дирекции и самостоятелните териториални отдели на ДАНС, службите „Военна информация“ и „Военна полиция“ към министъра на отбраната, Държавна агенция „Разузнаване“ и др.). Искането трябва да съдържа пълно и изчерпателно посочване на фактите и обстоятелствата, даващи основание да се предполага, че се подготвя, извършва или е извършено тежко умишлено престъпление от изброените по чл. 3, ал. 1 ЗСРС включително и в случаите на извършване на дейности, свързани със защитата на националната сигурност (чл. 4 ЗСРС), които налагат използването на СРС; пълно описание на извършените до момента действия и резултатите от пред-

варителната проверка или разследването (*евентуално тук е мислимо да се добавят евентуално генерирани в следствие на профилирането данни*); установъчни данни на лицата или обектите, спрямо които ще се използват СРС; срока, за който се иска ползването, и мотиви, които да обосновават продължителността му; оперативните способности, които следва да се приложат; оправомощеното длъжностно лице, което да бъде уведомявано за получените резултати; мотиви за невъзможността необходимите данни да бъдат събрани по друг начин или описание на изключителните трудности, с които е свързано събирането им (чл. 14, ал. 1, т. 1-7 ЗСРС).

Впоследствие допълнителна гаранция за законосъобразното прилагане на СРС е изискването за изрично разрешение/разпореждане от компетентен орган – в общия случай това са председателите на Софийския градски съд, съответните окръжни или военни съдилища, на специализирания наказателен съд или оправомощени от тях заместник-председатели (чл. 15, ал. 1 ЗСРС). Преди произнасянето заявителят е длъжен да предостави на органа, компетентен да даде разрешение, всички материали, на които се основава искането (*тук е мислимо да се осъществи съдебният контрол върху автоматизираното решение*) – чл. 15, ал. 2 ЗСРС. По изключение, при заплахата за националната сигурност СРС могат да се използват и без разрешение на органа по чл. 15 въз основа на разпореждане съответно на председателя на Държавна агенция „Технически операции“, председателя на ДАНС или главния секретар на МВР (чл. 18, ал. 1 ЗСРС). Видно от изложението, профилиращите технологии предлагат качествено нов инструментариум за защита на националната сигурност. Използването му обаче трябва да става в определени от правото рамки, което повдига темата за правните аспекти на автоматизираното профилиране.

4. Правни аспекти на използването на автоматизираното профилиране в сферата на сигурността и отбраната

Правовата държава, за каквато е прогласена Република България съгласно чл. 4, ал. 1 от Конституцията на Република България (КРБ), се основава на конституционализма и законността. В нея зачитането на човека с неговите основни права, свободи и интереси е най-висша социална ценност [6]. В този смисъл, осъществяването на всяка проява на публична власт (в т.ч. и прилагането на способности за гарантиране на националната сигурност) трябва да бъде съобразено със законите в страната. В противен случай, без действена държавна и правна институционалност обществото се разпада „*в резултат на собствените си антагонистични противоречия*“ [7] и се стига до анархия и произвол [8].

4.1. Правно основание за поддържането на масиви от данни от компетентните по опазването на националната сигурност органи. Първият съществен правен въпрос, свързан с евентуалното използване на автоматизираното профилиране за защита на националната сигурност, е дали действащото законодателство позволява събирането на данни в информационни масиви и обработването им с профилиращи технологии по автоматизиран път. Този въпрос е особено важен, защото органите, упражняващи властнически правомощия, осъществяват своята компетентност само и единствено въз основа и в рамките на закона – само тогава техните действия и актове са законосъобразни. Това важи с още по-голяма сила за органите и структурите, действащи в сферата на опазване на отбраната, националната сигурност и борбата с тероризма, т.к. те разполагат с най-съществения инст-

рументариум да навлязат в личната сфера и да засегнат (а при необходимост и да ограничат) правата и свободите на хората. Ето защо, осъществяването на автоматизирано профилиране в правовата държава е немислимо без изрична правна уредба.

Основание за поддържане на информационни масиви от данни в МВР се съдържа в чл. 24, ал. 1 от Закона за Министерството на вътрешните работи (ЗМВР). Съгласно цитираната разпоредба в МВР *„се изграждат информационни фондове и звена за събиране, обработване, систематизиране, съхраняване, анализиране, изготвяне и предоставяне на информация“*. Аналогично правило се съдържа в чл. 28, ал. 1 от Закона за Държавна агенция „Национална сигурност“ (ЗДАНС). Разпоредбата предвижда, че за изпълнение на възложените ѝ със закон правомощия ДАНС *„изгражда, поддържа и ползва информационни фондове“*. Според чл. 29, ал. 1 ЗДАНС *„информационната дейност е дейност по събиране, обработване, систематизиране, съхраняване, анализиране, използване и предоставяне на информация на потребителите от агенцията, на държавни органи, организации, юридически лица и граждани съобразно функционалната компетентност на агенцията“*. Чл. 29, ал. 2 ЗДАНС допуска структурните звена на ДАНС да събират лични данни за изпълнение на задачите и дейностите по ЗДАНС. Законът за Държавна агенция „Разузнаване“ (ЗДАР) също съдържа уредба относно изграждането на информационни масиви. Чл. 32, ал. 1 ЗДАР предвижда, че за изпълнение на поставените пред Държавна агенция „Разузнаване“ (ДАР) задачи държавните органи и ведомствата осигуряват безплатен достъп до информацията, с която разполагат, а съгласно ал. 2 агенцията ползва информация от информационни фондове на МВР, ДАНС и служба „Военна информация“ по начин, не позволяващ разкриване на интереса на ДАР, и при спазване на принципа *„необходимост да се знае“*.

Независимо от това, че посочените нормативни актове допускат създаването на т.нар. „информационни фондове“, никой от тях не съдържа изрична правна уредба, която да позволява вземането на автоматизирани решения с цел профилиране въз основа на обработката на съдържащите се в тях лични данни. Тези фондове не се изграждат и поддържат самоцелно, а само с оглед конкретна правна норма (правно основание за съществуването им) с оглед упражняване на конкретни правомощия. Иначе казано, в действащото законодателство **липсва уредба относно автоматизираното профилиране в сферата на националната сигурност**. При липсата на изрична уредба може да се твърди органите на публичната власт не могат законосъобразно да използват автоматизирани профилиращи технологии. В същото време, предприемането на каквито и да е действия с използването на профилиращи технологии за целите на националната сигурност би могло да застраши правата и свободите на гражданите, демокрацията и устоите на правовата държава като цяло, доколкото към момента законодателството не предвижда адекватни и ефективни механизми за защита срещу използването на такива технологии.

Ето защо, **липсата на изрична правна уредба относно автоматизираното профилиране на този етап на развитие на технологиите съставлява проблем както за органите на публичната власт, така и за индивида и обществото като цяло. Необходимо е внимателно да се обмисли и да се създаде подходяща правна уредба на автоматизираното профилиране за целите на опазване на националната сигурност** – по този начин както публичните органи ще могат да отговорят на най-новите тенденции и предизвикателства в сферата на защита на националната сигурност и ще могат да използват капацитета на новите ИКТ, така и

ще се постигне гаранция за защита правата и свободите на гражданите в правовата държава.

4.2. Законосъобразност и предели на автоматизираното профилиране на лични данни. Допустимост на автоматизираното вземане на решения. Безспорно масиви от данни, създадени и поддържани с цел автоматизирано профилиране, съдържат лични данни по смисъла на Закона за защита на личните данни (ЗЗЛД)³ или данни, които в съвкупност позволяват идентификацията на дадено физическо лице и поради това се разглеждат като лични [9]. Ето защо, основателно възниква въпросът доколко е законосъобразно тяхното обработване. В тази връзка следва да се посочи общото правило на чл. 1, ал. 4, т. 1-3 ЗЗЛД, според което ЗЗЛД се прилага и за обработването на лични данни за целите на отбраната на страната, националната сигурност и опазването на обществения ред и противодействието на престъпността, доколкото в специален закон не е предвидено друго. Съгласно чл. 37 ЗДАНС контролът по защитата на правата на физическите лица при обработването на личните им данни и при осъществяването на достъп до тези данни се упражнява от Комисията за защита на личните данни при условията и по реда на ЗЗЛД. Чл. 3, т. 4 от Наредба № 3 от 24.03.2008 г. за условията и реда за изграждане, експлоатиране, контрол и закриване на информационните фондове на Държавна агенция „Национална сигурност“ въвежда принципа на спазване на правилата за защита на класифицираната информация и на личните данни при изграждане, експлоатиране, контролиране и закриване на информационните фондове към ДАНС. По аналогичен начин ЗМВР (чл. 25, ал. 3) и Инstrukция № 81213-1122 от 12.09.2015 г. за реда за обработка на лични данни в Министерството на вътрешните работи (чл. 2) препращат към ЗЗЛД във връзка с обработката на лични данни. Иначе казано, **правилата на ЗЗЛД са приложими при обработката на личните данни в рамките на посочените ведомства, дори подобна обработка да е с цел закрила на националната сигурност.**

Това разрешение заслужава особено внимание, т.к. на всяка държава членка на Европейския съюз (ЕС) е предоставено правото на преценка дали да прилага общия режим за защита на личните данни при обработка на лични данни в сферата на националната сигурност и отбраната. В България ЗЗЛД намира приложение и в сферата на защита на личните данни. Това от една страна е позитивно, защото гарантира едно много високо ниво на защита на правата на гражданите при обработката на техните лични данни. В същото време обаче трябва да се държи сметка за факта, че тази уредба ще бъде сериозно променена по линия на членството на Република България в ЕС. На 04.05.2016 г. в Официалния вестник на ЕС бяха публикувани три законодателни акта, които формират дългоочакваната реформа в ЕС в сферата на личните данни:

- Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните);
- Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработване-

³ Чл. 2, ал. 1 ЗЗЛД дефинира личните данни като „всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци“.

то на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета;

- Директива (ЕС) 2016/681 на Европейския парламент и на Съвета от 27 април 2016 година относно използването на резервационни данни на пътниците с цел предотвратяване, разкриване, разследване и наказателно преследване на терористични престъпления и тежки престъпления.

Те безспорно ще променят действащата уредба в тази сфера, но дали реформата ще се окаже успешна или не тепърва предстои да се разбере.

Обработването на лични данни според ЗЗЛД е допустимо само при наличието на поне едно от условията по чл. 4, ал. 1, т. 1-6 ЗЗЛД. В този смисъл, нормативно основание за осъществяване на автоматизирана обработка на лични данни с цел профилиране би могло да бъде т. 1 „*обработването е необходимо за изпълнение на нормативно установено задължение на администратора на лични данни*“, доколкото МВР, ДАНС, ДАР и другите компетентни ведомства с подобни функции имат законово задължение да съдействат за опазване на националната сигурност. Друго основание би могло да бъде чл. 4, ал. 1, т. 5 ЗЗЛД – „*обработването е необходимо за изпълнението на задача, която се осъществява в обществен интерес*“, т.к. опазването на националната сигурност безспорно е задача от първостепенен обществен интерес. В същото време обаче личните данни трябва да се събират за конкретни, точно определени и законни цели и да не се обработват допълнително по начин, несъвместим с тези цели (чл. 2, ал. 2, т. 2 ЗЗЛД) и да бъдат съотносими, свързани със и ненадхвърлящи целите, за които се обработват; (чл. 2, ал. 2, т. 3 ЗЗЛД). Ето защо, ако личните данни, които са обект на автоматизирана обработка с цел профилиране, са събрани и се обработват **въз основа на конкретен сигнал и по конкретен случай** с оглед противодействие на подготвяно антидържавно деяние (напр. терористичен акт), подобна обработка би била в съответствие с изискванията на тези общи изисквания на ЗЗЛД. Нещо повече, оправдано е държавните органи да разполагат с правомощия да разследват при наличие на **конкретни** съмнения за подготвяни антидържавни действия да навлизат в личната сфера на всеки гражданин.

По друг начин обаче би стоял въпросът ако данните се събират и обработват не по повод конкретно оперативно-издирвателно мероприятие, а **с оглед цялостна превенция на потенциални деяния, застрашаващи националната сигурност**, или иначе казано за масово профилиране. Ако държавните органи осъществяват цялостно наблюдение, събиране и съхраняване на данните, които всеки един от нас ежедневно генерира при ползване на ИКТ, за да бъдат в състояние да предотвратят едно **бъдещо и абстрактно** поведение, което би застрашило националната сигурност, ще възникнат изключително сериозни въпроси относно зачитането на правото на неприкосновеност на личната сфера на индивида. Това право е прокламирано както на международно (вж. напр. чл. 8 от Европейската конвенция за защита на правата на човека, чл. 7 от Хартата на основните права на човека в ЕС и др.), така и на национално равнище (вж. напр. чл. 32 КРБ, чл. 1, ал. 2 ЗЗЛД и др.). Ето защо, всеобщ мониторинг от страна на държавните органи с цел бъдеща превенция на евентуални заплахи за националната сигурност би поставил под съмнение самите

устои на правовата държава, в основата на която стоят именно човешките права и свободи като най-висша ценност [6].

Подобна обработка би нарушила изискването на чл. 2, ал. 2, т. 3 ЗЗЛД личните данни да бъдат съотносими, свързани със и ненадхвърлящи целите, за които се обработват. Това изискване е особено важно, т.к. специалните закони, приложими в сферата на опазването на националната сигурност, предвиждат възможност да се събират и обработват данни, без лицата, за които се отнасят, да дават съгласие или бъдат уведомявани за обработката (вж. чл. 26, ал. 1, т. 1 и т. 2 ЗМВР, чл. 34, ал. 2, т. 1 и т. 2 ЗДАНС, чл. 28, ал. 1, т. 1 ЗДАР). Ето защо, изискването за пропорционалност на целите, за които се извършва обработването, се явява едно от малкото ограничения пред иначе практически неограничената възможност всеки гражданин да бъде наблюдаван (а данните му – обработвани с цел профилиране) под претекст гарантиране на националната сигурност.

Не на последно място, възниква и въпросът дали е допустимо автоматизирани технологии, работещи без човешка намеса, да вземат решения и да генерират данни, съществено засягащи отделната личност. ЗЗЛД наглед урежда въпроса за допустимостта на автоматизираното вземане на решения. Съгласно чл. 34б, ал. 1 ЗЗЛД решението на администратора е недопустимо, когато има *„правни или други съществени последици за физическото лице“* и *„е основано единствено на автоматизирано обработване на лични данни, предназначено да оценява лични характеристики на физическото лице“*. Тълкуването на посочената разпоредба на практика означава, че вземането на решения, пораждащи съществени правни или други последици за физическите лица (каквито безспорно са решенията, които се вземат в сферата на отбраната, националната сигурност и противодействието на престъпността) само въз основа на **автоматизирано профилиране към момента е забранено в Република България**. Единствените изключения, уредени в алинея 2 на посочената разпоредба, не предвиждат вземането на автоматизирани решения в сферата на защита на националната сигурност. Според тази разпоредба автоматизирано решение би било допустимо, ако: (1) е взето по време на сключването или изпълнението на договор, при условие че подадената от съответното физическо лице молба за сключване или изпълнение на договора е била удовлетворена или че съществуват подходящи мерки, гарантиращи законните му интереси или (2) е уредено в закон, предвиждащ и мерки за защита на законните интереси на лицето (като в момента подобен закон липсва).

Също така, автоматизираното взимане на решения в сферата на националната сигурност поставя и други правни проблеми – така например някои от правата на субектите на данни са неприложими при автоматизирано профилиране в сферата на националната сигурност. Съгласно чл. 28, ал. 1, т. 3 ЗЗЛД при упражняване на правото си на достъп физическото лице има право по всяко време да поиска от администратора на лични данни информация за логиката на всяко автоматизирано обработване на лични данни, отнасящи се до него, поне в случаите на автоматизирани решения по чл. 34б ЗЗЛД. Това правило няма как да се приложи при евентуално профилиране в сферата на националната сигурност, защото би направило съответните технологии и логиката на тяхното функциониране манипулируеми по злоумишлен начин.

На следващо място, според чл. 34б, ал. 3 ЗЗЛД субектът на данните има право да поиска от администратора на лични данни да преразгледа решението, прието в

нарушение на забраната за автоматизирано вземане на решения по чл. 34б, ал. 1 ЗЗЛД. Това право също не може да бъде ефективно упражнено в сферата на автоматизирана обработка за целите на националната сигурност при липса на изрична уредба на автоматизираното профилиране. Необходимо е предвиждането на законодателно равнище на гаранции, даващи възможност подобно решение да бъде преразгледано, като се отчита спецификата на отношенията в сферата на отбраната, националната сигурност и противодействието на престъпността. Подобни гаранции могат да бъдат напр. съдебен контрол върху подобно автоматизирано решение, допълнителното му подкрепяне със събрани по неавтоматизиран начин доказателства и данни и пр. Това не са единствените правни проблеми, които автоматизираното профилиране поражда.

Самото съществуване на забрана за автоматизирано вземане на решения далеч не е лишена от логика. В правната литература е познато делението на допустими и на недопустими за автоматизирано вземане решения (т.нар. формализуеми и неформализуеми знания) [10]. Този въпрос е не само правен, но и морално-етичен. Защото е безспорно, че ако в резултат на автоматизираната обработка едно лице условно казано попадне в категория „заплаха за националната сигурност“, последиците за него и личната му сфера биха били изключително сериозни [1]. Някоя технология, колкото е съвършена да е, не е застрахована срещу допускането на грешки при обработването на данни.

Още повече, че както бе посочено по-горе, автоматизираното профилиране получава само на **прогноза за едно бъдещо поведение или на хипотетичното наличие на дадени факти (т.е. в резултат на него се генерира хипотеза, предположение)**. Интервенирането в правната сфера на дадено лице на базата на автоматизирано решение би влязло в сериозно противоречие със закрепената още на конституционно равнище презумпция за невиновност (чл. 31, ал. 3 КРБ). Факторът „грешка“ също не следва да бъде пренебрегван. Ето защо, необходимо е определени факти, генерирани в резултат на профилирането, да бъдат доказани и с други средства и способности, а не само по автоматизиран път, преди да се предприемат някакви властнически действия спрямо дадено лице с цел опазване на националната сигурност. Това в крайна сметка ще допринесе не само за гарантиране правата на личността, но и за ефективното разходване на военни, полицейски и други ресурси – тяхното използване само въз основа на автоматизирани решения е немислимо, човешката намеса в тази област по никакъв начин не може и не бива да бъде изключвана.

Ето защо, на законодателно равнище *de lege ferenda* ясно трябва да се разпишат механизми, гарантиращи правата на лицата, чиито данни са обект на автоматизирана обработка за целите на защита на националната сигурност, като в същото време се обезпечи и човешката намеса при вземане на решения за предприемане на конкретни действия/ангажиране на ресурси.

5. Заключение

ИКТ и в частност автоматизираното профилиране са в състояние да революционизират концепцията за гарантиране на националната сигурност. Използването му обаче изисква едновременното осъществяване на правни, икономически, технологични, логистични и образователни предпоставки. От правна гледна точка е необходимо въвеждането на правила, които да определят пределите на неговата допус-

тимост с оглед постигане на нужния баланс между суверенното право на всяка държава да опазва сигурността на своите граждани и неприкосновеността на личната сфера на индивида. От икономическа гледна точка е нужен сериозен финансов ресурс за внедряването на съответните технологии. Това поставя и технологичната страна на използването на профилирането – нужно е изработването на подходящи и ефективни алгоритми, които да залежат в основата на профилиращите технологии. Логистичната страна изисква въвеждането на технологии, които отговарят на нуждите, компетентностите и задачите на съответната структура, където ще се прилага профилирането. Образователната страна предполага обучаването на служители, които да са в състояние да работят с технологиите. Едва след като всички посочени аспекти бъдат изпълнени е възможно въвеждането на автоматизираното профилиране като още един инструмент за гарантиране на националната сигурност.

Литература:

1. Pappalardo, J. – NSA Data Mining: How It Works, 2013, достъпно на интернет адрес <http://www.popularmechanics.com/military/a9465/nsa-data-mining-how-it-works-15910146/>, последно посетено на 20.03.2016 г.;
2. Sumathi and Sivanandam – Introduction to Data Mining and its Applications, Springer-Verlag Berlin Heidelberg, 2006, pp. 232–234;
3. Речник на чуждите думи в българския език от А до Я, изд. Наука и изкуство, София, 1978, с. 612;
4. Hildebrandt, M. – Defining Profiling: A New Type of Knowledge?, Chapter 2 in Profiling the European Citizen: Cross Disciplinary perspectives, editors: Hildebrandt, M. and Gutwirth, S., Dodrecht Springer, 2008, p. 40, 45, 50;
5. Čas – Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions, Chapter 7 in Computers, Privacy and Data Protection: an Element of Choice, editors: Gurtwirth, Serge; Pouillet, Yves; De Hert, Paul and Leenes, Ronald, Springer Science + Business Media B.V., 2011, p. 144;
6. Баламезов, Б., В. Киров Ст. Стойчев и др. – Конституция на Република България. Коментар, София, Сиела, 1999, с. 34;
7. Бойчев, Г. – Въведение в правото. Част втора – Философия на правото, Юриспрес, Университетско издателство „Св. Климент Охридски“, София, 2006, с. 66;
8. Dissenting opinion of Mr. Justice Brandeis on 277 U.S. 438 case Olmstead v. United States, decided on Decided: June 4, 1928, достъпно на интернет адрес https://www.law.cornell.edu/supremecourt/text/277/438#writing-USSC_CR_0277_0438_ZD_, последно посетено на 20.03.2016 г.
9. Димитров, Г. – Право на информационните и комуникационните технологии, Част втора: Административноправни и технологично аспекти, Фондация Право и интернет, София, 2014, 167–168 ;
10. Кискинов, В. – Правна информатика, Сиби, София, 2008, с. 324.

НАБЛЮДЕНИЕ НАД ХАРАКТЕРИСТИКИ ЗА СИГУРНОСТ И ТЯХНОТО ПРИСЪСТВИЕ И СТОЙНОСТИ СРЕД БЪЛГАРСКИТЕ УЕБ САЙТОВЕ

Ангел Н. Инков, Димитрина Л. Полимирова

Национална лаборатория по компютърна вирусология – БАН
София 1113, ул. „Акад. Георги Бончев“, блок 8, офис 104

MONITORING SECURITY CHARACTERISTICS OF THE BULGARIAN WEB SITES, THEIR PRESENCE AND VALUES

Angel N. Inkov, Dimitrina L. Polimirova

ABSTRACT: *In the recent years some new methods and techniques have been developed to target popular web application attacks and other to enhance the effectiveness of the HTTPS protocol. This paper aims to check their presence and values in the Bulgarian web sites, and does so in an automatic manner. The collected results give us clear vision about the current state, while the developed methodology would serve for future analysis and monitoring.*

KEY WORDS: *Computer Network Security, Web Application Security, HTTP protocol*

1. Увод

Неразделната вече част на уеб пространството от съвременните средства за информация и комуникация изисква и адекватни методи за защита на неговите потребители срещу възникналите слабости, които прерастват в атаки от рода на XSS, CSRF и Clickjacking, а така също и в регулярни инциденти с доставчици на удостоверителни услуги (Certificate Authorities) и удостоверяващи сертификати [1], [2], [3]. Настоящата работа ще разгледа някои от въведените за противодействие средства в HTTP(S) протокола. Това са хедърите X-Frame-Options [4], Content-Security-Policy (CSP) [5], Strict-Transport-Security (STS) [6] и Public-Key-Pins (PKP) [7]. Използването или неизползването на тези средства от уеб сайтовете се явява тяхна качествена характеристика за сигурност. В допълнение към така базираните характеристики за сигурност ще разгледаме и любопитният въпрос за количеството генерирани cross-site заявки, а също и използването на HTTPS протокола въобще, които несъмнено могат да бъдат погледнати в светлината на характеристики за сигурност. Наблюдението си над тях ще направим сред всички уеб сайтове под главният bg домейн, които са част от класацията за най-популярни уеб сайтове на Alexa [8]. Считано към 17 май 2016 година това са малко над 1100 български уеб сайта, участващи в списък от 1 милион. За тази цел ще извършим автоматизирано събиране и анализиране на HTTP(S) комуникацията при първоначално зареждане на всеки един от тези сайтове, като генерираните HTTP заявки и отговори от което, ще бъдат счестени за достатъчно показателни.

Мотивацията на настоящата работа следва да се търси както в получаването на отговор на въпроса до каква степен избраните средства за защита са

разпространени сред избраното множество от сайтове, а така също и в изграждането на система, позволяваща подобен род изследвания.

2. Характеристики за сигурност

2.1 Характеристики за сигурност, базирани на HTTP хедъри и критерии за оценка

Настоящата точка ще започнем с мотивация на избраните за разглеждането HTTP хедъри.

Content-Security-Policy е относително нов хедър, който предоставя средства за реализирането на допълнителен слой за защита срещу Cross Site Scripting атаки [9]. Пропуските, водещи до успешно извършване на такъв тип атаки, са в топ 3 на най-критичните грешки в сигурността на съвременните уеб приложения, дефинирани от Open Web Application Security Project (OWASP) [10]. Включването на този хедър в отговор на отправена заявка позволява на уеб сървъра да дефинира правила относно това какъв тип ресурси и от къде е позволено те да бъдат заредени в процеса на обработка на получения документ. Съвсем прост илюстративен пример би бил задаването на стойност за този хедър, равна на `"script-src 'self' https://apis.google.com"`, което ще инструктира уеб клиента да зарежда скриптови ресурси само от Origin [11], съответстващ на заявения документ, а така също и от зададеното изрично допълнително местонахождение. По този начин успешно злонамерено включване на скриптово съдържание може да бъде блокирано от изпълнение.

X-Frame-Options е хедър, предотвратяващ Clickjacking атаки, които са базирани на зареждане на атакуваната страница в невидими iframe елементи върху визуално видима част от друга уеб страница. Така например извършена операция по натискане на бутон от видимата част се превръща в операция, извършена върху атакуваната, невидима страница. Стойността на този хедър задава възможностите за зареждане на заявения ресурс в iframe елементи, като X-Frame-Options: DENY забранява това категорично. Лесното му използване и ефективност следва да бъде причина за по-широкото му разпространение сред уеб сайтовете и проверката на това предположение е целта на неговото включване.

Strict-Transport-Security и Public-Key-Pins са хедъри, повишаващи ефективността на използване на HTTPS протокола. Първият от тях инструктира уеб клиента да се обръща при последвали зареждания на заявената страница в рамките на зададен от хедъра период, изрично и единствено използвайки HTTPS, а вторият позволява да се валидира достоверността на веригата от удостоверения на достъпвания чрез HTTPS уеб сайт с цел избягване на нерегламентирано подменяне на удостоверението в следствие на инциденти с доставчици на удостоверителни услуги. За успешен ефект и на двата хедъра се изисква първоначално зареждане на уеб страницата по сигурен канал на достъп, което би гарантирало техните достоверни, неподменени стойности. За да намалат необходимостта от това, в случая на Strict-Transport-Security, много от съвременните уеб клиенти съдържат в себе си списък от сайтове, които следва да бъдат достъпвани единствено по HTTPS.

В контекста на използване на несигурни безжични мрежи за достъп до уеб документи, включването на Strict-Transport-Security би предотвратило

нерегламентираното пренасочване на заявките за работа от HTTPS към HTTP протокола и ще направи атаки от рода на SSLstrip ако не невъзможни то затруднени [12].

От друга страна, Public-Key-Pins позволява на уеб сайтове да заявят коя верига от удостоверения следва да бъде считана за валидна и така да предпазят своите потребители от използването на иначе коректни удостоверения, но издадени извън контрола на техните предполагаеми собственици с цел евентуално прихващане и наблюдение на осъществяваната комуникация.

Критерият за оценка, който ще използваме и ще определи дали дадена качествена характеристика за сигурност, базирана на HTTP хедър, присъства или не в даден уеб сайт, дефинираме на база наличието на съответният хедър в подмножеството от HTTP отговори, породени от първоначалното му зареждане пряко отнасящи се към проверявания първоначален домейн. Наличието например на Strict-Transport-Security в отговор на генерирана cross-site заявка към различен домейн от първо или второ ниво не означава, че проверяваният уеб сайт има положителна характеристика за сигурност базирана на този хедър. За определяне на пряко отнасящите се към проверявания домейн заявки и отговори дефинираме понятието “основен уеб сайт” и за такъв бива счетен домейнът на първата заявка с отговор не влизащ в категорията на пренасочванията. От тук насетне всяка заявка за домейн равен на този на основния уеб сайт или негов под-домейн се счита за пряко отнасяща се. Така в случаите на Strict-Transport-Security и Public-Key-Pins положителен резултат получават уеб сайтовете с наличието на тези хедъри в поне един от отговорите, отнасящи се за заявките, отправени към домейна на основния уеб сайт, а в случаите на Content-Security-Policy и X-Frame-Options, тези с наличието им в поне един от отговорите за пряко отнасящите се заявки. Това минимално разграничение се дължи на необходимостта от използване на Strict-Transport-Security и Public-Key-Pins в top-level домейн за тяхната максимална ефективност.

Важно е да отбележим, че наличието на положителна характеристика за сигурност, базирана на изброените HTTP хедъри по така дефинираните критерии не дава по никакъв начин пълна гаранция за правилното използване на съответния хедър, което не е цел на настоящото разглеждане.

2.2 Други характеристики за сигурност

В допълнение на вече разгледаните характеристики за сигурност ще добавим още една качествена такава, базирана на HTTPS протокола при комуникация с всеки пряко отнасящ се към основния уеб сайт домейн и една количествена, отразяваща броя различни домейни, към които биват изпратени заявки при първоначалното зареждане.

Използването на HTTPS не бива да се счита за привилегия и необходимост на онлайн магазини и сайтове за онлайн банкиране. Извършването на комуникацията по некриптирана връзка позволява нейното елементарно за извършване модифициране, излагайки потребителите и техните уеб клиенти на опасностите, породени от зареждането на злонамерено и неконтролирано съдържание.

Любопитен пример е подмянето и добавянето на допълнителни рекламни елементи в съдържанието на заявените сайтове. [13]

В същото време броят на различните домейни, с които уеб клиентът осъществява връзка при зареждане на дадена страница може да се тълкува като приблизителен брой на различни уеб сървъри, контролирани от различни лица и институции. С увеличаването на този брой нараства и рискът от зареждането на злонамерено съдържание поради увеличеният риск от компрометирането на някои от тези сървъри в следствие на по-голямото множество от различни софтуерни продукти с вече техните характеристики за сигурност.

3. Методология на автоматизирания анализ

Автоматизирането на процеса по определяне на така посочените качествени и количествени характеристики за сигурност бива разделен на две основни части. Първата включва събиране на осъществяваната HTTP(S) комуникация между уеб клиента и уеб сървър при първоначалното зареждане на всеки от разглежданите уеб сайтове, а втората нейното анализиране на база вече дефинираните критерии.

Събирането на HTTP(S) комуникацията е реализирано, използвайки комбинация от уеб клиент и прокси сървър, а именно Firefox версия 4.5 и mitmproxy [14] версия 0.16, като самото прихващане се извършва в прокси сървър. Този избор е ръководен от стремежът да се използва пълнофункционален, съвременен уеб клиент и в същото време реализираният метод да не е тясно свързан с него, както би се получило ако прихващането се имплементира в разширение към браузъра. С цел ускоряване на процеса се използват няколко инстанции на посочения уеб клиент, всяка от които със собствен профил, конфигуриран за съответстваща инстанция на прокси сървър и съответстващ TCP порт. За да се избегне наличието на несвързани заявки в прихванатите в процеса на зареждане на наблюдаваната страница такива, много от параметрите на уеб клиента, контролиращи негови функционалности, предизвикващи външна комуникация, са променени. Така също, за да си осигурим достъп до HTTPS съдържанието, параметри, касаещи функционирането на Public-Key-Pins, биват добавени, както и бива инсталиран допълнителен HTTPS сертификат използван от прокси сървър. Проблемът кога комуникацията по първоначалното зареждане е приключила, а то е такъв поради непрекъснатото изпращане на AJAX заявки от някои сайтове, в настоящото разглеждане е решен по крайно прост начин – на всяка уеб страница са отделени 2 минути, през които се прихващат заявките и отговорите.

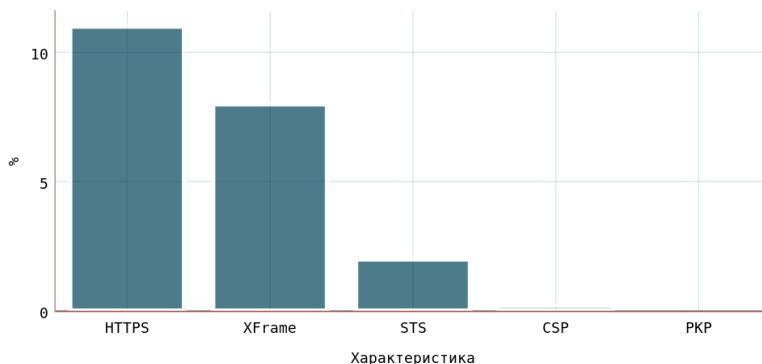
Финалният резултат от тази първа част се изразява в множество от файлове, всеки съдържащ цялата прихваната комуникация за съответния уеб сайт.

Анализирането на така прихванатата информация е реализирано като независим процес, което позволява неговото гъвкаво променяне без това да изисква повторно събиране. Използва се функционалността за скриптово изпълнение върху потокът от данни, предоставена от mitmproxy като се следват дефинираните по-горе критерии за определяне стойностите на качествените и количествени характеристики.

4. Резултати

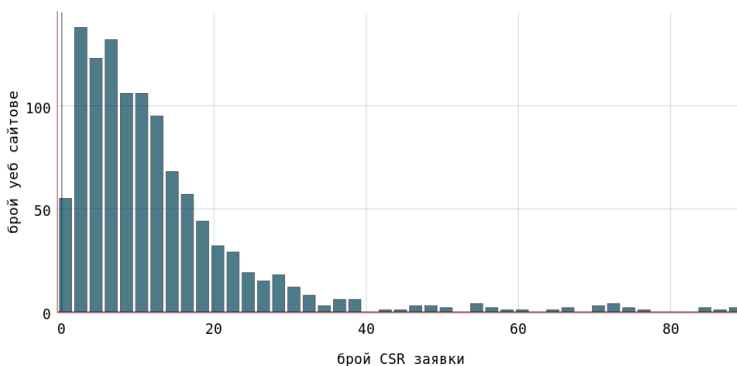
Получените резултати са онагледени в дадените по-долу графики.

Първата от тях представлява процентното отношение на сайтовете, имащи положителна характеристика за сигурност, базирана на споменатите HTTP хедъри, както и базирана на използването на HTTPS протоколът, спрямо общия брой разгледани такива (1100).



Нито един от разгледаните уеб сайтове не използва Public-Key-Pins, а тези, които използват Content-Security-Policy, са точно 2.

Втората графика е хистограма на разпределението на броя cross-site заявки (CSR), генерирани за разгледаните уеб сайтове.



5. Заключение и бъдеща работа

От показаните резултати ясно проличава твърде ниският процент на използване на описаните хедъри сред най-популярните сайтове под bg домейна. Причината за това може да бъде незапознатост с рисковете и средствата за тяхното преодоляване, като с настоящето разглеждане се надяваме да сме помогнали за нейното отстраняване.

Бъдеща насока за работа е разширение и допълнение на разгледаните характеристики за сигурност, както и потенциалната възможност за дефинирането на рейтинг, базиран на тези характеристики, който да бъде достъпен за потребителите и да допринесе за общата, по-широка информираност във връзка с подобрението на сигурността на българското уеб пространство.

Референции:

1. <https://security.googleblog.com/2015/03/maintaining-digital-certificate-security.html>
2. <http://www.symantec.com/connect/blogs/dell-computers-affected-edellroot-self-signed-root-certificate>
3. <https://www.theguardian.com/technology/2011/aug/30/faked-web-certificate-iran-dissidents>
4. <https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options>
5. <https://developer.mozilla.org/en-US/docs/Web/Security/CSP>
6. https://developer.mozilla.org/en-US/docs/Web/Security/HTTP_strict_transport_security
7. https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning
8. <http://s3.amazonaws.com/alexa-static/top-1m.csv.zip>
9. https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29
10. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
11. <http://www.ietf.org/rfc/rfc6454.txt>
12. <https://www.blackhat.com/docs/eu-14/materials/eu-14-Selvi-Bypassing-HTTP-Strict-Transport-Security-wp.pdf>
13. Ad Injection at Scale: Assessing Deceptive Advertisement Modifications (https://www.cs.berkeley.edu/~pearce/papers/injection_oakland_2015.pdf)
14. Mitmproxy (<https://mitmproxy.org/>)

ДЪРЖАВА И СИГУРНОСТ

МЯСТО НА ИНФОРМАЦИОННА СИСТЕМА „ЛОГИСТИКА НА БА“ В СТРАТЕГИЧЕСКОТО УПРАВЛЕНИЕ НА СНАБДЯВАНЕТО В БЪЛГАРСКАТА АРМИЯ

Даниел С. Манолов

didosm@abv.bg

POSITION OF INFORMATION SYSTEM “LOGISTIC BA” IN THE STRATEGIC MANAGEMENT OF SUPPLY IN BULGARIAN ARMED FORCES

Daniel S. Manolov

ABSTRACT: *The report presents the position of information system "Logistics of the Bulgarian Armed Forces" as link between the tactical, operational and strategic management level. This position is of strategic importance for the time for carrying out market research.*

KEY WORDS: *strategic management, information system “Logistic BA”, Bulgarian Armed Forces*

Създадената единна информационна среда в Българската армия е неотменима част от процеса на трансформация, като тя осигурява ефективно функциониране на системата за командване и управление. Изградената информационна среда на Министерството на отбраната и Българската армия се базира на съществуващите сегменти на публичната мрежа „Интернет“ и ведомствената мрежа „Автоматизирана информационна система на Българската армия“ (АИС на БА) за обмен на класифицирана информация, осигуряваща набор от стандартни услуги за общ достъп, както и достъп до вътрешноведомствени информационни системи. В цялостния процес по разработване на информационната система за управление на логистиката на Българската армия, разработването на модел на логистичната система се явява свързващото звено между анализа на текущото състояние на процесите и проектирането на информационната система. Създаването на модела – на основата на настоящата практика и опита на логистичните звена на Българската армия, съвременните тенденции в управление на логистичните процеси и възможностите на информационните технологии да оптимизират и интегрират бизнес–процесите. Осигурява се възможност да се конкретизират изискванията по отношение на информационното им осигуряване или да бъдат модифицирани с оглед на възможностите на информационната система да допълни, развие и промени много от

настоящите, както и да реализира дейности, които не съществуват към настоящия момент.

Промени в Българската армия, произтичащи от изменения на пространствено-времевите параметри на възлаганите ѝ задачи, в съчетание с проблемите, възникващи пред снабдяването ѝ с материални средства в операциите, провеждани на територията на страната и извън нея, вследствие реформирането на логистичната система доведоха до необходимостта от създаване на нова автоматизирана информационна система, която да обхваща всички класове материални средства и да бъде адекватна на съвременната среда в която функционира.

Целта на Информационната система „Логистика на БА“, е повишаване на ефективността на логистичните операции в БА. Това се постига чрез подобряване на информационното обслужване при подготовката на материалния план, управлението, отчетността, отчетта и контрола на разходването на материалните и финансовите ресурси за логистиката на БА.

Мястото на информационна система “Логистика” в стратегическото управление на снабдяването е в свързващо звено между финансовото осигуряване на армията, маркетинговото проучване, управлението на доставките, съхранението и използването на материалните средства и поддържането на единно счетоводство за целия организационен състав на БА.

Основните групи процеси в системата могат да бъдат обобщени по съдържание по следния начин:

- управление на материалните средства;
- планиране и бюджетиране;
- договаряне и закупуване;
- доставка и съхранение;
- използване на материалните средства;
- отчет и отчетност;
- финансов контрол.

При така представените групи процеси се наблюдава, че системата обслужва едновременно и оперативното и стратегическото ниво на управление на снабдяването на Българската армия. Именно тук е мястото на информационна система „логистика на БА“ в стратегическото управление на снабдяването в Българската армия, като свързващо звено между оперативното и стратегическото ниво на управление на снабдяването. Организационно-структурният обхват на системата е избрана така, че да отразява командната йерархия на БА с цел да могат да бъдат изпълнявани логистичните процеси, което включва и тактическото ниво на управление в снабдяването. Съобразно с променящите се потребности на БА, организационният състав на Информационна система “Логистика на БА” може да бъде променян.

Детайлният анализ на изискванията за достъп до информацията показва, че потребители от различните управленски нива от армейската структура имат различни права на достъп до данните и различни права на достъп до функциите. Достъпът до данните е организиран на принципа, че от всяка организационна единица се вижда сечение на данните на подчинените единици надолу по йерархията. Потребителите от високите нива, отговорни за определен вид материални средства, виждат надолу по йерархията данните само за тези групи материални средства.

В глобализиращото се общество информацията, информационните потоци, информационните модели, информационните средства и информационните сили способстват за подобряване на дейностите на ръководителите от различните йерархични нива на отбранителното стопанство. Едновременно с това функционирането на информационна система „логистика на БА“ се съпътства и с редица проблеми, като:

- Недостатъчно количество на номенклатурите от материални средства в базата данни;
- Липса на достатъчно количество данни за характеристиките на материалните средства;
- Неактуална база данни;
- Неправилно определяне на потребители на системата – не са включени необходимите длъжностни лица; не са определени ключовите потребители и не са включени командирите и основните длъжностни лица;
- Неосигуряване и забавяне на техническото развързване на системата;
- Недостатъчна подготовка на потребителите в системата;
- Поради недостатъчно финансиране прекъсване в развитието на проекта.

Инвестициите в информационната система са значителни, следователно и очакваните ползи от нея също са големи. При изясняване на същността на системата бяха очертани някои от ползите, които ще донесе информационната система а именно наличието на информация в реално време за вземане на най-целесъобразните управленски решения и бърз обмен на информацията. Като за стратегическото управление на снабдяването тя осигурява сравнително по голям период от време за извършване на маркетинговото проучване на пазара. В резултат на проведените проучвания се налага извода, че към момента основните ползи от нейното внедряване се състоят в следното:

- оптимизиране на дейностите, свързани с потока на информация;
- на информационната система следва да се разчита като на мощно средство за събиране и обработка на информация;
- елиминиране забавянето, вследствие преминаването на информацията през различни звена;
- осигуряване в по-ранни срокове на необходимата информация за стратегическото планиране;
- прозрачност;
- предоставяне на механизми за управление и контрол.

За определени процеси на Информационна система “Логистика на БА”, се използват бар-кодове, като това са реализация на бар-кодове с непрекъснат достъп и бар-кодове с прекъснат достъп. Сканирането на един код генерира информация за няколко полета от данни, които се попълват със съответните стойности. Така например в използвания софтуер на Информационната система се попълват стойностите на полетата: име на артикул, номер на партида, количество и мерна единица.

При реализация на бар-кодове с непрекъснат достъп софтуерът предоставя възможност за управление на процесите с материални средства, използвайки бар-код устройства. Предпоставките за изпълнение на тези функции са следните: материалното средство от склада да бъде регистрирано в информационната система с бар-код, както и да бъде създадена връзка между бар-кода на производителя и материалните средства от номенклатурния склад. За работа с бар-кодове е необходимо и изграждането на комуникационна структура. Тя включва изграждането на

мрежа в рамките на склад и закупуване на специални бар-код устройства, комбинирани с бар-код принтер. Процесите, в които може да се приложи тази нова технология са следните:

- приемане на материални средства с четене на бар-код;
- проверка за съответствие на рампа за приемане;
- управление на контейнери и идентификационни етикети на стоки;
- дефиниция на под-склад – зони, кодиране на локатори;
- частична и пълна инвентаризация;
- проследяване на срокове на валидност и годност на използване на материалните средства;
- опаковане и слагане в кашони;
- подготовка, обединяване и товарене на пратка от материални средства и др.

При реализацията на бар-кодовете с прекъснат достъп при липсата на постоянен връзка между информационната система и мобилните устройства с бар-код четци се налага устройствата и системата да имат протокол за синхронизация помежду им. Когато мобилното устройство е свързано с информационната система то получава набор от данни за да може да функционира пълноценно. Такива данни са: списъкът номенклатури за текущия склад, идентификатора на потребителя използващ устройството, списък с наличностите, както и други данни. След като първоначално зареденото устройство бъде прекъснато от системата, то преминава в автономен режим. По този начин материално отговорното лице може да извърши редица складови операции като техният резултат се записва в специална база данни. След приключване на работата в автономен режим, материално отговорното лице свързва устройството с централизираната система. Мястото на реализацията на тази връзка може да бъде и извън склада. След синхронизацията, всички данни в мобилното устройство се изтриват и то е готово за следващо първоначално зареждане.

Всички логистични информационни системи използват различни основни и спомагателни параметри на материалните средства и услугите, за да ги идентифицират и управляват материалните средства и услугите по време на целия им жизнен цикъл, а също и процесите по идентифициране и заявяване на потребността от тях - планиране, закупуване, организиране на доставките, складиране и съхранение, последваща експлоатация до снемането им от отчет. Идентифицирането и специфицирането на основните и спомагателните параметри на материалните средства и услуги, заедно със съответните бизнес процеси се явява ключов момент в разработването на всяка логистична информационна система.

В заключение мога да обобщя, че подготовката и структурирането на необходимата база данни, правилното определяне на потребителите на системата, както и актуалната и достоверна информация за наличностите и потребностите, за фактическия ход на материалните потоци могат да разкрият пълната същност на Информационната система” Логистика на БА” и реалните ползи, които тя носи за складовото стопанство на армията. Въпросът за ползите, които носи Информационната система остава отворен, тъй като в годините на нейното прилагане същата ще претърпи развитие и ще донесе допълнителни ползи за складовото стопанство на БА. На този етап основните ползи са: използването на бар-код технологията, поддържането на пълна база данни за параметрите на съхраняваните материални средства, обменът на информация в реално време и генерирането на информационни потоци за нуждите на управлението.

Литература

1. Доктрина за логистика на БА.
2. *Димитров, М.*, Същност и аспекти на приложение на информационна система “Логистика на БА”, Годишник на Факултет “Командно-Щабен” – ВА “Г.С. Раковски”, София, 2007.
3. *Димитрова, С.*, Управление на ресурсите за отбрана в сектора за сигурност, Издателски комплекс при НВУ “Васил Левски”, В. Търново, 2011.
4. *Коралиев, Я.*, Складова логистика, Университетско издателство “Васил Априлов”, Габрово, 2000.
5. Проект Информационна система “Логистика на Българската армия”, Рила Солюшънс ЕАД, София, 2008.

КРИТЕРИЙ ЗА ОЦЕНЯВАНЕ НА ЕФЕКТИВНОСТТА НА УПРАВЛЕНИЕТО НА ОБЩЕСТВЕНИТЕ ПОРЪЧКИ В МИНИСТЕРСТВО НА ОТБРАНАТА

Даниел С. Манолов

didosm@abv.bg

CRITERIONS FOR EVALUATION FOR EFFECTIVENESS OF MANAGEMENT OF PUBLIC PROCUREMENT IN MINISTRY OF DEFENSE

Daniel S. Manolov

ABSTRACT: *The report presents the main criterions for successful conduct of public procurement in the Ministry of defense. Application of these criterions is compared with the conditions of resource environment.*

KEY WORDS: *public procurement, Ministry of defense*

Ефективността е базова характеристика на процеса “Управление на обществена поръчка”. Този ѝ статус предопределя необходимостта от нейното многостранно оценяване. Проблемът може да се разреши с използването на множество критерии и техни показатели. Тези критерии може да се обособят в три основни групи, съдействащи за оценяване на: участник в процеса, съответствието между получения (очаквания) резултат и нормативните изисквания, производителността на компетентните органи и икономическа ефективност на полаганите усилия.

Критериите за оценяване на участниците в процеса са функционално ориентирани. Затова при тяхното определяне и прилагане се налага да бъде отчитана връзката между заявителите на обществената поръчка, ролята на Министъра на отбра-

ната като водещ възложител и способностите на организационните структури да реализират управленските си процедури и операции.

Заявителите на обществени поръчки са не само инициатори на разглеждания процес, но и потребители на постигнатите резултати. По тази причина с решаващо значение е към тях да се прилагат два основни критерия – за оценка на съответствието между направените заявки и обективно необходимите потребности, а така също - между потребностите и нивото на тяхното удовлетворяване.

Първият базов критерий отчита в каква степен заявките на потребителите са адекватни на актуалните потребности на въоръжените сили и на другите елементи на отбранителната система. Затова негови разновидности могат да бъдат критериите отчитащи съответствието на заявките на: мисийно ориентираните приоритети в развитието и използването на въоръжените сили, текущите цели на въоръжените сили, наличните способности, предвижданите организационно – структурни промени, постиженията на военно – техническия прогрес, перспективите за развитие на формиранията и др.

Вторият базов критерий се отнася до финала на разглеждания процес. Най – често се ползва за да бъдат оценени получените крайни резултати. Такива резултати би трябвало да бъдат времето, структурата и параметрите на реализираните доставки и тяхното отражение върху потенциала на формиранията, в които поръчките са реализирани.

Ролята на Министъра на отбраната като възложител също може да бъде оценена на основата на разглеждания критерий. С определящо значение са: приоритетите на отбранителната и по – конкретно на политиката за развитие на оперативните способности, нивото на генериране и ръководство на необходимите финансови и организационни ресурси, съдействие за правно – административна, комуникационна и научно – образователна поддръжка на разглеждания процес, равнището на взаимодействие с другите ведомства на национално ниво и с партньори от други държави и многонационални организации.

Критериите за оценка способностите на органите, които функционално са ангажирани с управлението на обществената поръчка характеризират експертния аспект на разглеждания процес, като тези органи се явяват и посредници между страните по съответната обществена поръчка.

Признаците, по които може да бъдат оценени т.н. посредници в разглеждания процес също са различни. Те зависят от ролята на организацията, която се привлича за изпълнение на услуга, пряко свързана с изпълнението на всяка от обществените поръчки. По тази причина се налага те да бъдат съобразени със спецификата, относителната тежест и времето за реализиране на съответната консултантска, правна, търговска, застрахователна, за гаранция, рекламна или друга услуга.

Критериите за оценка на съответствието между получените резултати и изискванията на нормативните документи се налага да бъдат подредени по базови функционални сектори на практиката. Такива сектори са отбранителният, правният, научно – технологичният и др.

Основа за дефиниране на критериите в отбранителния сектор са изискванията за съответствие между постигнатите и необходимите способности:

- по компоненти на въоръжените сили, времето и мястото за тяхното използване;

- за оперативна съвместимост в национален (съюзен или коалиционен) формат;
- за правно–административна, комуникационно–информационна, образователна, научна и социална поддръжка;
- за реализиране на разглеждания процес и т.н.

Ще акцентирам върху две от посочените изисквания и критериите, които показват в каква степен те са удовлетворени - за съвместимост и за осигуреност.

Критерият “За оперативна съвместимост на изделията” е инструмент с все нарастваща значимост. Причината за това е необходимостта доставяните изделия да бъдат съвместими с използваните както на национално, така и на съюзно (коалиционно) равнище. По тази причина се налага да бъдат отчитани множество стандарти, които заявителите трябва да афишират, а доставчиците - да удовлетворяват.

Посочените аргументи все по-масово се използват като база за коопериране на производители от съюзнически и партниращи държави. Така кръгът от необходими доставки съществено се разширява, а това означава, че и организацията на тяхното управление също се променя с високи темпове. Показателни в това отношение са интеграционните процеси в рамките на НАТО и ЕС.

Критериите отчитащи степента на осигуряване на отбранителните потребности са инструмент за оценяване равнището на подготовка на държавата за участие във военен конфликт или криза с висока обществена значимост. Същевременно е необходимо да се има предвид, че прилагането им в съвременни условия позволява да се оцени и степента на осигуряване на поръчки за националната икономика, укрепване на евроатлантическото икономическо сътрудничество и на връзките с други партньори.

От изложеното до тук, става ясно, че е налице възможност да бъдат оценени:

- степента на интегриране на фирмите от Българската отбранителна индустрия;
- способността им да участват в тръжните процедури провеждани от Агенцията на НАТО по поддръжката и снабдяването (НАМСА) и Агенцията на НАТО за консултации, командване и контрол (NC3A);
- да участват в провежданите процедури и се включат като подизпълнители в проектите на ЕАО.

Не по–малко важна е възможността да се определи в каква степен Република България участва в удовлетворяване на отбранителните потребности на съюзите, в които членува. Друг аспект на посочената е възможността да бъде дефиниран темпът, с който се реализира политиката на ЕС за отваряне на националните пазари за отбранителни доставки и за свободно конкуриране на потенциалните доставчици.

Критериите за съответствие на нормативните изисквания също са изключително разнообразни. С определящо значение са тези, които позволяват да се измери качеството на доставеното изделие или услуга, а така също нивото на съответствие между постигнатите резултати на изискванията за законност, прозрачност, хуманизъм и т.н.

Критериите за определяне качеството на услугите (дейностите), които предлагат (извършват) компетентните ръководно – експертни органи също са изключително разнообразни. По тази причина ще акцентираме на принципно важните и на основния ред за тяхното прилагане.

Критериите от разглежданата група се отнасят до параметрите на всяка услуга (дейност). Такива са критериите за определяне на:

- времето и мястото за реализация; сложност, значимостта и новостта на всяка услуга;
- наличието на рискове;
- технологична обвързаност в рамките на цялостния процес;
- степен на изпълнимост;
- методи и форми на провеждане;
- участващи лица и технически системи;
- повтораемост и др.

Отчитайки тяхното многообразие ще акцентирам само върху два специфични критерия - за прозрачност и за секретност на услугите (дейностите), които компетентните ръководно – експертни органи предлагат.

По-важните показатели за установяване на тази ефективност на дейностите по обществените поръчки са:

- разходът на работно време за обслужване на всяка процедура (оперативност);
- броят на проведените процедури, сключените договори, изпълнените договори, рекламациите по приключили договори.

Критериите за законност са водещи, като те позволяват да се постигне единство в усилията на обществото в отбранителния сектор и в областите свързани с удовлетворяване на неговите потребности. Тази му роля се реализира чрез анализа на съответствието на реалните действия с постановките на регламентиращите документи, в качеството им на водещ фактор за регулиране на обществените поръчки.

Критериите за оценка на прозрачността на процеса “Управление на обществена поръчка” са предпоставка за постигане на по-добра отчетност, отговорност и ефективност. Прилагането им предполага пълен достъп до информацията на всички етапи на процеса по подготовка и вземане на управленски решения. Най-същественото е, че прозрачността е средство срещу един от най-тежките пороци на управлението – корупцията.

Стойностите на критериите от разглежданата група могат да бъдат определени като съотношение между публикуваната информация и реално ползваната при реализацията на всяка от обществените поръчки. На основата на това съотношение става възможно да се повиши мотивацията на изпълнителите и увереността им, че действат правилно, а така също и да им се осигури по-висока обществена и бизнес подкрепа. По тази причина разглеждам прозрачността като база за оценяване на социалните, моралните и правните аспекти на ефективността в рамките на изследваната проблемна област на управленската практика.

Критериите за секретност са основа за измерване правно – административните аспекти на разглежданата ефективност. Изразява степента на достъп на участниците в разглеждания процес до класифицирана информация и с необходимостта да бъдат прилагани определени мерки за нейната защита. Измерва се с набор от конкретни показатели. Индустриалната сигурност в предприятията изпълняващи обществени поръчка за отбранителния сектор е свързано с тяхната икономическа стабилност и със съответствието на ръководещите ги органи на изискванията за сигурност на информацията.

В съответствие с изложеното, определен кръг от длъжностни лица придобиват правото на достъп до информацията отнасяща се до реализацията на специални поръчки и се запознава с последствията ако нарушат изискванията на Закон за защита на класифицираната информация. Прилагането на критерия прави възможно поточно да се оцени практиката или да се предвидят действени мерки по запазване на елементи от разглеждания процес в тайна, ако се налага и да подобри неговата устойчивост и интензивност. Същевременно се налага да посочим, че е налице възможност критерият да бъде използван неправилно и така да се увреди прозрачността на процеса и да се игнорира неговото конкурентно начало, а следователно и да се понижи ефективността му.

Критериите характеризиращи производителността на положените усилия от ангажираните ръководители и експерти са мерило и за определяне на тяхната ефективност. Поради това те са средство за оценяване, най-вече на дейността на органите, които генерират и ръководят реализацията на обществените поръчки.

В качеството си на такова средство, разглежданите критерии позволяват относително точно да бъдат измерени и оценени:

- съответствието между елементите на разглеждания процес и органите, които трябва да ги реализират;
- връзките между посочените органи в линеен, функционален и информационен аспект;
- механизмите разкриващи спецификата на полаганите усилия от ръководните органи и равнището на тяхната професионална компетентност и мотивация;
- перспективните потребности от експертна подкрепа и темповете на развитие на всяко от компетентните звена;
- организацията на работата във ведомствените и на аналогичните звена на съюзно равнище;
- параметрите на предлаганите и очакваните експертни предложения;
- заявените, утвърдените и изпълнените обществени поръчки за определено време и т.н.

Посоченото дава основание да се приложат различни подходи за оценяване на връзките между резултатите на съответната експертна структура и нейните цели, и дейност.

Критериите за оценка на икономическата ефективност също са много разнообразни. Те приоритетно визират съотношението „разходи-ползи”. Отчитайки важността на изложеното, се налага да подчертаем, че определянето и оценяването на необходимите или на направените разходи е многофакторно обусловен и затова трудно разрешим проблем. Посоченото обстоятелство предопределя необходимостта да бъдат прилагани критерии за измерване на специфичните и общите и разходи.

Специфичните разходи и тяхната относителна тежест са водещ аспект на проблема. Те могат да бъдат определени с помощта на показатели за разход на: труд на всички ангажирани с управлението на обществените поръчки в Министерство на отбраната, консултации и други услуги на външни организации, консумативи и други материали, комуникационна и енергийна поддръжка, такси и застраховки, пътни и други социални потребности. От значение е също така възможността посочените показатели да бъдат определени за всички етапи, процедури и операции на разглеждания процес. Така става възможно да се определи относителната те-

жест на всеки частен разход и да се намерят възможности за оптимизиране на общите.

Необходимо е да се има предвид, че платената цена произтича от обстоятелството, че разглежданите поръчки се правят от името и в интерес на обществото. Затова при оценяване на реда за тяхното изпълнение се налага по достойнство да бъде отчитана сложността на труда на всеки от служителите в експертните звена в министерство на отбраната, тяхната производителност и качеството на разработените от тях документи или извършени услуги в подкрепа на овластените водещи ръководители или други потребители (клиенти). При разрешаването на проблема е необходимо да се взема предвид, че трудът на непосредствено ангажираните ръководители и експерти е високо интелектуален, свързан е с големи отговорности и допринася за рационализиране на разглеждания процес по всяка от функционално обособените управленски вериги.

Ефективността на управлението на ресурсите освен във функционален план, може да се разгледа във времеви, като наслагващ се процес. За да се получи синергичен ефект, се налага ефективността да бъде отчитана на всеки един етап от процеса “Управление на Обществена поръчка”. Този ефект зависи от условията на реализация на процеса. В един момент определящи са цената, а в друг – сроковете за изпълнение, качеството на продукта и др.

Приключвайки по проблема се налага да подчертаем, че оценката на ефективността на управлението на обществена поръчка е комплексен проблем. Затова при неговото разрешаване се налага да бъде взето предвид влиянието на поне два фактора.

Първият е необходимостта от пестеливото изразходване на основните ресурси. Опитът показва, че само при възлагане на обществена поръчка по-добре планираната процедура може да се постигне високоефективен краен резултат. Това означава и интегриране на подходите за оценка функционалната и икономическата ефективност на компетентните ръководни и експертни органи.

Не по-малко важно е да се вземе предвид, че ефективността не е само икономичност. Тя е симбиоза между икономичност и полезност. Изпускането на полезността обезсмисля всяка дефиниция за ефективност.

Опитът показва, че не винаги е правилно да се приемат като оптимални най-малките разходи за създаването на определен продукт. Не бива да се забравя, че малките разходи са синоним на бедност и ниско качество, че може да се произведе много икономично един продукт и той да бъде безполезен за отделно формиrowание или за Въоръжените сили.

Вторият фактор е свързан с това, че ефективността трябва да се разглежда като интегритет между: вътрешна и външна; функционална, икономическа и социална; текуща и последваща. Само върху тази разширена основа може да се търсят реалните проекции на възпроизводството на публичното благо, наречено сигурност.

Планирането и разпределението на ресурсите на ведомствено ниво е свързано с планирането и оценяването на способностите на Въоръжените сили – съществуващи и бъдещи; оперативното планиране в отговор на възможностите за възникване на кризи и възможност за избор на вариант за действие; планиране на потребностите съобразно финансовите ограничения и ресурсното планиране.[1]

В заключение мога да кажа, че е от решаващо значение при анализа на ефективността в разглежданите аспекти да се правят изводи и за общото състояние на Въоръжените сили, и на Страната.

Литература:

1. *Димитрова, С.*, Мениджмънт на ресурсите в динамично променящата се среда на сигурност, Русе, 2014г., стр.56
2. *Павлова, М. и колектив.* Наръчник по обществени поръчки. С., ИК ”Труд и право”, 2005.
3. *Шаламанов, В. и Тагарев, Т.* “Прозрачност при управлението на отбранителните доставки”, Сдружение “Джордж С. Маршал – България”, София, 2003.
4. Доктрина за логистика на БА.
5. Закон за обществените поръчки.
6. Закон за отбраната и въоръжените сили.

ОСНОВНИ НАПРАВЛЕНИЯ В ПОДГОТОВКАТА И ОРГАНИЗИРАНЕТО НА ПРОЦЕДУРА ЗА ВЪЗЛАГАНЕ НА ОБЩЕСТВЕНА ПОРЪЧКА В МИНИСТЕРСТВО НА ОТБРАНАТА

Даниел С. Манолов

didosm@abv.bg

MAIN DIRECTIONS INTO THE PREPARATION AND ORGANIZATION OF THE PROCEDURE FOR PUBLIC PROCUREMENT IN MINISTRY OF DEFENSE

Daniel S. Manolov

ABSTRACT: *The report presents main directions into preparation and organization for public procurement in Ministry of defense, taking account the peculiarities of the environment planning and possible risks. The procedure brings significance of social responsibility.*

KEY WORDS: *public procurement, Ministry of defense*

Разглежданата проблематика е на примера на Министерство на отбраната, като набелязаните направления в подготовката и организирането на процедура за възлагане на обществена поръчка могат да бъдат отнесени към всички ведомства, агенции и организации в държавния сектор.

Организирането на реда за възлагане на всяка обществена поръчка е процедура водеща до създаването на предпоставки за постигане на желан краен резултат. Тя

се реализира от овластения експерт в Министерство на отбраната, който функционално е ориентиран към съответния клас поръчки.

Целта на процедурата е реализиращите я експерти да разработят документи и подходи, на чиято основа следващите действия да бъдат проведени своевременно, организирано и резултатно. Опитът показва, че тази цел трябва да бъде постигната колкото е възможно по-рано, за да се осигурят оптимални условия за възлагане на съответната поръчка.

От посочената цел, за водещия експерт (екип от експерти) произтичат множество задачи. С определящо значение са:

- подобряването на личната подготовка;
- анализът на поръчката и на възможните условия за нейното възлагане;
- изясняване изискванията на заявителя и на регламентиращите документи;
- отчитане на минал опит и информацията за пазарната ситуация;
- определяне типа на налагащата се възлагателна процедура;
- разработване на необходимата документация, и на съображения за нейното използване.

Посочените задачи се изпълняват в рамките на съвкупност от дейности. В тази връзка ще обърне особено внимание на възможностите за рационализиране на реда и времето за тяхното изпълнение.

Личната подготовка е първа предпоставка за успех. По тази причина тя трябва да бъде ориентирана към цялостно осмисляне на реда за възлагане на съответната поръчка и да включва усвояване на теоретичните и правно – административните основи на налагащата се дейност.

Анализът на условията за изпълнение на възложената експертна задача предполага да бъде отчетено влиянието на факторите, които непосредствено влияят на процеса. С основно значение е да се изяснят:

- какъв е предметът на поръчката;
- кой е възложителят и неговите специфични изисквания;
- заявката комплектована ли е с необходимите поддържащи документи;
- какви са параметрите на поръчката и сроковете за доставка;
- какви са изискванията за приемане на готовия продукт и при необходимост кой ще проведе налагащите се изпитания;
- на кого и къде трябва да бъде представено изделието;
- правно-административните разпоредби регламентиращи възлагането;
- актуалното състояние на пазара и как в него се отразява опита с възлагането на минали поръчки от същия тип;
- връзката между разглежданата и другите възложени поръчки.

Изискванията на заявителя и на регламентиращите документи са базова рамка за определяне на експертната позиция при разработване на документите необходими за възлагане на всяка конкретна поръчка. По тази причина се налага да бъдат идентифицирани, точните и подразбиращите се параметри на искания предмет или услуга. При анализа на параметрите е необходимо да се изясни в каква степен те съответстват на стандартните изисквания, включително чрез провеждането на консултации и искане на допълнителни становища.

Анализът на опита дава информация за положителните и отрицателните аспекти на практиката. На основа на него става възможно по-бързото и по-доброто разк-

риване на потенциалните рискове и да се намерят възможности за тяхното минимизиране.

Изборът на процедура за възлагането на обществена поръчка зависи от познаването на нормативната уредба, спецификата на управленския подход към проблема, параметрите на предмета на поръчката, налагащите се ограничения относно изпълнителите на поръчката и др.

Въз основа на събраната и обработена информация се формира определена позиция и след съгласуването ѝ с овластените лица се определя вида на процедурата и се пристъпва към разработване на конкурсната документация.

Разработването на необходимата документация е отражение на всичко извършено. То има своите концептуални, организационни и функционални аспекти.

Концептуалният аспект на проблема разглеждаме като израз на позицията на експертите спрямо ефективността на подготвяната сделка. Традиционно ефективността се възприема като оптимална, когато цената на продукта е минимално възможната, а качеството ѝ – максимално високо. Опитът показва, че постигането на такава ефективност е невъзможно. Затова считаме за целесъобразно, при формиране на посочената позиция:

- приоритетно значение да се отдава на параметрите за качество и на сроковете за доставка на желаните продукти в заявеното количество;
- да се създават условия за лоялна конкуренция, като средство за минимизиране цените на желаните продукти. Необходимо е да се има предвид, че в условията на пазарно регулиране определянето на взаимно-изгодната цена е основа за сключване на договор за изпълнение на конкретна поръчка. Затова е и приоритетна цел на всяка от страните.
- по-пълно да се отчита богатият опит на нашите съюзници. Вече посочихме, че в ЕС основание за оценка на една оферта като най-изгодна се приемат: срокът за доставяне и за поддържане на стоката; текущите и разходите по компонентни дейности; ценовата ефективност; качеството на изделието или услугата; естетичността и функционалността на продуктите; техническите им предимства; аспектите на след продажбеното обслужване и на техническата помощ; наличието на резервни части и сигурност на доставките на приемлива обща цена.
- приоритетно значение да се отдава на прозрачността на всяка сделка. Така поръчката става достъпна за всички потенциални изпълнители на обществената поръчка, предопределя по-голяма конкуренция между потенциалните изпълнители и предпазва от евентуални нарушения.

Приоритетното значение което отдаваме на прозрачността на всяка една сделка обект на обществен поръчка се определя от социалната отговорност, която носим по нейното законосъобразно и целесъобразно изпълнение.

Социалната отговорност е такова поведение, което е реакция на преобладаващите в обществото в съответния исторически момент, социални норми, дейности, стойности и очаквани резултати. Тя надхвърля рамките на закона и представлява поемането на обществени задължения от страна на организацията извън изискванията му. [1]

Основно значение при организирането на обществената поръчка има и определянето на експертите и техните взаимоотношения. Опитът показва, че формирането на експертен екип е целесъобразно при разработване на множество документи за кратко време. Редовното прилагане на този подход позволява:

- да се подобрят производителността на труда, специализацията на членовете на екипа и качеството на тържните книжа;
- по-пълно да се прилагат актуалните правила и стандартни изисквания за оформяне на документите.
- да се компенсират част от трудностите произтичащи от липсата на пълни данни в голяма част от постъпилите заявки.
- да се усвои единна технология за изпълнение на налагащите се субдейности.

Технологичният аспект отразява последователността в която се изпълняват възложените задачи. За постигане на желания ефект в Министерство на отбраната е разработен алгоритъм. Той онагледява трудния път за изготвяне на един документ от структурите, които го съгласуват преди утвърждаването му от възложителя.

Алгоритъмът определя следната последователност на работа:

- експертите от Министерство на отбраната осигуряват административните, техническите и правните данни, необходими за създаване на конкурсната документация. Тържните документи се подготвят за всяка обществена поръчка, като се проявява стремеж офертите да отговарят на посочените потребности на МО и БА.
- в съответствие с ограниченията произтичащи от Закона за защита на класифицираната информация, експертите искат становището от съответните органи и да се направи преглед на секретността от Служителя по сигурността на информацията. Така става възможно своевременно да се изясни, кои от необходимите отбранителни продукти представляват държавна тайна и с какви мерки за сигурност трябва да бъде съпроводена тяхната доставка и реализация.
- на основата на резултатите от извършената подготовка от името на Министъра на отбраната се стартира операцията по обявяване на обществената поръчка.

Редът за обявяване на разглежданите процедури се определя в зависимост от техните финансови прагове на национално и на европейско ниво.

Процедурата за възлагане на обществена поръчка трябва да отговаря на стандартните договорни формати и предписани процедури за централизирано снабдяване. Преди стартирането ѝ е необходимо потвърждаване на финансовите средства за съответната позиция от Единния финансов план за материално-техническо осигуряване.

Разглежданата процедура трябва да включва разработване и представяне по определен ред на изходно задание, спецификации, чертежи и планове, изисквания за гаранция на качеството и изпитанията, график на изпълнение или доставки, списък на необходимите документи, административни изисквания и всички приложими условия, включително за оценка на офертите и критериите за избор.

Законът предвижда оценка на офертите по най-ниска цена или икономически най-изгодната оферта, съобразно предварително обявения критерий. Когато критерият за оценка на офертите е икономически най-изгодната оферта, възложителят посочва в обявлението показателите, относителната им тежест и методиката за определяне на комплексната оценка на офертата.

Предпочитаната процедура на МО е избор на изпълнител на обществена поръчка въз основа на икономически най-изгодната оферта. Изборът на изпълнител на база "Най-изгодна оферта" се осъществява на основата на методика базирана на определени критерии за оценка и класиране. Методиката трябва да съдържа пока-

затели по всеки критерий (качество, цена и техническите предимства, срок на изпълнение, естетически и функционални предимства, ремонти през гаранционния период, техническа поддръжка, поддръжка след гаранционния период и др.) и указания как да се направи оценката и класификацията. При наличие на възможности е добре да бъде разработен софтуерен продукт, с който да се облекчи работата на експертите.

Експертите отговарящи за провеждането на отделните дейности изготвят проект на заповед на възможните членове на Комисията за оценка и избор на изпълнител, критерии за оценка и система за отчитане на резултатите, с цел подкрепа на методологията за официалното класиране за избор на най-добър изпълнител.

Комисията за оценка и избор на изпълнител се назначава със заповед на министъра или упълномощен от него зам.-министър на отбраната. В хода на дейността се попълват индивидуални оценъчни картони, които включват критериите и начина за оценяване на офертите, и избор на изпълнител. Опитът показва, че когато Изходното задание и спецификациите са коректно зададени и представени в офертата (според риска на разходите на очакваната дейност), процесът за избор на изпълнител има най-голяма вероятност да достигне целите на Министерство на отбраната - най-добра цена на договора на обществената поръчка.

В своята работа комисията трябва да следи за приемливостта на цената на офертата. Редно е предложена цена да се сравнява чрез независима оценка на разходите, с цел определяне на разумна цена по време на преговорите за възлагане на обществена поръчка. Ако има открити грешки кандидатът може да оттегли, но не и да промени офертата си.

Работата на комисията приключва с протокол или доклад. Член на комисията, който не е съгласен с мнозинството има право да подпише протокола с “Особено мнение” и писмено да изложи мотивите за несъгласието си.

Въз основа на съставения протокол от комисията за избор на изпълнител, възложителят с мотивирано решение определя класирането на кандидатите и кандидата избран за изпълнител на обществената поръчка.

В заключение мога да обобща, че изборът на методика за оценяване и определянето на критериите за оценяване, както и тяхната тежест са в основата на подготовката на изпълнението на процедура по обществена поръчка и са ключът към нейният успешен финал.

Литература

1. *Петрова, Е.*, Основи на управлението, В.Търново, 2013, стр.137
2. *Павлова, М. и колектив.* Наръчник по обществени поръчки. С., ИК ”Труд и право”, 2005.
3. *Шаламанов, В. и Тагарев, Т.* “Прозрачност при управлението на отбранителните доставки”, Служение “Джордж С. Маршал – България”, София, 2003.
4. Доктрина за логистика на БА.
5. Закон за обществените поръчки.
6. Закон за отбраната и въоръжените сили.

ДОГОВОРЪТ ЗА ВОЕННА СЛУЖБА СПОРЕД ДЕЙСТВАЩОТО БЪЛГАРСКО ЗАКОНОДАТЕЛСТВО

Силвия Д. Салтирова-Радкова

*Шуменски университет „Епископ Константин Преславски“, гр. Шумен
Педагогически факултет
e-mail: ssaltirova@gmail.com*

THE MILITARY SERVICE CONTRACT ACCORDING TO THE BULGARIAN LEGISLATION

Silviya D. Saltirova-Radkova

ABSTRACT: *The present report aims to clarify the nature of the military service contract according to the Bulgarian legislation as a special kind of contract with a mixed administrative and employment law nature. The main issues discussed in the report are connected with the occurrence of military service relationship, the amendment of the military service contract and its termination.*

KEY WORDS: *contract, military service, national security, amendment, termination*

Съгласно действащото българско законодателство военната служба се изпълнява от лица, отговарящи на определени изисквания – военнослужещи. За да стане едно лице военнослужещ, е необходимо да бъдат извършени определени правни действия. Най-важното и основното е сключването на договор за военна служба.

Като всеки вид договори и договорът за военна служба по своята правна характеристика представлява съглашение между две лица, с което се уреждат определени отношения.

Съгласно чл. 133, ал. 2 от ЗОВСРБ [1] военната служба е професия, а съгласно чл. 133, ал. 1 от ЗОВСРБ „Военната служба е държавна служба с особено предназначение [...]“. Ето защо договорът за военна служба по своята юридическа същност е особен вид трудов договор, който обаче урежда специфичен вид правоотношения. Спецификата на тези правоотношения се поражда от особената функция, която изпълняват военнослужещите – да осъществяват въоръжена защита на страната и да осигуряват националната сигурност. Ето защо договорът за военна служба може да се определи като особен вид договор със смесен административно-трудов характер.

Историческо развитие на договора за военна служба

През 1958 г. беше приет Закона за всеобщата военна служба в Народна Република България (ЗВВСНРБ) [2]. Съгласно неговите разпоредби военната служба е задължителна за всички граждани на страната без разлика на раса, народност, вероизповедание, образователен ценз, социален произход и положение. Чл. 9 от ЗВВСНРБ военната служба се състои от действителна военна служба и служба в

запаса. На действителна военна служба се намират маршалите, генералите, офицерите, свръхсрочнослужещите старшини и сержанти, приети за кадър във Въоръжените сили, и всички срочно служещи от сержантския, войнишкия и курсантския състав, които служат редовната си военна служба. Срочнослужещи са служещите редовната си военна служба от сержантския и войнишкия състав, а свръхсрочнослужещи – приетите на щатна служба след изслужване на редовната военна служба. Законът обаче не поставя изисквания за сключване на някакъв вид договор или издаването на нарочна заповед (с изключение на случаите по чл. 13, б. „г“ и „д“).

През 1995 г. Законът за всеобщата военна служба в Народна Република България беше отменен с преходните и заключителни разпоредби на новия Закон за отбраната и въоръжените сили на Република България (ЗОВСРБ) [3]. С този закон за първи път в българското законодателство беше въведен договора за военна служба – тогава наричан „договор за кадрова военна служба“. Условията и редът за сключване, изменение и прекратяване на договора за кадрова военна служба, обаче, са уредени в Правилника за кадрова военна служба [4].

През 2009 г. беше приет сега действащият Закон за отбраната и въоръжените сили на Република България (ЗОВСРБ), който въведе термина „договор за военна служба“.

Правна уредба на договора за военна служба

За разлика от трудовия договор, който се урежда в Кодекса на труда (КТ) и заповедта за възникване на служебното правоотношение по Закона за държавния служител (ЗДСл), правната уредба на договора за военна служба се съдържа в ЗОВСРБ, както и в Правилника за прилагане на Закона за отбраната и въоръжените сили на Република България (ППЗОВСРБ) [5].

Съгласно разпоредбата на чл. 134а, ал. 1 от ЗОВСРБ, правоотношението по изпълнение на военна служба възниква въз основа на договор за военна служба. Задължителното съдържание на договора е посочено в чл. 134а, ал. 2 от ЗОВСРБ и включва:

- ✓ наименованието на длъжността, на която военнослужещият се назначава;
- ✓ съответстващото й военно звание;
- ✓ срокът на службата;
- ✓ условията за обучение и повишаване на квалификацията;
- ✓ условията и редът за кариерно развитие;
- ✓ правата, задълженията и отговорностите на страните по договора.

Провеждане на конкурс

Специфика разкрива приемането на военна служба на лица, завършили граждански средни или висши училища в страната и в чужбина. Съгласно разпоредбите на Закона и на Правилника, те се приемат на военна служба след провеждането на конкурс (чл. 144, ал. 1 от ЗОВСРБ и чл. 4, ал. 1 във вр. чл. 2, т. 3 от ППЗОВСРБ). Конкурсът се обявява със заповед на министъра на отбраната или на оправомощено от него длъжностно лице, в която задължително се определят:

- ✓ длъжностите, за които се организира конкурсът;
- ✓ длъжностното лице, отговорно за провеждането на конкурса;
- ✓ условията и редът за провеждане на конкурса.

След издаването на заповедта задължително се публикува обява, която съдържа задължително следната информация:

- ✓ наименованията и броя на вакантните длъжности;
- ✓ изискванията за тяхното заемане;
- ✓ изискването се ниво за достъп до класифицирана информация за длъжността;
- ✓ населеното място, където се намира формирането (структурата), и неговия военнопощенски номер;
- ✓ длъжностното лице, отговорно за провеждането на конкурса;
- ✓ начина на провеждане на конкурса;
- ✓ необходимите документи, които кандидатите трябва да представят;
- ✓ мястото и срока за подаване на документите.

Обявата задължително се публикува на интернет страницата на Министерството на отбраната, както и в Агенцията по заетостта.

Длъжностното лице, отговорно за провеждането на конкурса, назначава комисия за допускане до участие и комисия за провеждане на конкурса. За разлика от провеждането на конкурс по Закона за държавния служител [6], където е предвидено създаването само на една комисия (която първо допуска кандидатите и след това провежда самия конкурс), ППЗОВСРБ предвижда създаването на две отделни комисии с различни по своя характер задачи:

Комисията за допускане до участие в конкурса:

- ✓ извършва проверка на подадените документи;
- ✓ допуска до конкурса кандидатите, които отговарят на условията за конкурса;
- ✓ връща документите на кандидатите, които не са допуснати до участие в конкурса, като мотивира отказа.

Комисията за провеждане на конкурса, от своя страна:

- ✓ провежда конкурса при условията и по реда, предвидени в заповедта на министъра на отбраната;
- ✓ изготвя протокол, в който класира кандидатите според показаните резултати;
- ✓ писмено уведомява кандидатите за резултатите от класирането и връща документите на некласираните кандидати.

Подобно на предвиденото обжалване на конкурсните резултати по ЗДСл. и ППЗОВСРБ предвижда, че некласираните кандидати имат право на жалба пред длъжностното лице, отговорно за провеждането на конкурса, в 7-дневен срок от уведомяването. Длъжностно лице трябва да се произнесе в 14-дневен срок от получаването на жалбата, като решението му е окончателно (чл. 6, ал. 4 от ППЗОВСРБ).

Сключване на договор за военна служба и приемане на военна служба след провеждане на конкурс

Министърът на отбраната или оправомощено от него длъжностно лице сключва договор за военна служба с лицето, спечелило конкурса. Договорът се сключва след изтичането на сроковете за обжалване и при наличие на разрешение за достъп до класифицирана информация със съответното ниво на класификация, изисквано за длъжността (чл. 7, ал. 2 от ППЗОВСРБ).

Интерес представлява разпоредбата на чл. 8 от ППЗОВСРБ, съгласно която „След сключване на договора за военна служба лицето се приема на военна служба и се назначава на длъжност със заповед на министъра на отбраната или на оправомощено от него длъжностно лице“. Тази разпоредба въвежда един сложен

фактически състав за възникване на правоотношението по изпълнение на военна служба – провеждане на конкурс, подписването на договори и издаването на заповед.

Въпреки че въпросите, свързани със сключването на договора и издаването на заповед за приемане на военна служба, са уредени непосредствено след уредбата на конкурса, следва да се има предвид, че това не е специфичен случай, който се прилага единствено и само в случаите на назначаване на лица, завършили граждански средни или висши училища в страната и в чужбина.

Съгласно чл. 146 от ЗОВСРБ, приемането на военна служба, назначаването и освобождаването от длъжност на военнослужещите във военно звание се извършват с:

- ✓ указ на президента на републиката по предложение на Министерския съвет – за офицерите от висшия команден състав;
- ✓ заповед на министъра на отбраната или оправомощено от него длъжностно лице – за останалите офицери, офицерските кандидати, сержантите (старшините) и войниците (матросите).

Следователно, за разлика от трудовите и служебните правоотношения, фактическият състав за възникване на правоотношение по изпълнение на военна служба (който по аналогия с останалите може да наречем „военнослужески правоотношения“) е сложен и включва задължително сключването на договор за военна служба и издаването на заповед (с изключение на случаите на приемане с указ на президента).

Изменение на договора за военна служба

Правилника за прилагане на ЗОВСРБ предвижда редът и условията, при които договорът за военна служба може да бъде изменен.

Съгласно разпоредбата на чл. 65, ал. 1 от ППЗОВСРБ, изменението на договора за военна служба се извършва чрез сключване на допълнително споразумение към него в следните случаи:

- ✓ при изменение на правата и задълженията на страните;
- ✓ при изменение на условията и срока на договора.

Допълнителното споразумение се изготвя в писмена форма и се счита за неразделна част от договора за военна служба.

Правилникът предвижда и случаите, в които задължително се сключва писмено допълнително споразумение). Това са (чл. 65, ал. 3 от ППЗОВСРБ):

- ✓ при приемане на военнослужещ за обучение за придобиване на образователно-квалификационна степен „магистър“ по военна специалност;
- ✓ при приемане на военнослужещ за обучение в професионални сержантски (старшински) колеж или в приравнено на него военно училище в чужбина;
- ✓ при постъпване на военнослужещ на редовно обучение за придобиване на образователна и научна степен „доктор“;
- ✓ при разрешаване на военнослужещ на обучение за придобиване на образователно-квалификационна степен „бакалавър“ или „магистър“ по гражданска специалност;
- ✓ при разрешаване на военнослужещ, дипломирал се по специалността „Право“, да завърши изисквания се стаж като стажант-юрисст;

- ✓ при изпращане на военнослужещ на обучение в чужбина в случаите, когато това обучение е с продължителност не по-малка от 6 месеца;
- ✓ при удължаване срока на договора;
- ✓ при назначаване на длъжност „инструктор“ във военна академия или висши военни училища за срок до 5 години;
- ✓ при назначаване на академична длъжност „асистент“ във военна академия или висши военни училища за срок 6 години.

Освен посочените основания за изменение на договора за военна служба, разпоредбата на чл. 66, ал. 1 от ППЗОВСРБ предвижда още и, че не по-късно от три месеца преди изтичане срока на договора всяка от страните по него може да отправи предложение до другата за удължаването му с не по-малко от 2 години.

Прекратяване на договора за военна служба

Договорът за военна служба се прекратява със заповед на министъра на отбраната или на оправомощено от него длъжностно лице, в която задължително се посочват (чл. 73, ал. 1 и 2 от ППЗОВСРБ):

- ✓ длъжностното лице, което я издава;
- ✓ правните и фактическите основания за прекратяването на договора;
- ✓ разпоредителна част, която съдържа:
 - права и задължения, както и реда за тяхното изпълнение;
 - разпоредби за зачисляване на военен отчет или за снемане от отчет;
 - срок за сдаване на длъжността;
 - имуществени последици от прекратяването на договора;
 - срока и реда за обжалване на заповедта.

Случаите, в които военнослужещите се освобождават от военна служба, отново са посочени в ППЗОВСРБ (чл. 72):

- ✓ при преназначаване на друга длъжност;
- ✓ при вземане в специален щат или във временен задграничен щат на министъра на отбраната;
- ✓ при прекратяване на договора за военна служба.

ЗОВСРБ обаче предвижда и други основания, при които се прекратява военнослужесното правоотношение. Чл. 162 от ЗОВСРБ предвижда основанията за прекратяване на договора за военна служба без предизвестие:

- ✓ По взаимно съгласие на страните, изразено писмено. Страната, към която е отправено предизвестие, е длъжна да вземе отношение по него и да уведоми другата страна в 30-дневен срок. Ако тя не направи това, приема се, че предложението не е прието.
- ✓ С изтичане на уговорения срок (ако никоя от страните не е предприела действия по чл. 66 от ППЗОВСРБ).
- ✓ При навършване на пределна възраст от военнослужещия.
- ✓ При настъпила негодност за военна служба или психологична непригодност, установена от военномедицинските органи, съответно от органите по чл. 141, ал. 3 от ЗОВСРБ (основание, свързано с изискванията за заемането на военна служба).
- ✓ При преминаване на платена изборна длъжност (с изключение на случаите по чл. 187, ал. 3 от ЗОВСРБ).

- ✓ При отказ на военнослужещия да приеме предложената му длъжност по реда на чл. 206, ал. 3 от ЗОВСРБ.
- ✓ Когато военнослужещият не се яви за заемане на длъжността в срока по чл. 172, ал. 2 от ЗОВСРБ, освен когато този срок не бъде спазен по уважителни причини.
- ✓ Със смъртта на военнослужещия.

Едностранното прекратяване на договора за военна служба от министъра на отбраната или от оправомощено от него длъжностно лице е предвидено в чл. 164 от ЗОВСРБ. Съгласно тази законова разпоредба правоотношението се прекратява с 6-месечно писмено предизвестие, отправено до военнослужещия, при:

- ✓ организационно-щатни промени или при пълна или частична ликвидация въз основа на акт на Министерския съвет или при съкращаване числеността на въоръжените сили или на отделни техни формирования по решение на Народното събрание. В решението може да бъде определен друг срок за предизвестие;
- ✓ промяна в изискванията за заемане на длъжността по Класификатора на длъжностите на военнослужещите в Министерството на отбраната, структурите на пряко подчинение на министъра на отбраната и Българската армия, на които военнослужещият не отговаря;
- ✓ изтичане на максималния срок за престояване в старши офицерски звания и невъзможност на военнослужещия да се предложи длъжност, изискваща по-високо военно звание и съответстваща на образованието и професионалната му квалификация;
- ✓ изтичане на максималния срок за престояване в длъжност и невъзможност да се предложи длъжност, съответстваща на образованието и на професионалната квалификация на военнослужещия;
- ✓ придобиване право на пенсия при условията на чл. 69 от Кодекса за социално осигуряване [7].

Основанията за прекратяване на договора за военна служба без предизвестие от министъра на отбраната или оправомощено от него длъжностно лице са посочени в чл. 165 от ЗОВСРБ:

- ✓ при отпадане на основанието за приемане на военна служба по чл. 141, ал. 1, т. 6 от ЗОВСРБ (с изключение на случаите по чл. 141, ал. 5 от ЗОВСРБ);
- ✓ когато след приемането на военна служба лицето не завърши обучението за придобиване на военна квалификация;
- ✓ при налагане на дисциплинарно наказание „уволнение“;
- ✓ от датата на регистриране на военнослужещия като кандидат за изборна длъжност от политическа партия или коалиция в избори за президент, вицепрезидент на Република България, народни представители, членове на Европейския парламент от Република България, общински съветници или кметове;
- ✓ при установяване на несъвместимост по чл. 188;
- ✓ при отказ за издаване, при отнемане на разрешението за достъп до класифицирана информация или при отказ на военнослужещия да подаде документи за проучване при условията и по реда на Закона за защита на класифицираната информация;

- ✓ при изтичане на максималния срок за престояване в старши офицерски звания и отказ на военнослужещия да заеме предложената му длъжност, изискваща по-високо военно звание и съответстваща на образованието и професионалната му квалификация;
- ✓ при изтичане на максималния срок за престояване в длъжност и отказ на военнослужещия да заеме предложената му длъжност, съответстваща на неговите образование и професионална квалификация;
- ✓ при установяване на конфликт на интереси по Закона за предотвратяване и установяване на конфликт на интереси, с влязъл в сила акт.

Разпоредбите на ЗОВСРБ и ППЗОВСРБ относно прекратяването на договора за военна служба по своя характер се доближават до основанията за прекратяване на трудовия договор по Кодекса на труда и за прекратяване на служебните правоотношения по ЗДСл., което е още една причина договорът за военна служба да бъде определен като административно-трудова по своята правна същност.

В заключение следва да се отбележи, че посочените законови и подзаконови разпоредби не изчерпват реда за назначаване на военнослужещи съгласно действащото българско законодателство. Съгласно разпоредбата на чл. 4, ал. 3 от ППЗОВСРБ приемането на военна служба в служба „Военна информация“ се извършва при условия и по ред, определени с правилника по чл. 100, ал. 5 от ЗОВСРБ, който обаче е отменен, което оставя открит въпроса какви са редът и условията за назначаването на служителите в тази служба. Приемането на военна служба в служба „Военна полиция“ пък се извършва при условията и по реда, предвидени в Правилника за прилагане на Закона за военната полиция.

Източници:

1. **Закон за отбраната и въоръжените сили на Република България** (обн. ДВ, бр. 35 от 12 май 2009 г., посл. изм. и доп. ДВ, бр. 17 от 1 март 2016 г.).
2. **Закон за всеобщата военна служба в Народна Република България** (обн. ДВ, бр. 13 от 14 февруари 1958 г., отм. ДВ, бр. 112 от 27 декември 1995 г.).
3. **Закон за отбраната и въоръжените сили на Република България** (обн. ДВ, бр. 112 от 27 декември 1995, отм. ДВ, бр. 35 от 12 май 2009 г.).
4. **Правилник за кадрова военна служба** (обн. ДВ, бр. 2 от 5 януари 2001 г., отм. ДВ, бр. 44 от 12 юни 2009 г.).
5. **Правилник за прилагане на Закона за отбраната и въоръжените сили на Република България** (обн. ДВ, бр. 25 от 30 март 2010 г., посл. изм. ДВ, бр. 27 от 5 април 2016 г.).
6. **Закон за държавния служител** (обн. ДВ, бр. 67 от 27 юли 1999 г., посл. изм. и доп. ДВ, бр. 98 от 15 декември 2015 г.).
7. **Кодекс за социално осигуряване** (обн. ДВ, бр. 110 от 17 декември 1999 г., посл. изм. ДВ, бр. 102 от 29 декември 2015 г.).

ПРЕСТЪПЛЕНИЯТА СРЕЩУ МАЛОЛЕТНИ И НЕПЪЛНОЛЕТНИ КАТО ЗАПЛАХА ЗА СИГУРНОСТТА НА СТРАНАТА

Силвия Д. Салтирова-Радкова

Шуменски университет „Епископ Константин Преславски“, гр. Шумен
Педагогически факултет
e-mail: ssaltirova@gmail.com

CRIMES AGAINST MINORS AS A THREAT TO NATIONAL SECURITY

Silviya D. Saltirova-Radkova

ABSTRACT: *The present report aims to analyse the crimes against infants and minors as a threat to national security. The Constitution of Republic of Bulgaria provides special protection of children and the provisions of the Criminal Code are expression of this special protection.*

KEY WORDS: *crime, infants, minors, special protection, national security*

Основен принцип, залегнал още в Конституцията на Република България (КРБ) [1], е, че децата са под закрилата на държавата (чл. 14 от КРБ). Ето защо българският наказателен закон предвижда редица мерки за закрила на малолетните и непълнолетните, като основен акцент в теорията обикновено се поставя върху специалния режим на тяхната наказателна отговорност. Мерките за закрила на малолетните и непълнолетните, обаче, не се изчерпват единствено с разпоредбите на Общата част на Наказателния кодекс (НК) [2]. Израз на тези мерки са предвидените квалифицирани състави на някои от престъпленията, предвидени в Особената част на НК, тогава, когато жертва на тези престъпления са малолетни или непълнолетно лица.

Съгласно разпоредбата на чл. 1, ал. 1 от НК задачата на закона е да защитава от престъпни посегателства личността и правата на гражданите, както и цялостния установен в страната правов ред – обстоителство, което може да се обобщи с извода, че целта е защита сигурността на страната.

Основание за възрастово деление на лицата

Още в Общата част на НК законодателят прави възрастово разграничение на лицата, като определя три групи лица:

- ✓ пълнолетни - лицата, които са навършили 18-годишна възраст;
- ✓ непълнолетни – лицата, които са навършили 14-годишна възраст, но не са навършили 18 години;
- ✓ малолетни – лицата, които не са навършили 14-годишна възраст.

Когато става въпрос за особения режим на наказателна отговорност на малолетните и непълнолетните лица, като основна причина за това деление се изтъква

тяхната психическа и физическа недоразвитост (формиране на личността, развитие на главния мозък и др.) [3].

Когато, обаче говорим за защита на малолетните и непълнолетните лица в Особената част на НК, като основание за това възрастово деление може да изтъкнем обстоятелствата, свързани с невъзможността на тези лица да се защитават, да отвърнат на нападението, да осъзнаят характера на деянието, податливостта и лесната им доверчивост и др. под.

Конкретни мерки за защита на малолетните и непълнолетните лица, предвидени в Особената част на НК

Конкретните мерки за защита на малолетните и непълнолетните лица, предвидени в Особената част на НК, се изразяват в предвиждането на по-строги наказания за престъпления, извършени срещу малолетни или непълнолетни лица. Голяма част от тези състави се съдържат в разпоредбите на глава втора „Престъпления против личността от Особената част на НК.

Съгласно чл. 115 от НК за основния състав на убийството предвиденото наказание е лишаване от свобода от 10 до 20 години. Чл. 116, ал. 1, т. 4 от НК, обаче, предвижда, че за убийство на малолетно лице наказанието е лишаване от свобода от 15 до 20 години, доживотен затвор или доживотен затвор без замяна.

Чл. 118 от НК предвижда по-леко наказание (лишаване от свобода до 8 години), когато убийството е извършено в състояние на силно раздразнение, което е предизвикано от пострадалия с насилие, с тежка обида или клевета или с друго противозаконно действие. Наказанието, обаче, ще бъде лишаване от свобода от 1 до 8 години, ако става въпрос за квалифицираните случаи на убийство по чл. 116, ал. 1, т. 1 – 6 от НК, включително и за убийство на малолетно лице.

Въпросът, който би могъл да възникне в конкретния случай е доколко е оправдана такава по-лека наказуемост с оглед на обстоятелството, че малолетните лица са наказателно неотговорни, тъй като не са достигнали онази физическа и психическа зрялост, която им позволява да разбират свойството и значението на извършеното от тях и да ръководят постъпките си. Ако законът ги освобождава от наказателна отговорност поради тези техни особености, то редно ли е действията на малолетните да бъдат взети предвид и да обосноват по-лека наказуемост особено за такова тежко престъпление като убийството?

По-тежко наказание предвижда и чл. 127, ал. 2 от НК относно подпомагането или склоняването на друго лице към самоубийство, когато престъплението е извършено срещу непълнолетно лице или срещу лице, за което виновният знае, че е неспособно да ръководи постъпките си или че не разбира свойството или значението на извършеното (а малолетните определено спадат към тази група лица). Така по основния състав на това престъпление (чл. 127, ал. 1 от НК) наказанието е лишаване от свобода от 1 до 6 години, а за квалифицирания състав по чл. 127, ал. 2 от НК наказанието е лишаване от свобода от 3 до 10 години. По-тежко наказуем е съставът на чл. 127, ал. 3 от НК: *„Който чрез жестоко отнасяне или системно унизяване на достойнството на лице, намиращо се в материална или друга зависимост от него, го доведе до самоубийство или до опит за самоубийство [...]“*. Малолетните и непълнолетни лица със сигурност се намират в материална и друга зависимост, поради което извършеното срещу тях престъпление може да бъде

квалифицирано като деяние по чл. 127, ал. 3 от НК, за което се предвижда лишаване от свобода от 2 до 8 години.

Другата група престъпления, при които се предвиждат по-тежки наказания за престъпления, извършени срещу малолетни и непълнолетни, са телесните повреди.

Наказанията, предвидени в основните състави на телесните повреди са:

- ✓ за тежка телесна повреда – лишаване от свобода от 3 до 10 години (чл. 128, ал. 1 от НК);
- ✓ за средна телесна повреда – лишаване от свобода до 6 години (чл. 129, ал. 1 от НК);
- ✓ за лека телесна повреда – лишаване от свобода до 2 години или пробация (чл. 130, ал. 1 от НК).

Когато обаче престъплението е извършено срещу малолетно лице (чл. 131, ал. 1, т. 4 от НК), наказанието е:

- ✓ за тежка телесна повреда – лишаване от свобода от 3 до 15 години (по-тежката наказуемост се изразява в определянето на по-висок максимум на наказанието);
- ✓ за средна телесна повреда – от 2 до 10 години (по-тежката наказуемост тук се изразява в определяне на специален минимум и по-висок максимум на предвиденото наказание);
- ✓ за лека телесна повреда – до 3 години (по-тежката наказуемост се изразява в по-високия максимум и липсата на алтернативното наказание пробация).

Квалифициран състав е предвиден и за заразяването друго с венерическа болест, когато пострадалият е непълнолетно лице до 16-годишна възраст. Наказанието по основния състав (чл. 135, ал. 1 от НК) е лишаване от свобода до 3 години и глоба до 200 лв., а по квалифицирания състав (чл. 135, ал. 2 от НК) – лишаване от свобода до 5 години или глоба до 500 лв.

При злепоставянето също са предвидени специални състави за престъпления, извършени срещу малолетни или непълнолетни. Съгласно разпоредбата на чл. 137 от НК: *„Който изложи лице, лишено от възможността да се самозапазва поради малолетство, престарялост, болест или изобицо поради своята безпомощност, по такъв начин, че животът му може да бъде в опасност, и като съзнава това, не му се притече на помощ, се наказва с лишаване от свобода до три години“*. Разпоредбата на чл. 138 от НК пък предвижда, че с лишаване от свобода до 1 години или с пробация се наказва всеки, *„който съзнателно не окаже помощ на лице, за което е длъжен да се грижи и което се намира в опасност за живота си и няма възможност да се самопази поради малолетство, престарялост, болест или изобицо поради своята безпомощност, в случаите, когато е могъл да окаже помощ“*.

Следващата група престъпления, при което се предвижда особена по-тежка отговорност за деяние, извършено срещу малолетно или непълнолетно лице, е отвлечането и противозаконното лишаване от свобода. Съгласно разпоредбата на чл. 142, ал. 2, т. 3 от НК, когато отвлеченото лице не е навършило 18 години, наказанието е лишаване от свобода от 7 до 15 години (за сравнение наказанието по основния състав на чл. 142, ал. 1 от НК е лишаване от свобода от 3 до 10 години). Чл. 142а, ал. 3 от НК предвижда наказание лишаване от свобода от 3 до 10 години за противозаконно лишаване от свобода на малолетно или непълнолетно лице (наказанието по основния състав е лишаване от свобода до 6 години).

Раздел VIII „Разврат“ от глава втора на Особената част на НК съдържа цяла група престъпления, които са извършени срещу малолетни и/или непълнолетни лица (чл. 149 – 151 от НК). По-тежко наказание е предвидено и за изнасилване на ненавършило 14 години момиче (чл. 152, ал. 4, т. 1 от НК). Чл. 154а НК предвижда наказателна отговорност за лице, което извърши блудствени действия или съвкупление с непълнолетно лице, което се занимава с проституция. По-тежко наказание се предвижда и за склоняване към проституция или свождане към блудствени действия или съвкупление, склоняване или принуда към употреба на наркотични вещества или техни аналози с цел проституиране, съвкупление, блудствени действия или извършване на полово сношение или действия на полово удовлетворение, когато пострадащото лице не е навършило 18 години (чл. 155, ал. 5, т. 2 от НК). Почти целият раздел до края съдържа разпоредби, касаещи извършването на различни престъпления срещу малолетни и/или непълнолетни лица. В раздел IX „Трафик на хора“ също са предвидени по-тежки наказания за престъпления, жертва на което са малолетни и/или непълнолетни лица.

Целият раздел II „Престъпления против младежта“ на глава четвърта „Престъпления против брака, семейството и младежта“ от Особената част на НК, е посветен на престъпления срещу малолетни и/или непълнолетни лица.

Отделни разпоредби относно по-тежката наказуемост на престъпленията, извършени срещу малолетни и/или непълнолетни лица могат да бъдат намерени и в останалите глави и раздели от Особената част на НК.

Внимателният анализ на разпоредбите от Особената част на НК показва, че малолетните и непълнолетните лица се намират под особената закрила на държавата, като за престъпленията, извършени срещу тях законодателят предвижда по-тежки наказания. Това е израз на особената роля на наказателното право да защитава сигурността на страна и по-специално конституционно закрепеният принцип за особената закрила на децата.

Източници:

1. **Конституция на Република България** (обн. ДВ, бр. 56 от 13 юли 1991 г., посл. изм. и доп. ДВ, бр. 100 от 18 декември 2015 г.).
2. **Наказателен кодекс** (обн. ДВ, бр. 26 от 12 април 1968 г., посл. изм. ДВ, бр. 32 от 22 април 2016 г.).
3. **Стойнов, Ал. Наказателно право. Обща част.** София, Сиела, 1999.

СТАТУТ НА ДЪРЖАВНИТЕ СЛУЖИТЕЛИ В МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ

Силвия Д. Салтирова-Радкова

Шуменски университет „Епископ Константин Преславски“, гр. Шумен
Педагогически факултет
e-mail: ssaltirova@gmail.com

THE STATUS OF CIVIL SERVANTS IN THE MINISTRY OF INTERNAL AFFAIRS

Silviya D. Saltirova-Radkova

ABSTRACT: *The present report aims to analyse the special status for the civil servants in the Ministry of Internal Affairs specifically – the Police authorities and the Fire Safety and Protection of Population authorities. Those civil servants are obliged to execute very special and responsible tasks wherefore they are subject to special requirements, have special rights and obligations in as opposed to other civil servants.*

KEY WORDS: *civil servants, internal affairs, police, fire safety, protection of population*

Основен нормативен акт в областта на държавната служба е Законът за държавния служител (ЗДСл.) [1]. Той урежда „възникването, съдържанието и прекратяването на служебните правоотношения между държавата и държавния служител при и по повод изпълнението на държавната служба [...]“ (чл. 1 ЗДСл.).

Въпреки опита това да бъде един кодифициращ нормативен акт, който да урежда правната материя относно служебните правоотношения на държавните служители, специфичните функции, които някои държавни служители изпълняват, налагат въвеждането на специална уредба на техните служебни правоотношения. Такъв е случаят със служителите в Министерството на вътрешните работи (МВР).

Според статута, който имат, служителите в МВР се разделят на три основни групи [2, с. 191]:

- ✓ държавни служители, чийто статут се определя със Закона за Министерството на вътрешните работи (ЗМВР) [3]. Това са полицейските органи и органите по пожарна безопасност и защита на населението;
- ✓ държавни служители, чийто статут се определя със ЗДСл.;
- ✓ лица, работещи по трудово правоотношение, чийто статут се определя с Кодекса на труда (КТ).

Статутът на държавните служители по ЗДСл. и на лицата, работещи по трудово правоотношение, не разкрива специфични особености. Не така, обаче, стоят нещата с държавните служители – полицейски органи и органи по пожарна безопасност и защита на населението. Ето защо именно тази група ще обект на изследване в настоящия доклад.

Обща характеристика на държавната служба по ЗМВР

Видовете длъжности, на които се назначават служителите по чл. 142, ал. 1, т. 1 от ЗМВР, са изчерпателно посочени в ЗМВР (чл. 143, ал. 1). Това са:

- ✓ висши ръководни длъжности;
- ✓ ръководни длъжности;
- ✓ изпълнителски длъжности;
- ✓ младши изпълнителски длъжности.

Подобно на Класификатора на длъжностите в администрацията, ЗМВР предвижда създаването на Класификатор на длъжностите в МВР, в който се определят длъжностите и специфичните им наименования. Класификаторът се приема от министъра на вътрешните запоеди заедно със заповед за неговото прилагане.

По подобие на Кодекса за поведение на служителите в държавната администрация за държавните служители по чл. 142, ал. 1, т. 1 от ЗМВР министърът на вътрешните работи утвърждава Етичен кодекс за поведение на държавните служители в МВР (чл. 150, ал. 1 от ЗМВР). Клетвата, която държавните служители в МВР полагат съгласно ЗМВР е аналогична на клетвата, която полагат държавните служители по ЗДСл.

Едно изключително важно различие между държавните служители по ЗМВР и тези по ЗДСл. се съдържа в разпоредбата на чл. 148 от ЗМВР, съгласно която: *„На държавните служители е забранено, включително в извънработно време, да участват в събрания, митинги и манифестации на политически партии, да извършват политическа дейност, както и да предприемат други действия, с които се нарушава политическият им неутралитет“*. Въпреки, че тази разпоредба не представлява директна забрана за членуване в политически партии, тя съществено се различава от правната уредба в ЗДСл.¹

Чл. 153, ал. 3 от ЗМВР определя основанията за несъвместимост със службата в МВР. За държавните служители в МВР възниква несъвместимост когато:

- ✓ биха се оказали в непосредствена йерархическа връзка на ръководство и контрол със съпруг или съпруга, лице, с което се намират във фактическо съжителство, роднина по права линия, по съребрена линия - до четвърта степен включително, или роднина по сватовство - до втора степен включително;
- ✓ са еднолични търговци, неограничено отговорни съдружници в търговски дружества, управители, търговски пълномощници, търговски представители, прокуристи, търговски посредници, ликвидатори или синдици, членове на органи на управление или контрол на търговски дружества или кооперации;
- ✓ извършват търговска дейност;
- ✓ работят по трудово правоотношение или по граждански договор, освен за осъществяване на научна, преподавателска дейност или упражняване на авторски права, по ред, определен от министъра на вътрешните работи;

¹ Чл. 42, ал. 1 от ЗДСл., например, предвижда, че държавният служител има право да членува в политически партии, доколкото не съществува забрана, установена в специален закон, а съгласно чл. 4, ал. 2 от ЗДСл. при изпълнение на своята служба държавният служител трябва да бъде политически неутрален.

- ✓ са избрани за президент, вицепрезидент, народни представители, членове на Европейския парламент от Република България, кметове или общински съветници.

Разпоредбата на чл. 153, ал. 3 от ЗМВР се доближава като текст до чл. 7, ал. 2 от ЗДСл. (в ЗМВР липсват основанията на т. 3, 4 и 5 на чл. 7, ал. 2 от ЗДСл.).

Изисквания за постъпване на служба в МВР

ЗМВР поставя специални изисквания за заемането на държавна служба в структурата на МВР. За да бъде едно лице държавен служител в МВР, то трябва да отговаря на следните изисквания:

- ✓ да е дееспособно;
- ✓ да има само българско гражданство;
- ✓ да не е осъждано за умишлено престъпление от общ характер, независимо от реабилитацията;
- ✓ да не е привлечено като обвиняем или да не е подсъдимо за умишлено престъпление от общ характер;
- ✓ да отговаря на специфичните изисквания за възраст, образование, физическа годност и психологична пригодност, определени с наредба на министъра на вътрешните работи;
- ✓ да отговаря на медицинските изисквания за работа в МВР, определени с наредба на министъра на вътрешните работи.

Назначаване на държавна служба в МВР

Назначаването на държавна служба в МВР се извършва въз основа на конкурс. Условието и редът за провеждането на конкурса са определени в Наредба № 8121з-344 от 25 юли 2014 г. за назначаване на държавна служба в Министерството на вътрешните работи [4]. Наредбата определя специфичните изисквания за възраст, образование, физическа годност и психологична пригодност за постъпване на държавна служба в МВР, както и условията и редът за провеждане на конкурса за назначаване на държавна служба в МВР.

Конкурсът се обявява със заповед на министъра на вътрешните работи или на оправомощено от него длъжностно лице. В заповедта се определят:

- ✓ видът на конкурса - конкурс за длъжности, за които се изисква задължителна първоначална професионална подготовка, или конкурс за длъжности, за които не се изисква такава подготовка;
- ✓ вакантните длъжности, разпределени по видове и направление на дейност в структурите;
- ✓ условията за участие в конкурса, както и изискванията по чл. 155, ал. 1 от ЗМВР към кандидатите;
- ✓ необходимите документи за участие в конкурса и срокът за подаването им;
- ✓ звената „Човешки ресурси“, в които се подават документите за участие в конкурса;
- ✓ конкурсните етапи и срокът за провеждане на конкурса;
- ✓ съставът на конкурсната комисия и технически секретар(и);
- ✓ членовете на конкурсната комисия - ръководители на експертни групи;

- ✓ нормативите за проверка на физическата годност, когато конкурсът е за длъжности, за които се изисква задължителна първоначална професионална подготовка.

При необходимост от установяване нивото на специфични знания и/или умения за изпълнение на длъжността със заповедта за обявяване на конкурса се определя провеждането на изпит с допуснатите до участие кандидати. В заповедта се определя тематика, начин на провеждане, оценяване и елиминаторен праг (чл. 5, ал. 4 от Наредбата за назначаване на държавна служба в МВР).

Конкурсът за назначаване на държавна служба в МВР се провежда на няколко етапа:

- ✓ изследване на физическата годност;
- ✓ психологично изследване;
- ✓ заключително интервю.

Всеки етап приключва с обявяване на резултатите от него, класиране на кандидатите по бал и обявяване на етапните резултати, както и на допуснатите до следващия етап. Конкурсната процедура приключва с обявяване на крайното класиране.

Професионална подготовка

ЗМВР предвижда задължителна професионална подготовка на държавните служители по чл. 142, ал. 1, т. 1 от ЗМВ. Тя се провежда под формата на професионално образование и професионално обучение. Професионалното обучение на служителите, постъпващи за първи път на държавна служба в МВР се провежда от Академията на МВР, а професионалното обучение на другите служители в МВР се извършва от Академията на МВР, научноизследователските и научно-приложните институти на МВР, обучаващи звена на МВР и други обучаващи институции.

Възнаграждения, материално и социално осигуряване на служителите на МВР

ЗМВР предвижда специални разпоредби за определяне на възнагражденията на държавните служители в МВР, както и за тяхното материално и социално осигуряване.

Брутното месечно възнаграждение на държавните служители в МВР се състои от основно месечно възнаграждение (заплатата за длъжността, определена на база, посочена в чл. 177 от ЗМВР) и допълнителни възнаграждения.

Допълнителните възнаграждения на държавните служители в МВР са за (чл. 178, ал. 1 от ЗМВР):

- ✓ прослужено време – 2% от основното месечно възнаграждение за всяка година стаж, но не повече от 40%;
- ✓ изпълнение на специфични служебни дейности;
- ✓ извънреден труд;
- ✓ работа при специфични условия;
- ✓ постигнати резултати в служебната дейност;
- ✓ за научна степен;
- ✓ за труд през нощта (в интервала от 22:00 до 6:00 часа);
- ✓ за полагане на труд през дните на официални празници;
- ✓ за времето на разположение.

Както се вижда от разпоредбите на ЗМВР, за разлика от държавните служители по ЗДСл., държавните служители в МВР имат право да получават допълнително възнаграждение за прослужено време.

Съгласно разпоредбата на чл. 181 от ЗМВР на служителите на МВР (държавни и тези по трудово правоотношение) се осигурява храна или левовата ѝ равностойност, а на държавните служители – работно и униформено облекло и друго вещеве имущество и снаряжение. На неносещите униформа се изплаща ежегодно парична сума за облекло.

Подобно на държавните служители в другите администрации, задължителното социално и здравно осигуряване на държавните служители се извършва за сметка на държавния бюджет. Освен това служителите на МВР при изпълнение на служебните си задължения имат право да пътуват безплатно в обществения градски транспорт.

Работно време и отпуски

Законът за МВР предвижда и специални разпоредби относно работното време и отпуските на държавните служители в МВР. Работното време е 8 часа седмично при 5-дневна работна седмица или 40 часа седмично.

Разпоредбата на чл. 187, ал. 2 от ЗМВР установява намалено работно време за държавни служители, които изпълняват служебните си задължения при специфични условия и рискове за живота и здравето.

Изчисляването на времето по принцип е подневно, но поради спецификата на изпълняваните дейности някои от държавните служители се налага да работят на смени (8-, 12- или 24-часови). В тези случаи се прилага сумирано изчисляване на работното време. Държавните служители, които не работят при специфични условия и рискове за живота и здравето, но работят на смени, се установява ненормиран работен ден, като те са длъжни при необходимост да изпълняват служебните си задължения и след изтичане на редовното работно време.

Съгласно разпоредбата на чл. 187, ал. 5 от ЗМВР: *„Работата извън редовното работно време до 280 часа годишно се компенсира със:*

1. *допълнителен платен годишен отпуск за работата в работни дни и с възнаграждение за извънреден труд за работата в почивни и празнични дни – за служителите на ненормиран работен ден;*
2. *възнаграждение за извънреден труд за отработени до 70 часа на тримесечен период – за служителите, работещи на смени. “*

Заплащането на извънредния труд по чл. 187, ал. 5 от ЗМВР се извършва с 50% увеличение върху основното месечно възнаграждение.

Чл. 189 от ЗМВР определя видовете отпуски, на които имат право държавните служители. Те са:

- ✓ редовен платен годишен отпуск - в размер 30 работни дни;
- ✓ допълнителен платен годишен отпуск - по един ден за всяка прослужена година, включително за приравнения трудов стаж, но не повече от 10 работни дни;
- ✓ допълнителен платен годишен отпуск по чл. 187, ал. 5, т. 1 от ЗМВР - до 12 работни дни;

- ✓ допълнителен платен годишен отпуск при преместване на работа в друго населено място - в размер на един работен ден, който не може да се ком-пенсират с парично обезщетение;
- ✓ неплатен отпуск - до 6 месеца за цялата служба;
- ✓ неплатен отпуск - за времето на заемане на длъжност по срочен договор в институции или структури на Европейския съюз или в международни ор-ганизации;
- ✓ неплатен отпуск по реда на чл. 247;
- ✓ неплатен служебен отпуск по реда на чл. 161, ал. 1 - 3 от Изборния ко-декс;
- ✓ неплатен отпуск - за времето на провеждане на стаж по чл. 294 от Закона за съдебната власт;
- ✓ неплатен отпуск по реда на чл. 77 от Закона за дипломатическата служба.

Прави впечатление, че за разлика от работещите по Кодекса на труда и ЗДСл., държавните служители по ЗМВР имат право на увеличен размер на редовен пла-тен годишен отпуск (30 дни) и не повече от 6 месеца неплатен отпуск за цялата служба, който се признава за трудов стаж.

Държавните служители жени в МВР се ползват от специалната закрила на же-ните по Кодекса на труда с изключение на правото на надомна работа и закрила при уволнение.

Дисциплинарна отговорност

ЗМВР предвижда и специални правила за дисциплинарната отговорност на държавните служители по ЗМВР.

Видовете дисциплинарни нарушения, които законодателят определя са:

- ✓ неизпълнение на разпоредбите на този закон и на издадените въз основа на него подзаконовни нормативни актове, на заповедите и разпореждания-та на министъра на вътрешните работи, заместник-министрите и главния секретар на МВР и на преките ръководители;
- ✓ неизпълнение на служебните задължения;
- ✓ неспазване на служебните правомощия;
- ✓ неспазване на правилата на Етичния кодекс за поведение на държавните служители в МВР.

И тук важи общото правило, че дисциплинарни наказания се налагат не по-късно от 2 месеца от откриване на нарушението и не по-късно от 1 година от из-вършването му. Чл. 195, ал. 2 от ЗМВР, обаче, предвижда една специална хипотеза – при извършено тежко нарушение на служебната дисциплина дисциплинарното наказание се налага не по-късно от 2 месеца от откриването му и не по-късно от 2 години от извършването му.

Дисциплинарни наказания по ЗМВР също показват някои специфики спрямо дисциплинарни наказания по КТ и ЗДСл. Съгласно разпоредбата на чл. 197, ал. 1 от ЗМВР дисциплинарни наказания са:

- ✓ мъмрене;
- ✓ писмено предупреждение;
- ✓ порицание;
- ✓ забрана за повишаване в длъжност за срок от една до три години;
- ✓ предупреждение за уволнение;

✓ уволнение.

Следва да се има предвид, че тук законодателят е предвидил хипотезите за налагане на всеки един от видовете наказания (за разлика от КТ, където се съдържат специални изисквания единствено за налагането на дисциплинарно наказание „уволнение“). Така чл. 198 от ЗМВР предвижда, че дисциплинарното наказание „мъмрене“ се налага за маловажни дисциплинарни нарушения, т.е. тези, при които отклонението от изискванията е незначително.

И тук важи правилото за задължително изслушване на държавния служител или приемане на писмените му обяснения преди налагането на самото дисциплинарно наказание.

В заключение може да се направи обобщението, че статутът на държавните служители по ЗМВР показва доста общи черти с правната уредба на статута на държавните служители по ЗДСл., но предвид спецификата на извършваната дейност са налице доста значителни различия.

Източници:

1. **Закон за държавния служител** (обн. ДВ, бр. 67 от 27 юли 1999 г., посл. изм. и доп. ДВ, бр. 98 от 15 декември 2015 г.).

2. **Ц. Сивков, Д. Зиновиева, Г. Димитров, Е. Панайотова, Р. Николова, С. Янкулова, Г. Чернева и К. Милчева, Административно право. Специална част : Курс лекции.** София, Сиби, 2015.

3. **Закон за Министерството на вътрешните работи** (обн. ДВ, бр. 53 от 27 юни 2014 г., посл. доп. ДВ, бр. 61 от 11 август 2015 г.).

4. **Наредба № 8121з-344 от 25 юли 2014 г. за назначаване на държавна служба в Министерството на вътрешните работи** (обн. ДВ, бр. 64 от 5 август 2014 г., посл. изм. и доп. ДВ, бр. 33 от 8 май 2015 г.).

ОПАСНОСТ ОТ ХИМИЧЕСКИ АВАРИИ

Доника В. Диманова

Шуменски Университет „Епископ Константин Преславски“, Шумен
Факултет по технически науки
e-mail: d.dimanova@gmail.com

RISK OF CHEMICAL ACCIDENTS

Donika V. Dimanova

ABSTRACT: Economic activity in the country is associated with the operation of multiple sites of energy, chemical, petrochemical, metallurgical and pharmaceutical industries. Most of them work with explosive, flammable, combustible and highly toxic substances that can cause industrial accidents and fires, releasing highly toxic substances. Not excluded is the possibility of a breach of technological discipline and breaches of safety. All these circumstances influence vulnerability and risk status of the facilities of national economy.

KEY WORDS: *factors, dangers, risk, accidents, hazardous chemicals, protection of population*

Въведение

Аварии с отделяне на опасни химически вещества (ОХВ) включват:

- отделяне на ОХВ в резултат на изтичане или разлив;
- разрушаване на целостта на магистралните продуктопроводи за течни или газообразни химически вещества;
- пожари, взривове и разрушения, свързани с отделяне на опасни химически вещества;
- нарушаване на технологичния процес с отделяне на опасни химически вещества;
- аварии при транспорт на опасни химически вещества.

В тази връзка целите на доклада са:

1. Да се направи класификация на аварията.
2. Да се определят потенциалните фактори и опасности за възникване на химически аварии на територията на България и най-често използваните ОХВ в промишлеността.

Изложение

Като „голяма авария“ се определя възникването на голяма емисия, пожар или експлозия, която става в резултат на неконтролируеми събития в хода на операциите на всяко предприятие или съоръжение, която води до сериозна опасност за

човешкото здраве или за околната среда. Тази опасност е непосредствена, забавена, вътре или вън от предприятието и включва едно или повече опасни вещества, класифицирани в една или повече от категориите на опасност [2].

Промислена авария - внезапна технологична повреда на машини, съоръжения, агрегати или извършване на дейности с рискови вещества и материали в производството, обработката, използването, съхраняването, натоварването, транспорта или продажбата им, когато това води до опасност за хората, общностите или околна среда [1, 3].

Съгласно Директива 96/82/ЕС – Севезо II и изменящата я Директива 2003/105/ЕС относно контрола на риска от големи аварии с опасни вещества изискванията на Закона за опазване на околната среда и Наредбата за предотвратяване на големи аварии с опасни вещества и за ограничаване на последствията от тях, предприятията, работещи на територията на България са класифицирани като „предприятия с висок рисков потенциал” и „предприятия с нисък рисков потенциал” [6]. Това са предимно предприятия от химическата промишленост, производството и търговията с взривни вещества, предприятия за нефтопреработка и търговия с петролни продукти и газ. Към 31.12.2013 г. числеността на „предприятия с съоръжения с висок рисков потенциал” наброява 76 броя, а регистрираните като „предприятия и съоръжения с нисък рисков потенциал” от големи аварии с опасни вещества са 99 [4].

Промислени обекти с висока степен на риск са [5]:

- „Лукойл Нефтохим“ АД - Бургас;
- „Юниън Миниер Пирдоп Мед“ АД - Пирдоп;
- „Полимери“ ЕАД - Девня;
- „Агрополихим“ ЕАД - Девня;
- „Неохим“ АД - Димитровград;
- „Оловно-цинков комбинат“ АД - Кърджали.

Промислени обекти със средна степен на риск са:

- „Комбинат за цветни метали“ ЕАД - Пловдив;
- „Свилоза“ АД – Свищов.

Промислени обекти с ниска степен на риск са:

- „Соловей-Соди“ АД - Девня;
- „Химко“ АД – Враца.

Химическите аварии могат да се обособят в няколко групи [7]:

1. *По своя произход:*

- по място на възникване биват – в производствените предприятия, стопанските обекти, при транспортиране на химически вещества и съхранението им;

- по вида на опасните вещества се делят на – токсични, запалителни, разяждащи, взривоопасни, опасни за околната среда;

- по вида на последствията се различават – кратковременни, средновременни (до няколко дни или няколко месеца) и трайни (от няколко месеца до няколко години и повече);

- по вида на ефектите от аварията се различават – аварии, при които съществува или не влияние върху други системи и дейности;

- по обема на аварията биват – в рамките на работното място, в рамките на предприятието, извън предприятието (в случай, когато са нанесени поражения на населението, околната среда, фирми в близост, инфраструктурата и др.);

- по възможността за ликвидиране се различават – аварии, при които е възможно или не ликвидиране на последствията.

2. *В зависимост от степента на замърсяване на въздуха, съществуват:*

- локални аварии със замърсяване на въздуха. Това са аварии, които засягат само отделен участък от производството и заразяват ограничено въздуха с ОХВ. Тези аварии са съпроводени с изтичане на малки количества ОХВ от тръбопроводи, апаратура съдове и отстраняването не изисква спиране на производството. От такъв тип аварии могат да бъдат поразени само отделни хора;

- местни аварии със замърсяване на въздуха. Това са аварии, при които изтича по-голямо количество ОХВ и се получава висока степен на замърсяване. Разпространението на ОХВ на площадката на предприятието не води до опасност от замърсяване извън обекта. Производството се спира частично или временно;

- крупни аварии със замърсяване на въздуха извън площадката на производството предприятие. Тези аварии предизвикват внезапно спиране на дейността и са свързани с големи материални щети. Когато замърсяването на въздуха се разпространява извън територията на предприятие, аварията често са съпроводени с експлозии, пожари и разпръскване на големи количества ОХВ. В резултат на това се създават големи огнища на химическо замърсяване, образуват се отровни облаци, които представляват опасност за хора, животни, растения и околната среда.

Въздействието на големите промишлени аварии често може да засегне територии не само в страната, но и извън националните граници. Като фактор за увеличаване на риска от големи аварии с отделяне на опасни вещества може да се посочат:

- природните бедствия (земетресения, наводнения, пожари, много ниски температури и др.), възникващи на територията на промишлените предприятия;

- транспортирането на опасни вещества (живак, пестициди, амоняк, хлор и други пожароопасни химически продукти) чрез сухоземен, воден или въздушен транспорт, които при катастрофа създават условия за замърсяване на околната среда и са заплаха за живота и здравето на населението;

- технологични аварии във фирми от фармацевтичната, химическата, металургичната и текстилната промишленост, както и в обекти, осъществяващи дейности по утилизация на боеприпаси и взривни вещества;

- аварии в складове и бази със запаси от промишлени отровни вещества;

- аварийни спирания или грешки в обслужването на технологичния процес;

- разрушаване на отделно съоръжение или на цяла група в резултат на механични повреди;

- корозия на метални тръбопроводи и цистерни, съхраняващи силно токсични и агресивни вещества;

- възникване на повреди или умишлено изключване на контролно-измервателната апаратура и автоматизирани устройства;

- умишлено прекъсване или аварии на преминаващи през страната продуктопроводи, нефтопроводи и газопроводи, които заедно с газовото хранилище „Чирен“ са потенциални пожароопасни и взривоопасни обекти;

- осъществяване на терористичен акт с разпръскване на опасни вещества.

Основните фактори при определяне на опасността от големи аварии с отделянето на химически вещества за даден обект, са видът и максималните количества ОХВ, които се употребяват или съхраняват на територията му. В зависимост от свойствата на ОХВ се определят и съответните сценарии за възникване и протича-

не на аварийните ситуации. От съществено значение при анализа е максималното разстояние, до което би достигнало въздействието от аварията и засегнатата площ.

В промишлеността и производството най-често се използват следните ОХВ: хлор, амоняк, серен диоксид, въглероден оксид, циановодородна киселина, фосген и дифосген, серовъглерод, фосфороводород и фосфорен трихлорид.

Заклучение

Потенциална опасност от възникване на големи аварии представляват хранилищата за нефтопродукти, втечнени и компресирани въглеводородни газове и компресорните станции за природен газ и други технологични газове, които могат да доведат до възникване на експлозии и пожари. Чувствителни са зоните и инфраструктурните обекти в близост до газопроводи. Поради това е необходимо приемането на подходящи превантивни действия за осигуряване на високо ниво на защита за населението и околната среда, и ограничаването на последствията от аварии.

Благодарности

Този доклад е подкрепен по Проект № РД-08-144/08.02.2016 г. “Ситуационен център за управление на кризи и реагиране при бедствия ”, финансиран от ШУ „Епископ Константин Преславски“.

Литература:

1. Закон за защита при бедствия, изм. ДВ. бр.81 / 20.10.2015.
2. Закон за опазване на околната среда, изм. ДВ. бр.101 / 22.12.2015.
3. Инструкция № 81213-953 за условията и реда за осъществяване на химическа, биологическа и радиационна защита при пожари, бедствия и извънредни ситуации, изм. ДВ. бр.104 / 16.12.2014.
4. Национален доклад за състоянието и опазването на околната среда. София, 2015.
5. Национален аварийен план за борба с нефтени разливи в Черно море. МС София, 2011, Приложение № 10.
6. Ръководство за класифициране на предприятия и съоръжения. <http://www.chemicals.moew.government.bg/chemical/site/File/manuals/Classification_guidance.pdf> (03.02.2016).
7. Сандев, Г. Лекции по Гражданска защита. Шумен, 2014.

НАЦИОНАЛНА СИСТЕМА ЗА ЗАЩИТА ПРИ БЕДСТВИЯ

Доника В. Диманова

Шуменски университет „Епископ Константин Преславски”, Шумен
Факултет по технически науки
e-mail: d.dimanova@gmail.com

NATIONAL SYSTEM FOR DISASTER PROTECTION

Donika V. Dimanova

ABSTRACT: *The National System for Disaster Protection is created to ensure the actions of the structures of the ESS management of forces and means of preventing and coping with calamitous nature and overcoming the consequences of such.*

KEY WORDS: *disaster protection, a national system, governance bodies, forces for disaster response.*

Въведение

Състоянието на Националната система за защита при бедствия и аварии е в пряка връзка с политическото и икономическото положение на страната, което дава отражение върху системите за сигурност в национален и регионален аспект.

Националната система за защита осигурява [4]: анализ и оценка на риска от възникване на бедствия и аварии, поддържане на готовност за действие при бедствия и аварии, постоянен обмен на информация, координация на действията на органите за управление и на силите за реагиране при бедствия и ефективно използване на наличните ресурси.

Основните компоненти на Националната система за защита при бедствия и аварии са функционално свързани и са:

- органи за управление;
- центрове на управление;
- комуникационно-информационна система;
- сили за реагиране при бедствия.

В тази връзка целта на доклада е да се направи анализ и оценка на основните компоненти на Националната система за защита при бедствия и аварии.

Изложение

Съгласно действащото законодателство, защитата при бедствия в Република България се извършва от **органите на изпълнителната власт**, юридическите лица и едноличните търговци в изпълнение на възложените им функции от Закона за защита при бедствия (чл. 3 и чл. 5) и други нормативни актове, регламентиращи тяхната дейност.

Съгласно Закона за защита при бедствия (чл.62), Министерският съвет (МС) формира държавната политика в областта на защитата при бедствия, като осъщест-

вява общото ръководство и предвижда финансови средства за защита при бедствия чрез създадения към него Консултационен съвет. Консултативният съвет включва представители на министерствата, ведомствата, Българската академия на науките, висши училища, научно-изследователски институти, Националното сдружение на общините в Република България и юридически лица, имащи отношение към защитата от бедствия.

В случай на заплаха или възникнали бедствия и аварии на територията на страната се предоставя еднаква по обем и съдържание информация за ситуацията на президента на Република България и на председателя на Народното събрание.

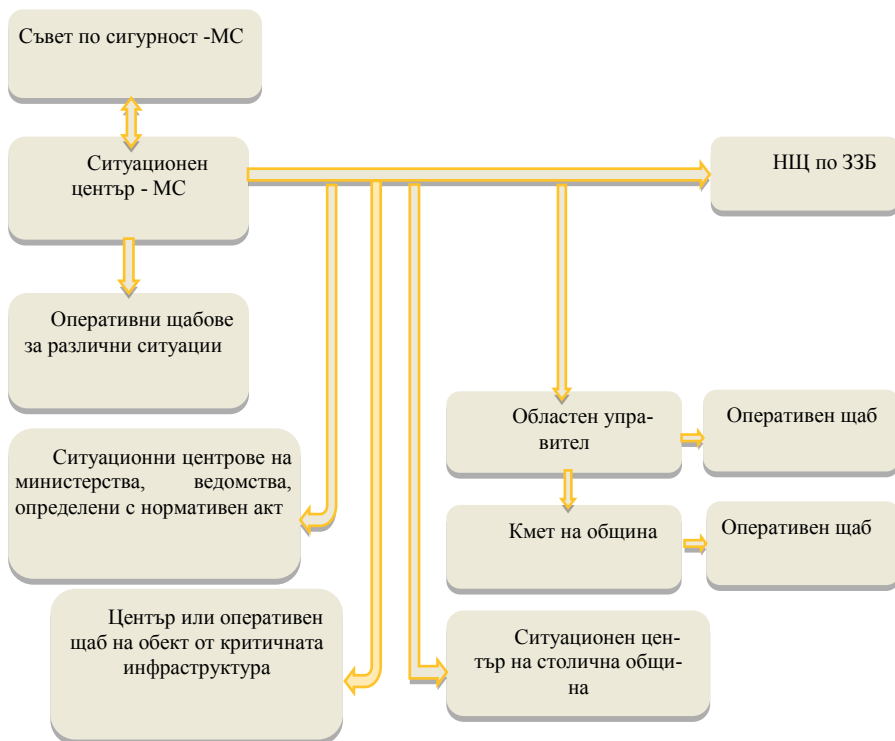
За по-ефективно функциониране на системата останалите органи на изпълнителна власт - министри, председатели на държавни агенции и държавни комисии, изпълнителни директори на изпълнителни агенции, получават конкретни задачи за ръководство на дейностите по управление на бедствия в подчинените им структури и в ръководената от тях сфера. Тези дейности са регламентирани и описани в Закона за защита при бедствия и Национална програма за защита при бедствия.

За подпомагане на ръководителите при вземането на решения при бедствия, са създадени звена за управление при бедствия, аварии и катастрофи.

В *центровете за управление* при бедствия е съсредоточена по-голямата част от управленския ресурс за оперативно управление. Центрове се създават в администрациите на МС, в министерствата, ведомствата, областните и общинските администрации, като се интегрират в единна система с непрекъснато оперативно дежурство и постоянно наблюдение.

При бедствие на територията на страната, министър-председателят със заповед въвежда Националния план за защита при бедствия, чрез който се създава Национален щаб. Към момента в състава на НЩ поименно са включени министри и заместник-министри, ръководители на ведомства и институции, имащи задължения за изпълнението на Националния план за защита при бедствия [1]. Това са министрите на: вътрешните работи; външните работи; регионалното развитие и благоустройството; здравеопазването; отбраната; транспорта, информационните технологии и съобщенията; икономиката, енергетиката и туризма; околната среда и водите; труда и социалната политика; земеделието и храните; културата; образованието и науката; председателят на ДА "Държавен резерв и военновременни запаси; БЧК; председателят на Агенцията за ядрено регулиране (АЯР); Геофизичният институт (ГФИ) към Българската академия на науката (БАН); Националният институт по метеорология и хидрология (НИМХ) към БАН; председателят на Националния статистически институт; областният управител на засегнатата област; кметът на засегнатата община; юридическите лица и едноличните търговци; Националното сдружение на общините в Република България; Националната ветеринарно медицинска служба; Национална служба по растителна защита и Националният медицински координационен център.

На фиг. 1 е представена система за управление при бедствия и аварии.



Фиг. 1. Система за управление при бедствия и аварии

Основните функции и дейности на Националния щаб са да [1]:

- анализира и оценява обстановката при бедствие;
- взема решения за необходимия обем и ресурсно осигуряване на спасителни и неотложни аварийно-възстановителни работи за предотвратяване, ограничаване и ликвидиране на последствията от бедствието и за подпомагането на засегнатото население;
- организира и координира действията на: министрите, ръководителите на ведомствата, областните управители, кметовете на общини, юридическите лица и едноличните търговци, на които са възложени функции за защита при бедствия;
- осъществява контрол по изпълнението на задачите и мерките за овладяване на бедствието;
- информира чрез медиите населението за развитието на бедствието, за предприеманите действия за неговото ограничаване и овладяване и за необходимите предпазни мерки и действия;

- докладва на министър-председателя, президента на Република България и на председателя на Народното събрание за хода на провежданите защитни мероприятия.

Дейността на НЩ се обслужва от ГДПБЗН към МВР, както и от компетентните с оглед характера на бедствието министерства, ведомства и институции. При необходимост се създават работни групи от експерти, чийто поименен състав е предварително определен и въведен в групи за оповестяване в Националната система за ранно предупреждение и оповестяване на органите на изпълнителната власт и населението при бедствия, аварии и катастрофи.

Освен НЩ, към всяко министерство и ведомство има изградени оперативни щабове или ситуационни центрове. Щаб за изпълнението на Националния план за защита при бедствия се сформира и на областно, и на общинско ниво, като се ръководи от областния управител или кмета на засегнатата община.

Комуникационно-информационната система е интегриран организационно-технически комплекс от органи, комуникационни и информационни ресурси, процедури и документи за осигуряване на обмен, обработка, съхранение и защита на информацията в системата за управление при бедствия [4].

Комуникационно-информационната система служи за обмен на информация между оперативни щабове или ситуационните центрове за управление на бедствия. Създаването на добра комуникационна и информационна среда дава възможност на органите за управление да моделират и да прогнозират естеството на бедствията. Целта е навременно получаване на актуална и точна информация, което дава възможност на органите за управление и силите за реагиране да вземат правилни решения в изпълнение на задачите си при различна оперативна обстановка. Като подсистема на комуникационно-информационната система е Националната система за ранно предупреждение и оповестяване, чрез която се информира населението и органите на изпълнителната власт при заплаха или възникване на бедствия. Информация и данни постъпват от много и различни източници като:

- данни от системи за мониторинг на метеорологични, хидрологични, сеизмологични, химически, радиологични, екологични, ядрени и други обекти и явления;
- информация за опасни явления от НИМХ, Агенцията за проучване и поддържане нивото на река Дунав;
- информация и данни от центрове на Националната система за спешни повиквания с единен европейски номер 112;
- информация и данни от географските информационни системи на Центъра за аерокосмическо наблюдение към МВР;
- от международния обмен на информация и данни.

Силите за реагиране при бедствия включват: Главна дирекция ПБЗН към МВР с нейните териториални звена, Областна дирекция на МВР (Районни управления полиция), центрове за спешна медицинска помощ, доброволни формирования, структурите на Българския червен кръст, въоръжените сили, министерства, ведомства, общини, търговски дружества и др. Те изпълняват дейности по предотвратяване и овладяване на бедствия и преодоляване на последиците от тях. При такива ситуации на територията на цялата страна или на част от нея законът предвижда възможност за обявяване на бедствено положение. Също като крайна мярка може

да бъде обявена и мобилизация на граждански ресурси за времето на бедственото положение, което става с решение на МС.

Заклучение:

Защитата на населението, инфраструктурата и националното стопанство при възникване на природни бедствия и аварии е комплексна дейност. В момента защитата се организира и осъществява от Главна дирекция ПБЗН, която е национална специализирана структура на МВР за пожарна безопасност и защита на населението при пожари, бедствия, аварии и катастрофи. Дирекцията осъществява дейността си самостоятелно или съвместно с органите на изпълнителната власт, юридическите лица и едноличните търговци в изпълнение на възложените им функции, при условията и по реда на Закона за Министерството на вътрешните работи, Закона за защита при бедствия (чл. 3 и чл. 5) и други нормативни актове.

Благодарности

Този доклад е подкрепен по Проект № РД-08-144/08.02.2016 г. “Ситуационен център за управление на кризи и реагиране при бедствия”, финансиран от ШУ „Епископ Константин Преславски“.

Литература:

1. Закон за защита при бедствия, изм. ДВ. бр.81 / 20.10.2015.
2. Национален план за защита при бедствия, МС София, 2010.
3. Национална програма за защита при бедствия 2014 – 2018. МС София, 2013.
4. Правила за организацията на дейността на МВР при извънредни ситуации. София, 2012.

ФУНКЦИИ НА ОРГАНИТЕ НА ИЗПЪЛНИТЕЛНА ВЛАСТ ЗА ЗАЩИТА ПРИ БЕДСТВИЯ

Доника В. Диманова

Шуменски Университет „Епископ Константин Преславски“, Шумен
Факултет по технически науки
e-mail: d.dimanova@gmail.com

FUNCTIONS OF THE EXECUTIVE AUTHORITIES TOR DISASTER PROTECTION

Donika V. Dimanova

ABSTRACT: Accordance with the effective legislation, disaster protection in Bulgaria is carried out by the executive authorities, legal persons and sole traders in the performance of their duties of the Law on Disaster Protection and other normative acts regulating their activities.

KEY WORDS: *planning, disaster protection, governance bodies*

Въведение

Защитата на населението при бедствия се планира и провежда от органите на изпълнителната власт, които организират и координират [3]:

- анализа, оценката и прогнозата за характера и последствията от най-често проявяващите се бедствия;
- разработване и актуализиране на планове за защита при бедствия;
- провеждане на мероприятия за усвояване на планове;
- поддържане на непрекъснато денонощно дежурство;
- формиране и поддържане на сили и средства за провеждане на спасителни и неотложни аварийно-възстановителни работи във възникналите огнища на поражения (заразяване) на територията на страната;
- създаване на организация за действие и взаимодействие между органите за управление и силите за провеждане на мероприятия по защитата на населението и извършване на спасителни и неотложни аварийно-възстановителни работи;
- поддържане в добро състояние на общинските и местните пътища;
- защита на водоизточниците, поддържане на готовност при недостиг на питейна вода за осигуряване на допълнителни пунктове за снабдяване с вода и включване във водоснабдителната система на допълнителни водоизточници;
- осигуряване (в министерствата, ведомствата и в техните структури) на финансови и материални средства за комплектуване, обучение и поддържане в постоянна готовност на органите за управление и силите за реагиране при бедствия;
- дейности по осигуряване на производството и доставката на основни строителни материали за нуждите на неотложните аварийно-възстановителни работи;

- участие на дружествата със строително-монтажна и пътностроителна дейност във възстановителните работи и по осигуряване и поддържане на пътища;
- организиране на експертни и проектантски екипи за участие в работата по планиране на защитата и инженерното осигуряване на спасителните и аварийните дейности;
- информиране на населението за възможните бедствия на територията на страната, както и за правилата за действие и поведение при възникването им.

Изложение

Съгласно Закона за защита при бедствия (чл.62), Министерският съвет формира държавната политика в областта на защитата при бедствия, като осъществява общото ръководство и предвижда финансови средства за защита при бедствия чрез създадения към него Консултационен съвет. Консултативният съвет включва представители на министерствата, ведомствата, Българската академия на науките, висши училища, научно-изследователски институти, Националното сдружение на общините в Република България и юридически лица, имащи отношение към защитата от бедствия.

Министерски съвет в рамките на своята компетентност приема [2]:

- Национална програма за защита при бедствия и годишни планове за изпълнението ѝ;
- Национален план за защита при бедствия;
- Стратегия за намаляване на риска от бедствия;
- Правилник за устройството и дейността на Консултативния съвет;
- въвежда Национална система за ранно предупреждаване и оповестяване на органите на изпълнителната власт и населението при бедствия и определя с наредба условията и реда за функционирането ѝ по предложение на министъра на вътрешните работи;
- Национален план за провеждане на спасителни и неотложни аварийно-възстановителни работи;
- Наредба за условията и реда за провеждане на временно извеждане, евакуация и разсредоточаване;
- Национална система за спешни повиквания с единен европейски номер 112 и Правилник за организацията и дейността на центровете за приемане на спешни повиквания към него;
- Наредба за реда за създаване и организиране на дейността на доброволните формирования за предотвратяване или овладяване на бедствия, пожари и извънредни ситуации и отстраняване на последиците от тях;
- Наредба за реда начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях;
- Правилник за организиране на дейността на Междуведомствената комисия за възстановяване и подпомагане;
- предвижда финансови средства за защита при бедствия.

При бедствие министър-председателят на Република България въвежда в действие Националния план за защита при бедствия, чрез който се създава Национален щаб (НЩ).

В случай на заплаха или възникнали бедствия на територията на страната се предоставя еднаква по обем и съдържание информация за ситуацията на президента на Република България и на председателя на Народното събрание.

Министрите и органите от ЕСС извършват спасителни операции в рамките на своята компетентност, като [1, 2]:

- предприемат мерки за намаляване на риска от бедствия;
- участват в разработването на Националния план за защита при бедствия и планират и осигуряват неговото изпълнение;
- поддържат в готовност сили и средства и осигуряват участието на подчинените си структури като съставна част на единната спасителна система в съответствие с Националния план за защита при бедствия;
- извършват контрол за изпълнението на мерките по защитата в съответствие с делегираните им от законите правомощия.

В рамките на своята компетентност областният управител [2, 4]:

- организира и ръководи защитата при бедствия в областта;
- организира и отговаря за обучението на областната администрация, за начините на поведение и действие при бедствия и за изпълнение на необходимите защитни мерки;
- организира и контролира изпълнението на превантивни мерки за недопускането или намаляването на последиците от бедствия;
- координира и контролира подготовката за предотвратяване на бедствия, извършвана от областната администрация, териториалните звена на министерствата и ведомствата, юридическите и физическите лица в областта;
- одобрява програма за почистване на речните участъци и контролира дейностите по почистването извън границите на урбанизираните територии, като назначава междуправителна комисия;
- създава организация за оповестяване при бедствия;
- предоставя данни за изготвянето на Националния план за защитата при бедствия;
- представя в МВР ежегоден доклад за дейността по защитата при бедствия;
- създава със заповед Щаб за изпълнение на областния план за защита при бедствия и за взаимодействие с НЩ.

При възникване на бедствие на територията на областта областният управител [2]:

- въвежда със заповед в изпълнение областния план за защитата при бедствия;
- може да обяви бедствено положение на територията на областта или на част от нея;
- организира, координира и контролира процеса на подпомагане и възстановяване при бедствия;
- координира спасителните и неотложните аварийно-възстановителни работи, възникнали на територията на областта, когато те излизат извън територията на една община, както и когато кметът на общината е поискал това.

В рамките на своята компетентност кметът на община [2, 4]:

- организира и ръководи защитата при бедствия на територията на общината;
- организира, координира и провежда превантивни мерки за недопускането или намаляването на последиците от бедствия;

- планира в проекта на общинския бюджет финансови средства за осигуряване на дейностите по защита при бедствия в общината, както и резерв за неотложни и непредвидени разходи, свързани със защитата на населението;

- изгражда, поддържа и включва в дейностите по защитата създадените доброволни формирования съгласно Закона за защита при бедствия и Закона за МВР;

- одобрява програмата за планово почистване на речните участъци и издава заповед за определяне на участъци от реките с намалена проводимост като назначава междуведомствена комисия;

- осъществява своевременното оповестяване и информиране на населението при заплаха от възникване или за възникнало бедствие;

- представя на областния управител ежегоден доклад за дейността по защитата при бедствия;

- създава със заповед щаб за изпълнение на общинския план за защита при бедствия и за взаимодействие с щабове.

При възникване на бедствие на територията на общината кметът [2, 3]:

- въвежда със заповед в изпълнение общинския план за защита при бедствия;

- може да обяви бедствено положение на територията на общината;

- извършва обмен на информация с оперативния център на ГДПБЗН към МВР в областта;

- може да привлича юридически и физически лица за предоставяне на лична или материална помощ в съответствие с възможностите им;

- може да включва в дейностите по защитата и създадените доброволни формирования;

- може да поиска координация от областния управител;

- организира и координира временното извеждане и предоставя неотложна помощ на пострадалите лица;

- организира и координира предоставянето на възстановителна помощ на населението при бедствия;

- организира и контролира извършването на неотложни възстановителни работи при бедствия.

Заклучение

За по-ефективно функциониране на системата останалите органи на изпълнителна власт - министри, председатели на държавни агенции и държавни комисии, изпълнителни директори на изпълнителни агенции, получават конкретни задачи за ръководство на дейностите по управление на бедствия в подчинените им структури и в ръководената от тях сфера. Тези дейности са регламентирани и описани в Закона за защита при бедствия и Национална програма за защита при бедствия. За подпомагане на ръководителите при вземането на решения при бедствия, са създадени и звена за управление при бедствия.

Благодарности

Този доклад е подкрепен по Проект № РД-08-144/08.02.2016 г. "Ситуационен център за управление на кризи и реагиране при бедствия ", финансиран от ШУ „Епископ Константин Преславски“.

Литература

1. Закон за администрацията, изм. ДВ. бр.27/25.03.2014.
2. Закон за защита при бедствия, изм. ДВ. бр.81 / 20.10.2015.
3. Национален план за защита при бедствия, МС София, 2010.
4. Национална програма за защита при бедствия 2014 – 2018. МС София, 2013.
5. Стратегия за национална сигурност на Република България, МС София, 2011.

ПРОБЛЕМЪТ ЗА РИСКА В ОРГАНИЗАЦИЯТА

Красимир М. Марков

*Шуменски университет „Епископ Константин Преславски”
Педагогически факултет, катедра „Педагогика и управление на образованието”*

PROBLEM OF RISK IN THE ORGANIZATION

Krasimir M. Markov

ABSTRACT: *Discuss the problems of risk in the organization in terms of risk management by analyzing the process of risk management in the organization in terms of negative and positive consequences for her.*

KEY WORDS: *risk management organization, consequences*

Практиката, включително и в България в последните години убедително показва, че независимо от типа на организацията стабилността на нейното развитие определено зависи от възможностите ѝ да прецени и в известни степени да управлява риска. Следователно става дума за така наречения мениджмънт на риска. Авторите, изследващи този проблем [4; 6; 7; 8; 9], считат, че той представлява система за управление на риска насочена към постигане на необходимия баланс между получените приходи и съкращаване на разходите от дейността в организацията и в този смисъл мениджмънта на риска се явява съставна част на цялостния мениджмънт на организацията, което само по себе си означава, че той би трябвало да бъде включен както в общата ѝ политика, така и в нейните бизнес планове и дейност. Това се счита за необходимо условие за ефективност. От друга страна сам по себе си мениджмънта на риска предполага необходима култура и инфраструктура на бизнеса насочена към [4]:

- изясняване на причините и основните фактори за възникване на риска;
- идентификация, анализ и оценка на рисковете;
- вземане на решение въз основа на направената оценка;
- изработване на антирисковото управляващо въздействие;
- снемане риска до приемливо ниво;

- организация на изпълнението на набелязаната програма;
- контрол върху изпълнението на планираните дейности;
- анализ и оценка на резултатите от рисковото решение.

Ако бъдат изпълнени тези условия ще се осигури стабилност на развитието на организацията и ще се повиши обосноваността на приемането на решения в рисковите ситуации.

Същевременно в литературата изследваща проблема се сочи, че съществуват определени предпоставки, които следва да осигурят прилагането на рисковия мениджмънт. От една страна всички организации се сблъскват с необходимостта да се управляват различни видове рискове, което означава, че ръководството на организацията трябва да осигури възможността, необходимостта от прилагането на мениджмънта на риска да се признава от всички звена в организацията и от целия персонал в качеството си на фактор с първостепенна важност. Условия за това са следните особености на мениджмънта на риска [4;6]:

- управлението на риска е свързано както с благоприятни, така и с неблагоприятни последствия като същността на това управление е в това да се определят възможните отклонения от планираните резултати с цел те да се управляват, за да се подобрят перспективите, да се съкратят разходите и да се подобри обосноваността при вземане на решение;

- управлението на риска означава да се определят перспективите и да се изясняват възможностите за усъвършенстване на дейността от една страна, а от друга страна да се съкрати или да не се допуска нежелан ход на събитието;

- управлението на риска предполага анализ на условията за вземане на решение и в този смисъл това е логичен и систематичен процес, който следва да се разбира като възможност за избор на път за по-нататъшно усъвършенстване на дейността и повишаване на ефективността на организацията;

- управлението на риска изисква мислене в перспектива, в крайна сметка ние се мъчим да установим какво може да се случи и същевременно как бихме могли да реагираме като осигурим готовност за това, което ще се случи. Това означава, че мениджмънта на риска в никакъв случай не е реактивен. Създаването на възможна формална структура работеща по мениджмънта на риска позволява да имаме налице система за управление на организацията, чиято дейност е насочена към предупреждаването на ръководството и органите в организацията за възникването на възможни проблеми;

- управлението на риска изисква ясно разпределение на отговорностите и пълномощията, които е необходимо да има във връзка с вземането на решение. Естествено е, че висшето ръководство в организацията ще носи и най-високата отговорност за управлението на рисковете. Неговите най-големи пълномощия всъщност са в разпределението между органите в организацията на отговорностите и пълномощията, което означава, че то е длъжно да намери най-добрия баланс между отговорността за риска и способността този риск да бъде контролиран;

- управлението на риска зависи от ефективния процес на взаимодействието между участниците в мениджмънта на риска. В крайна сметка процесът на управление на риска се осъществява както във вътрешната, така и във външната среда на организацията, което налага необходимост от взаимодействие между вътрешните и външните участници в процеса.

– Сам по себе си мениджмънта на риска има определени преимущества, които имат своята характеристика. Те могат да бъдат определени така [1;2;3;8;9]:

– първо преимущество – снижаване на фактора на неопределеност при осъществяване на дейността на организацията – характеризира се с контрол над негативните събития, които съпровождат конкретните действия, отнасящ се до намаляване на вероятността за тяхното възникване и намаляване на тяхното влияние;

– второ преимущество – използване на перспективните възможности за подобрене – характеризира се с идеята, че в процеса на управлението на риска има възможност да се оценят благоприятните възможности за организация в рискова ситуация. Това е много по-ефективно, ако персонала осъзнава риска и има навиците за неговото управление;

– подобряване на планирането и повишаване на ефективността на дейността – характеризира се с използването на обективните налични данни за организацията, нейните цели и перспективи за подобряване качеството на планирането;

– икономия на ресурси – характеризира се с предварителния разчет на икономическата целесъобразност от провеждането на една или друга дейност в организацията;

– подобряване взаимоотношенията с заинтересованите страни – характеризира се с идеята, че в процеса на управлението на риска сътрудниците на организацията се явяват заинтересована вътрешна страна, което предполага наличието на диалог и обмяна на мнение между тях и ръководството на организацията, явяващ се информационен канал за ръководството, даващ сведения за това как заинтересованата страна би реагирала на съответните промени;

– повишаване на качеството на информацията при приемането на решения – характеризира се с идеята, че сам по себе си процесът на управлението на риска повишава точността на информацията и анализа, които пък са необходими за приемането на стратегически решения на различни нива на управлението в организацията;

– ръст на деловата репутация – характеризира се с идеята, че всички които работят със съответната организация искат да работят с нея, ако тя е доказала себе си като надежден партньор, който управлява своите финансови и производствени рискове;

– поддръжка от страна на учредителите – характеризира се с идеята, че качествено управление на рисковете повишава авторитета на ръководството на организацията в очите на нейните учредители;

– контрол на дейността на организацията и хода на реализирането на инвестиционни проекти – характеризира се с факта, че в управлението на риска особено внимание се отделя на въпросите свързани с мониторинга и измеренията на бизнес процесите, което осигурява твърд контрол върху реализацията на инвестиционните програми.

Вече споменахме, че процесът на управление на риска трябва да съпровожда управлението на решение на всички нива на мениджмънта на организацията и както подчертахме, само по себе си, управлението на рисковете трябва да се интегрира в целия мениджмънт на бизнес процеса или в неговите съставни части. Това се отнася и към изменението на политиката и към представянето на нови стратегии, и процедури, и към управлението на проекти и инвестиции, и към оптимиза-

цията при разрешаването на вътрешно-организационни конфликти и противоречия.

В чисто приложен аспект можем да кажем, че при изследването на процеса на управлението на риска се оказват няколко практически сфери на приложение. Анализирането на литературата посветена на мениджмънта на риска позволява тези сфери на приложение ориентировъчно да бъдат сведени до [1;2;3;4;6;7]:

- стратегическо, оперативно и бюджетно планиране;
- управление на активите и планиране на разпределението на ресурсите;
- изменения в предприемаческата дейност, които могат да имат стратегически, технологичен и организационен характер;
- проектиране и разработване на нови видове продукция;
- мениджмънт на качеството;
- социални аспекти на взаимодействието с обществеността;
- екология и опазване на околната среда;
- делова и професионална етика;
- въпроси на гражданската отговорност;
- информационна сигурност;
- анализ на изискванията на потребителите и оценка на възможностите за тяхното изпълнение;
- оценка на съответствието на бизнес процесите с изискванията предявени към тях;
- проблеми на здравословните и безопасни условия на труд;
- управление на проекти;
- управление на сделки, доставчици и покупки;
- управление на подчинени организации;
- управление на персонала;
- корпоративно управление.

Осъществяването на каквато и да е дейност свързана с предприемачество в една или друга степен винаги е свързана с риск. От гледна точка на мениджмънта на риска отличителни признаци на предприемачеството, което е необходимо да отчитаме при анализа и оценка на последствията от риска са [4;6;8;9]:

- насоченост на организацията към получаване на печалба от своята дейност;
- диференциация по видовете на предприемаческа дейност;
- отговорност по договорените обвързаности с клиентите;
- необходимост от вземане на управленски решения с отчитане на последствията от риска.

От казаното дотук е видно, че основна цел на мениджъра по управление на риска е да създаде такава ситуация, че даже и най-лошият вариант на развитието на събитията да предполага сравнително малко намаление на планираните резултати и гарантиране на по-нататъшното съществуване на организацията. Самата поява на предприемачески риск е обективно неизбежна, което се обуславя от две основни причини – неопределеност на условията в предприемаческата среда и ограниченост на ресурсите на организацията. Ако трябва да бъдат изброени факторите влияещи върху неопределеността на средата бихме могли да посочим като такива следните:

- нестабилност на макросредата на пазарните отношения;

- неопределеност на политическата и социалната ситуация;
- отсъствие на пълна и достоверна информация за външната среда;
- ограничена възможност на мениджъра да възприема и преработва постъпващата информация;
- случайно появяване на неблагоприятни събития в процеса на самата дейност;
- противодействие на участниците на пазара.

Ясно е, че рискът се поражда основно от неопределеността на средата. Именно в тази неопределеност са скрити причините, факторите на риска и рисковата ситуация.

Причини на риска са самите негови източници – икономически, политически, социални, екологични, технологични и други условия на общественния живот и на средата.

Фактори на риска – това са обстоятелствата при които се появяват причините за риска. Те са и тези, които водят до рисковата ситуация.

Рискова ситуация – събитие, което се обуславя от причините и факторите на риска и може да доведе до негативни или позитивни последици за организацията.

В крайна сметка анализирайки проблема за риска в организацията на база на проучената литература бихме могли да обобщим следното:

- рискът, това е съотношението между вероятността за възникване на рискова ситуация и нейните възможни последици;
- рискът трябва да се разглежда главно по отношение на планирания резултат, т.е., на целите, които се стремим да постигнем чрез дейността на организацията;
- мениджмънта на риска предполага да се вземат решения за неговото управление при наличие на няколко алтернативи, които определят възможността за използването на ограничените ресурси;
- възможността да не се достигнат планираните резултати е следствие от вероятностната природа на пазарната дейност;
- рискът характеризира степента на недостигане на поставените цели и възможните последици за организацията.

Което означава, че в заключение бихме могли да кажем, че технологията на риск-мениджмънта се основава на представата за него като за целенасочена дейност на ръководството на организацията предполагаща структуриране на процеса на управление на риска.

Литература:

1. Кузманов, З. Политики на Европейския съюз при управление на кризи. Сборник научни трудове от Научна конференция 2014 „Новата парадигма за сигурност в киберпространството“, НВУ „В. Левски“, факултет „Артилерия, ПВО и КИС“, Ш., 2014
2. Кузманов, З. Политики на Руската Федерация при управление на кризи. Сборник научни трудове от Научна конференция 2014 „Новата парадигма за сигурност в киберпространството“, НВУ „В. Левски“, факултет „Артилерия, ПВО и КИС“, Ш., 2014
3. Кузманов, З. Политики на Съединените американски щати при управление на кризи. Сборник научни трудове от Научна конференция 2014 „Новата парадиг-

ма за сигурност в киберпространството“, НВУ „В. Левски“, факултет „Артилерия, ПВО и КИС“, Ш., 2013

4. Марцынковский Д. А., А. В. Владимирцев, О. А. Марцынковский. Руководство по риск-менеджменту. Береста, СПб., 2007

5. Петров А. Н. и др., Стратегический менеджмент. Питер СПб. 2005

6. Ступаков В. С., Г. С. Токаренко. Риск-менеджмент. Финансы и статистика, М., 2005

7. Тренев Н. Н. Стратегическое управление. Уч. пос. М., 2000.

8. Robey P., Sales A. Designing organizations. Burr, 1996.

9. Rowe A., Mason R., Dickel K. Strategic management. N.Y., 1996.

ГЛОБАЛНАТА БОРБА С ИЗМЕНЕНИЕТО НА КЛИМАТА

Велико П. Петров, Калоян А. Илиев

“Vasil Levski” National Military University, “Artillery, Air-defence and Communication and Information Systems” Faculty, “Organization and management of the Field Artillery tactical formations” Department; town of Shumen.

GLOBAL FIGHT AGAINST CLIMATE CHANGE

Veliko P. Petrov, Kaloyan A. Iliev

ABSTRACT: This report aims to acquaint readers with one of the greatest global challenges of our time, namely climate change, making it necessary to take immediate action and cooperation between (local, regional and national) authorities and international organizations from all over the world. Combating climate change is a major item on the agenda of the international community and the European Union. Undoubtedly the problem of climate change is an issue of international environmental law and that as a statutory regulator should set the framework in which this problem can be resolved. They are tracked over time some of the most important initiatives related to the problems of climate World Meteorological Organization and the European Union. The first multilateral agreement on climate change is the Agreement of Paris (the "Global Agreement"), which covers almost all emissions worldwide. It is a success for the world and the confirmation of the EU to go on the road to a low carbon economy. Crucial to the conclusion of this agreement was a negotiation strategy of the EU and he led by his experience in conducting effective policy change, pushing for ambitious results.

KEY WORDS: global climate change, greenhouse gases, an ozone hole, global fight against climate change

Изменението на климата е едно от най-големите предизвикателства, с които човечеството ще трябва да се справи през следващите години. Повишаващите се

температури, топящите се ледове и все по-честите суши и наводнения са доказателство, че изменението на климата е факт. Рисковете за цялата планета и за бъдещите поколения са огромни и затова са необходими спешни мерки.

Някои от последици от изменението на климата са:

- покачването на морското равнище заплашва ниско разположените островни държави и крайбрежни общности;
- екстремните климатични условия застрашават производството на храни, особено в най-бедните развиващи се държави;
- жегите през изминалото десетилетие причиниха преждевременната смърт на хиляди хора в Европа;
- недостигът на вода и храна може да предизвика регионални конфликти, глад и поява на бежанци;
- някои растителни и животински видове ще бъдат изложени на нарастващ риск от изчезване;
- ако не се адаптираме към изменението на климата, се очаква дължащите се на това разходи да достигнат поне 100 млрд. евро годишно до 2020 г. за ЕС като цяло².

Ако температурата на Земята се повиши с повече от 2 °C над равнищата от преди индустриалната епоха, има вероятност изменението на климата да стане необратимо, а последиците в дългосрочен план могат да бъдат неизмерими. Големи части от много европейски страни с малка надморска височина, могат в крайна сметка да изчезнат под покачващото се равнище на моретата. В много части на света може да се стигне до недостиг на питейна вода за всички. Извънредните метеорологични явления, причиняващи разрушения и икономически щети, вероятно ще стават все по-чести. Някои икономики могат да западнат заради цената на приспособяването към променения климат. Международната общност се сблъсква с един от най-важните проблеми към настоящия момент, като промяната на климата, защото други глобални проблеми като запазване на биологичното разнообразие, опазване на чистата питейна вода, опазване на морето и горските масиви, бедността, осигуряването на храна и условия за добър живот неизменно ще бъдат (и са) повлияни от случващите се промени в глобалния климат.

Средната температура на Земята е била сравнително стабилна в продължение на 10 000 години до индустриалната революция, а от 1850 г до сега се правят редовни и точни измервания и тя се е повишила с 0,76 °C. Ако не се предприемат мерки, вероятно е през настоящото столетие тя да се повиши с още 1,8-4 °C, като е възможно това увеличение да достигне дори 6,4 °C според международната група от учени, свикана от Организацията на обединените нации (ООН). В момента е в ход надпревара с времето да не се допусне повишаването на температурата на планетата да достигне до това, което се смята за повратна точка – увеличение от 2 °C. Тази надпревара най-вероятно ще бъде загубена, ако емисиите в глобален мащаб не бъдат стабилизирани най-късно до около 2020 г. и ако след това до 2050 г. не бъдат намалени до около половината от равнищата им от 1990 г.

Изменението на климата има два аспекта:

- **смекчаване** означава намаляване на емисиите на парникови газове от всички сектори на икономиката и от ежедневиия ни живот. За целта се изпълняват различ-

² Политиките на Европейския съюз: Действия в областта на климата, Европейски съюз, ноември 2014 г., стр. 4.

ни мерки за енергийна ефективност, за преминаване към горива с ниски нива на емисиите на въглероден диоксид и др.;

– **адаптация** означава предприемане на действия за приспособяване към измененията на климата, които вече са настъпили. Адаптационните мерки също се отнасят до всички сектори на икономиката и до ежедневието ни, включително до здравето на хората.

Борбата срещу изменението на климата е основна точка в дневния ред на международната общност и Европейския съюз (ЕС). През 1972 г. ООН провежда първата международна конференция по „Човешката среда“ в Стокхолм (Швеция). От тази конференция води началото си принципа **„Мисли глобално, действай локално“**. При откриването и локализирането на нарастващата „озонова дупка“ над южния полярен регион в началото на 80-те години на XX в. се прие Виенската конвенция за защита на озоновия слой (1985 г.), която беше последвана от Монреалския протокол за веществата, които нарушават озоновия слой (1987 г.), който фокусира вниманието върху доста по-широкия и по-сложен въпрос за влиянието на парниковите газове върху глобалната атмосферна система.

Учените смятат, че повишаването на концентрацията на антропогенно произведените парникови газове в атмосферата е основният виновник за промяната на климата. Изтъняването на озоновия слой позволява по-голяма част от ултравиолетовите лъчи от по-вреден тип да достигат земната повърхност и по този начин е предпоставка за увеличаването на нанасяните от тях щети на гените на живите организми.

Към края на 80-те години промяната на климата вече е поставена в дневния ред на проблемите на международната общност и през 1988 г. Общото събрание на ООН приема Резолюция 43/53 за запазването на глобалния климат за настоящите и бъдещите поколения на човечеството. В нея се посочва, че проблемът „засяга до цялото човечество“ и се обявяват действията на Програмата за околната среда на ООН (UN Environment Programme) и Световната метеорологична организация (WMO) по общ проект за създаване на Междуправителствен комитет за климатичните промени (*Intergovernmental Panel on Climate Change – IPCC*). Неговата цел е „да предоставя международно координирани научни оценки на интензитета, времето и потенциалното влияние на климатичните промени върху околната среда, икономиката и обществата и да създава реалистични стратегии в отговор“. Две години по-късно, през 1990 г., с Резолюция 45/212 на Общото събрание на ООН се създава Междуправителствен преговорен комитет, който да разработи правен инструмент, който да обхваща климатичните промени. Последващите две години на интензивни преговори довеждат до създаването на Рамковата конвенция на ООН по изменение на климата (United Nations Framework Convention on Climate Change – UNFCCC) през 1992 г.³

Рамковата конвенция на ООН за измененията на климата (РКОНИК), която е подписана през 1992 г. по време на Конференцията на ООН по околна среда и развитие в Рио де Жанейро, Бразилия и е ратифицирана от 194 държави. Конвенцията влиза в сила на 21 март 1994 г. *Основната цел на конвенцията* (заложена в чл. 2), е не да спре емитирането на парникови газове, а да ги стабилизира на „ниво,

3 Иво Емануилов, Климатичните промени като проблем на международното екологично право. Перспективите за международноправно споразумение след Копенхагенската конференция на ООН през 2009 г., стр. 3

което би предотвратило опасна антропогенна намеса върху климатичната система”. Този член продължава, като поставя изискването това стабилизиране да бъде „достигнато в рамките на период от време, който да е достатъчен за естественото приспособяване на екосистемите към изменението на климата, да не застрашава производството на храни и да дава възможност за осъществяване на устойчиво икономическо развитие”. Тя очертава общата рамка на международните усилия за справяне с предизвикателствата, породени от изменението на климата и приема принципа за „общи, но диференцирани отговорности“. Според нейните разпоредби правителствата на страните-членки:

- събират и обменят информация за емисиите парникови газове, националните си политики и най-добри практики – чрез т. нар. Национални съобщения и годишни Национални инвентаризации на парникови газове;
- изготвят национални стратегии за смекчаване на и адаптиране към очакваните последици от изменението на климата;
- си сътрудничат в подготовката за адаптиране към последиците от изменението на климата, включително чрез предоставянето на финансова и технологична помощ за развиващите се страни.

През декември 1997 г. е подписан Протоколът от Киото (ПК), но влиза в сила на 16.02.2005 г. с който се въвеждат количествени ангажменти на страните по РКОНИК за намаляване на емисиите на парникови газове (ПГ) през периода 2008-2012 г. спрямо базовата 1990 г. (за България базовата година е 1988 г.).

Протоколът от Киото към РКОНИК е първият правно обвързващ глобален инструмент, ангажиращ развитите държави с конкретно количествено намаляване на техните емисии парникови газове. Съгласно Протокола индустриализираните държави като цяло трябва да намалят емисиите си на шест парникови газа с около 5% спрямо нивата от 1990 г. през т. нар. „първи период на задължения“ от 2008 до 2012 г. За развиващите се страни не са определени цели за емисиите. Протоколът предвижда намаленията да се постигнат както чрез редуциране на емисиите в самите държави, така и посредством инвестиции в пречистващи или по-екологосъобразни технологии в други страни (т. нар. гъвкави механизми по Протокола от Киото).

Световната метеорологична организация (СМО) е специализираната агенция на ООН по въпросите на времето, климата и водите. Една от основните задачи и дейности на СМО е да координира и обобщава наблюденията върху промените в състава на атмосферата и глобалния климат. Тези наблюдения се извършват унифицирано за всички 189 страни членки, с цел съпоставимост и сравнимост на резултатите. Някои от по-важните инициативи на СМО и ЕС, свързани с проблемите на климата, са представени накратко в таблица 1.

Таблица 1.

По-важни инициативи, свързани с проблемите на климата
на Световната метеорологична организация и ЕС

1979 г.	СМО организира Първата световна климатична конференция (СКК-1).
1988 г.	СМО и Програмата на ООН за околна среда създават Междуправителствената група от експерти по изменение на климата (IPCC).
1990 г.	Излиза Първият доклад за оценка на промените в климата на IPCC. От 1990 г. насетне IPCC създава четири такива доклада, съдържащи оцен-

	ка на климатичните промени. Те разширяват по обхват, детайли и задълбоченост статистическия анализ през годините. Първият доклад, публикуван през 1990 г., засяга науката и влиянието на климатичните промени.
1990 г.	СМО организира Втората световна климатична конференция (СКК-2).
1992 г.	Провежда се Конференцията на ООН по околна среда и развитие в Рио де Жанейро, по време, на която е подписана Рамковата Конвенция на ООН за изменението на климата (РКОНИК), влязла в сила през 1994 г.
1995 г.	Излиза Вторият доклад за оценка на промените в климата на IPCC и покрива икономическите и социалните измерение на промените на климата.
1995 г.	Провежда се Първата сесия на Конференцията на страните (COP-1) по РКОНИК.
1997 г.	Подписва се Протоколът от Киото, който влиза в сила през 2005г.
2001 г.	Излиза Третият доклад за оценка на промените в климата на IPCC и включва синтез на предишните доклади на IPCC и адресира широк кръг от политически свързани въпроси.
2003 г.	Директива 2003/87/ЕС въвежда Европейска схема за търговия с квоти на емисии на парникови газове, която влиза в сила за България като член на ЕС от 01.01.2007г.
2005 г.	ЕС стартира своята система за търговия с емисии (СТЕ на ЕС)
2007 г.	Излиза Четвъртият доклад за оценка на промените в климата на IPCC. Четвъртият доклад от 2007 г. се състои отново от синтез на предишните доклади плюс доклади от всяка от трите работни групи на IPCC (Working groups - WG), които се отнасят до: научните основания на климатичните промени (WGI), влиянието на климатичните промени, включително уязвимостта и адаптируемостта към тях (WGII) и намаляване на вредните ефекти от тях (WGIII).
2008 г.	Приема се политика на ЕС – пакет „Енергетика и климат“, основана на следните цели: ● намаляване на емисиите на ПГ до 2020 г. най-малко с 20 % в сравнение с 1990г.; ● намаляване с 20 % на потреблението на енергия спрямо предвижданията за 2020 г.; ● увеличаване до 20 % на дела на възобновяеми енергийни източници (ВЕИ) в общото енергийно потребление на ЕС до 2020г. (за България националната цел е от 16 %); ● задължителен за всички държави членки минимум от 10 % дял на биогоривата спрямо цялостното потребление на бензин и дизелови горива за транспорта до 2020г.
2009 г.	СМО организира Третата световна климатична конференция (СКК-3).
2009 г.	Провежда се 15-та сесия на Конференцията на страните (COP-15) по РКОНИК. От 7 до 18 декември 2009 г. в датската столица се състоя 15-та сесия на Конференцията на страните (COP-15) по РКОНИК, в която взеха участие делегации от 192 държави - страни по Конвенцията, международни правителствени и неправителствени организации и граждански движе-

	ния. Основна цел на тази сесия бе постигане на обща позиция за справяне с климатичните промени и по-точно за ограничаване покачването на глобалната температура до не-повече от 2 градуса в сравнение с доиндустриалните стойности. Постигането на международно споразумение за периода след 2012 г. е наложително поради изтичането на договореното по Протокола от Киото, а също поради все по-ясната необходимост от реални резултати от предприеманите действия с отчитане на темповете и проявите на промени в климата, особено на неблагоприятните такива. Оценките за резултатите от COP-15 са противоречиви, като дори и положителните са твърде общи, за да може да се каже, че е била успешна. Подписаният в Копенхаген документ („Copenhagen Accord“) на практика не е законов акт и всъщност представлява договореност между САЩ и големите развиващи се страни. Европейският съюз като цяло не успя да осъществи роля на катализатор за постигане на договореност за по-амбициозни цели след 2012 г.
2010 г.	На 16-та Конференция на страните по РКОНИК (COP16), която се проведе в Мексико. Страните постигнаха политическо споразумение по въпроса за ограничаване на глобалното повишаване на температурата до под 2 градуса по Целзий (при необходимост дори 1,5 градуса) спрямо температурните равнища преди началото на индустриализацията. Не се привеждат обаче научни доказателства, че това политическо споразумение ще доведе до постигането на целта.
2011 г.	На 17-та Конференция на страните по РКОНИК в Дърбан, Южна Африка, с цел да се предотврати „празен период“ преди влизане в сила на ново глобално правнообвързващо споразумение на страните по Протокола от Киото (първият период на който изтече в края на 2012 г.) държавите членки на Европейския съюз се споразумяха да продължат периода на задълженията си по него за още пет или осем години (от 1 януари 2013 г. до края на 2017 г., или до края на 2020 г. в зависимост от напредъка по новото споразумение).
2014 г.	100 световни лидери се събират при срещата на високо равнище на ООН относно климата в Ню Йорк; Петият доклад на МКИК за оценка на изменението на климата сочи, че целта за ограничаване на температурното повишение в рамките на 2 °C все още е достижима; ЕС договаря своя пакет в областта на климата и енергетиката за 2030 г., включително цел за намаляване на емисиите на парниковите газове на ЕС с поне 40 %.
2015 г.	През декември 2015 г. в Париж, Франция се проведе 21-вата Конференция на страните (COP 21). Както беше обещано, се прие новото световно споразумение относно климата и най-сетне бяха изготвени необходимите амбициозни, справедливи и обвързващи решения за всички 196 страни под формата на „световно споразумение“ (global deal). То би трябвало да влезе в сила през 2020 г. се прие новото световно споразумение относно климата.

Някои държави, включително ЕС, договориха правно обвързващи цели за ограничаване на своите емисии в периода до 2020 г. по едно споразумение, наречено

Протокол от Киото. Общо над 90 страни от цял свят също се ангажираха да предприемат доброволни действия до 2020 г. Тези ангажименти обаче няма да бъдат достатъчни за предотвратяване на опасните промени в климата. Благодарение на натиск от страна на ЕС и други държави започнаха преговори на ООН за постигане на едно ново правно обвързващо споразумение в областта на климата, което ще изисква действия от всички държави за намаляване на емисиите на парниковите газове. Гражданите и предприятията също имат определена роля.

Споразумението от Париж от 2015 г. е исторически значимо събитие в глобалната борба с изменението на климата. Споразумението е жизненоважно – последна възможност да предадем на бъдещите поколения по-стабилен свят, по-чиста планета, по-справедливи общества и по-проспериращи икономики, разгледано също така в контекста на Програмата за устойчиво развитие до 2030 г. То ще поведе световния преход към глобална чиста енергия. Този преход ще изисква промени в начина на вършене на бизнес и на инвестиране, както и стимули в целия спектър на политиките. За ЕС това открива добри възможности, най-вече за създаване на работни места и растеж. Преходът ще стимулира инвестициите и иновациите в областта на енергията от възобновяеми източници, като по този начин ще допринесе за реализирането на амбицията на ЕС да се превърне в световен лидер в тази област, и ще увеличи растежа на пазарите за стоки и услуги, произведени в ЕС, например в областта на енергийната ефективност⁴.

Изпълнението на ангажиментите по Споразумението от Париж („Глобално споразумение“) изисква поддържане на динамиката и силен политически ангажимент, за да се гарантира преходът към устойчиво и неутрално по отношение на климатичните изменения бъдеще, извършен по социално справедлив начин. Изменението на климата трябва да остане в политическия дневен ред на съответните международни форуми, включително на срещите на Г-20 и Г-7. Във връзка с това ЕС ще продължи да играе водеща роля на международната сцена и да развива дипломацията в областта на климата.

В Споразумението от Париж е изложен *глобален план за действие*, който да насочи света към предотвратяването на опасно изменение на климата, като се отчита, че това ще изисква възможно най-скоро да бъде постигнат пикът на световните емисии на парникови газове, а през втората половина на настоящия век – неутралност по отношение на климата. Споразумението има следните основни характеристики:

- с него се определя дългосрочна цел за насочване на света към ограничаване на глобалното затопляне до значително под 2°C в сравнение с нивата от предииндустриалния период, както и за продължаване на усилията за ограничаване на повишението на температурата до 1,5°C. Пожелателната цел от 1,5°C беше договорена, за да бъдат предизвикани по-амбициозни действия и за да се акцентира върху опасенията на най-уязвимите държави, които вече изпитват последиците от изменението на климата;

4 Съобщение на Комисията до Европейския парламент и Съвета, Пътят след Париж: оценка на въздействието на Споразумението от Париж, придружаваща предложението за решение на Съвета относно подписването от името на Европейския съюз на Споразумението от Париж, прието съгласно Рамковата конвенция на ООН по изменение на климата Брюксел, 2.3.2016 г. COM (2016) 110 final, стр. 2.

- тя изпраща ясен сигнал до всички заинтересовани страни, инвеститори, предприятия, до гражданското общество и политиците, че глобалният преход към чиста енергия е неотменим и че трябва да се премине към различни от ископаемите горива ресурси; Понастоящем с изготвянето на 189 национални плана в областта на климата, обхващащи около 98 % от всички емисии, справянето с изменението на климата се превърна в истинско глобално усилие. Със Споразумението от Париж се преминава към всеобщи действия, а не само от малцина;

- то предоставя динамичен механизъм за преглед и засилване на амбициозните действия с течение на времето. Считано от 2023 г. нататък, страните по Споразумението ще се срещат на всеки пет години в рамките на „общ преглед“, за да разгледат напредъка в областта на намаляването на емисиите и адаптирането, както и предоставената и получена подкрепа с оглед на дългосрочните цели на Споразумението;

- страните имат правно обвързващо задължение да изпълняват вътрешни мерки за смекчаване с цел постигането на целите, предвидени в техния принос;

- със Споразумението се постига по-голяма прозрачност и отчетност, включително чрез: представяне на всеки две години от всички страни на инвентаризации на парниковите газове и информация, необходима за проследяване на техния напредък; експертно техническо проучване; многостранен преглед в помощ на напредъка на страните; както и механизъм за улесняване и насърчаване на спазването на изискванията;

- с него се предоставя амбициозен пакет за солидарност с подходящи разпоредби относно финансирането на борбата с изменението на климата и посрещане на нуждите по отношение на адаптацията, както и загубите и щетите, дължащи се на неблагоприятните последици от изменението на климата. С цел насърчаване на индивидуалните и колективните действия за адаптация със Споразумението от Париж за пръв път се установява глобална цел за увеличаването на капацитета и устойчивостта спрямо изменението на климата, а също и за намаляване на уязвимостта в това отношение. В международен план с него се насърчава по-доброто сътрудничество между страните с цел споделяне на научни знания относно адаптирането, както и на сведения относно практики и политики.

При подготовката и по време на Конференцията в Париж ЕС бе в центъра на коалицията на високите амбиции, съставена от развити и развиващи се държави. За да осигури ефективен преход към икономика с ниски въглеродни емисии, ЕС трябва да поддържа тази амбиция във вътрешен и международен план:

- споразумението от Париж следва да бъде подписано и ратифицирано възможно най-бързо. Предложението за подписване на Споразумението е приложено към настоящото съобщение;

- ЕС трябва да консолидира благоприятните условия за прехода към икономика с ниски въглеродни емисии чрез широк кръг от взаимодействащи си политики, стратегически рамки и инструменти, отразени в 10-те приоритета на Комисията „Юнкер“ — по-специално устойчивият енергиен съюз с ориентирана към бъдещето политика по въпросите на изменението на климата;

- регулаторната рамка в областта на енергетиката и изменението на климата за 2030 г. трябва да бъде завършена бързо в съответствие със заключенията на Европейския съвет от октомври 2014 г. Европейският парламент и Съветът трябва да се

разгледат предстоящите законодателни предложения във възможно най-кратки срокове;

- всички страни трябва да са готови да участват пълноценно в процесите на преразглеждане съгласно Споразумението от Париж, предназначени да гарантират постигането на целта за ограничаване на изменението на климата под 2 °C и продължаването на усилията за ограничаване до 1,5 °C.

Изводи:

1) Изменението на климата вече е факт и е едно от най-големите глобални предизвикателства на нашето време, което налага да се предприемат незабавни действия и сътрудничество между (местни, регионални и национални) власти и международни организации от всички краища на света.

2) Безспорно проблемът за климатичните промени е проблем на международното екологично право и то като нормативен регулатор трябва да постави рамките, в които този проблем да бъде разрешен. В противен случай човечеството рискува да постави под въпрос не само своето оцеляване, но и съществуването си въобще. Международното право е средството, което ще даде отговорът на въпроса „как да се справим с климатичните промени?“.

3) Държавите по света трябва да намерят баланса – между националното и международното, между личното и общото, между икономическия интерес и правото. Вече не е въпрос на желание от страна на държавите да се разработи ново правно решение. Усилията трябва да бъдат насочени към каузата да се опази Земята като най-голямото богатство на бъдещите поколения – кауза, която е „обща грижа на човечеството“.

4) Местните и регионалните власти са основни двигатели на енергийния преход и борбата срещу изменението на климата, тъй като именно те стоят най-близо до гражданите и независимо от социално-икономическата си ситуация и географско местоположение, стоят на фронтната линия в борбата за намаляване на уязвимостта на своите територии от различните въздействия на изменението на климата. Въпреки че усилията за намаляване на въглеродните емисии вече са в ход, адаптацията остава необходимо и задължително условие за смекчаване на последиците от климатичните промени.

5) През последните години ЕС придоби добра репутация в световен мащаб в областта на смекчаването на изменението на климата. В световен мащаб ЕС следва да продължи да бъде благонадежден партньор и да дава положителен пример. Той може да изпълнява убедително тази роля на пионер само когато политиката в областта на изменението на климата и положителното икономическо развитие доказано вървят ръка за ръка. Следователно ЕС има с какво да служи за пример в глобален мащаб. Той показва, наред с останалото, че икономическият растеж може да бъде отделен от увеличаването на емисиите. Така например никое друго икономическо пространство в света не емитира по-малко парникови газове на единица БВП, отколкото ЕС. Много европейски предприятия са лидери по отношение на енергийната и ресурсната ефективност. Това е свързано до голяма степен с техническите достижения и следователно с иновационния потенциал на европейските предприятия, които са резултат от сравнително строгото законодателство на ЕС в областта на околната среда.

6) Въпреки показания напредък на Европа, предстои да се решават още много задачи: поставените цели за намаляване на емисиите на CO₂ с 80-95 % до 2050 г. няма да могат да бъдат постигнати единствено с технически иновации. Това става ясно например в транспортния сектор, където иновациите в технологиите за работни газове бяха най-малкото частично неутрализирани от увеличаването на превозните средства и пътната инфраструктура. Ето защо ще бъдат необходими също и структурни промени, т.е. съществува необходимост от много по-голямо съгласуване отколкото досега между политиката в областта на климата и останалите политики.

7) Първото многостранно споразумение относно изменението на климата е споразумението от Париж („Глобално споразумение“), което обхваща почти всички емисии в световен мащаб. То е успех за света и потвърждение на избора на ЕС да върви по пътя на икономика с ниски въглеродни емисии. От решаващо значение за сключване на това споразумение беше преговорната стратегия на ЕС и той воден от опита си, свързан с провеждането на ефективна политика по отношение на климата, настояваше за постигането на амбициозни резултати.

Литература:

1. „Действия на ЕС срещу изменението на климата: водещата роля на ЕС в световен мащаб до 2020 г. и след това“ (брошура): ec.europa.eu/environment/climat/pdf/eu_action_against_climate_change.pdf

2. Европейска комисия, Борба срещу изменението на климата, Водещата роля на ЕС, поредица „Европа в движение“, 2008.

3. Съобщение на Комисията до Европейския парламент и Съвета, Пътят след Париж: оценка на въздействието на Споразумението от Париж, придружаваща предложението за решение на Съвета относно подписването от името на Европейския съюз на Споразумението от Париж, прието съгласно Рамковата конвенция на ООН по изменение на климата Брюксел, 2.3.2016 г. COM (2016) 110 final

4. Становище на Европейския икономически и социален комитет относно „Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите - Стратегия на ЕС за адаптация към изменението на климата“, COM (2013) 216 final

5. Иво Емануилов, Климатичните промени като проблем на международното екологично право. Перспективите за международноправно споразумение след Копенхагенската конференция на ООН през 2009 г.

6. Рамкова конвенция на Обединените нации по изменение на климата, ратифицирана със закон, приет от 37-то НС на Р. България на 16.03.1995 г. - ДВ, бр. 28 от 28.03.1995 г.

7. Работен документ на службите на комисията придружаващ Бялата книга „Адаптация спрямо изменението на климата: към европейска рамка за действие“, Брюксел, 1.4.2009 SEC(2009) 388

8. Веселин Александров и колектив, Климатични промени (второ издание), НИМХ-БАН, октомври, 2010 г., <http://meteorology.meteo.bg/brobura.pdf>

9. Политиките на Европейския съюз: Действия в областта на климата, Европейски съюз, ноември 2014 г.

10. Съвременни климатични проблеми, <http://meteotv.bg>.

11. Веселин Александров и колектив, Климатични промени (второ издание), НИМХ-БАН, октомври, 2010 г., <http://meteorology.meteo.bg /bro6ura.pdf>

СЪВРЕМЕННИ ЗАПЛАХИ ЗА НАЦИОНАЛНАТА СИГУРНОСТ ОТ ВОЕНЕН ХАРАКТЕР

Калоян А. Илиев, Велико П. Петров

“Vasil Levski” National Military University, “Artillery, Air-defence and Communication and Information Systems” Faculty, “Organization and management of the Field Artillery tactical formations” Department; town of Shumen.

MODERN THREATS TO NATIONAL SECURITY OF A MILITARY NATURE

Kaloyan A. Iliev, Veliko P. Petrov

ABSTRACT: The national security of the Republic of Bulgaria is assessed on the basis of the Constitution of the Republic of Bulgaria and the National Security Strategy. The current security environment is characterized by dynamic, diverse challenges and changes difficult to predict, including asymmetric risks and threats. Today the Republic of Bulgaria finds itself in one of the areas with the greatest concentration of risks and threats in the Euro-Atlantic community. Trends for their development are negative in the medium and in many cases and in the long term. Source of significant risks to the national security of the Republic of Bulgaria remains instability in regions located near the borders of our country. This assessment aims to support policy making in the field of national security and present the main directions of work in this area to achieve security and stability at national, regional and global level.

KEY WORDS: National security risk, threat, armed forces, asymmetric risks and threats, security environment.

В синтезиран вид същността на термина “защита на националната сигурност” може да се определи като комплекс от дейности за придобиване на информация за реални и потенциални заплахи за сигурността на страната и организиране на противодействие за тяхното неутрализиране. Нейната основна цел е постигане на стратегическо превъзходство над източниците на заплахите чрез тяхната постоянна оценка и прилагане на адекватни мерки.

Предизвикателствата, рисковете и заплахите в областта на сигурността налагат извода, че развитието на глобалната и регионалната среда за сигурност за дълго време ще запази динамичния си и противоречив характер с възможности за усложняване. В тези условия страната отстоява своите интереси, като най-голямо влияние върху сигурността й оказва широкият спектър от нови рискове и предизвикателства.

Процесите на глобализация влияят нееднозначно върху формирането на различните аспекти на средата на сигурност. Те създават условия за развитие на връзките между държавите, но и задълбочават икономическото и социалното неравенство и дисбалансът в развитието на страните и демографските диспропорции. Кризисните финансови и икономически явления в света се отразяват негативно не само върху вътрешната стабилност на държавите и международните отношения, но и върху сектора на сигурност и отбрана. 2/13

Страните със слаба държавност оказват съществено влияние върху формирането на стратегическата среда на сигурност. Същевременно нараства ролята на различни недържавни структури (икономически и финансови групировки, неправителствени организации, племенни обединения, радикални религиозни общности, трансгранични криминални мрежи, екстремистки групи и др.), които се опитват да влияят върху световния ред, обстановката и облика на военните действия в кризисните региони.

Военните аспекти на средата на сигурност придобиха нови измерения вследствие на политическите промени в света и в Европа, разширяването на спектъра на асиметричните рискове и заплахи и намаляването на значението на някои фактори, които в миналото влияеха върху мисиите и подготовката на въоръжените сили. Заплахата от възникване на мащабен международен военен конфликт е значително редуцирана, поради липсата на междублоково противопоставяне и наложилата се необходимост от взаимодействие между държавите за неутрализиране на съвременните рискове и заплахи. Продължават обаче да съществуват регионални огнища на напрежение и нестабилност, в които са ангажирани и военни ресурси.

Приоритетно значение за гарантирането на националната сигурност има членството на страната ни в НАТО и в ЕС, както и активното и участие в международното сътрудничество. Заедно с това България се старее да развива своята икономика и гражданското общество, като важни условия за гарантиране на сигурността и защитата на националните интереси⁵.

Основните проблеми в средата за сигурност са породени не от риска от мащабни военни конфликти между държави в света и в региона, а главно поради широкия спектър от асиметрични рискове и заплахи.

Тероризмът и организираната престъпност заедно със социалните конфликти, бедността, миграционните проблеми, разпространението на оръжия за масово унищожаване, наркотиците и трафикът на хора, природните бедствия, техногенните катастрофи, инфекциозните болести и през следващите години се очертават като основни заплахи за международната сигурност и сигурността на България^{6, 7}.

Борбата с тероризма е продължителна и предполага решително използване на военни, полицейски, политически, финансови и информационни мерки и ресурси, както и наличие на специална антитерористична система. За неутрализиране на съществуващите и нововъзникващи заплахи и рискове се засилва тенденцията за сътрудничество между държавите и нарастване ролята на ООН, ЕС и НАТО. Необходимо е да се ангажира целият арсенал на международната общност от диплома-

⁵ Доктрина на Въоръжените сили на Република България, С., 2011 г.

² Стратегия за национална сигурност на Република България, С., 2011 г.

³ Национална отбранителна стратегия, МО на РБ, София, 2016

⁴ Бяла книга за отбраната, МО на РБ, София, 2010

тически, икономически, правозащитни и военни мерки, както и мобилизация на всички национални ресурси.

НАТО играе основна роля в гарантирането на сигурността на страните от евроатлантическата общност. Алиансът осигурява степен на защита на националната сигурност, която надхвърля възможностите на която и да е от индивидуалните му страни-членки.

Засилва се ролята на НАТО като форум за политически консултации по въпросите на сигурността за евроатлантическата общност, включително и по въпросите, които излизат извън географската рамка на Алианса и извън военните аспекти. Уникалните възможности на НАТО, в съчетание с тези на ЕС, могат да бъдат в основата на решенията на множество значителни международни проблеми. В тази връзка може да се очаква срещите на най-високо равнище на НАТО да доведат до разширяване ролята на Алианса като форум за консултации по въпросите на сигурността, както и до по-широко сътрудничество с ЕС и нов тласък на процеса на трансформация на НАТО.

Глобализация, както и засилващата се политическа роля на НАТО и все по-широкият спектър на неговите операции увеличават и заинтересоваността на страни от различни региони на света да развият специални отношения с Алианса, тъй като го разглеждат като важна и ефективна организация, действаща в сферата на сигурността. Същевременно, НАТО, чрез своите съществуващи партньорства, е един от основните фактори за стабилността и интеграцията в международната общност на редица страни от Източна Европа, Централна Азия и Средиземноморието. В тази връзка се очаква, че вече съществуващите партньорства на НАТО ще получат нов тласък и е вероятно да бъдат положени основите на нови такива, далеч надхвърлящи географски съседните региони на Алианса, особено в отношенията със страни, споделящи основните ценности, които споделят и страните-членки на НАТО.

Европейският съюз продължава активно и последователно да формира общата външна политика и политиката за сигурност, както и да прилага Европейската стратегия за сигурност. Република България участва в европейската политика за сигурност и отбрана (ЕПСО), като ще допринася за засилване на военните и невоенните способности на ЕС.

Република България се ангажира с поемането на по-широки отговорности от ЕС за военно и невоенно регулиране на кризи. Това се осъществява в тясно сътрудничество с НАТО без излишно дублиране на усилия и ресурси.

Независимо от трудностите и произтичащите в отделните страни сложни и противоречиви процеси, в Югоизточна Европа (ЮИЕ) се очертава трайна тенденция за стабилизиране на обстановката. Реализирането на регионалните инициативи (Процеса за сътрудничество в ЮИЕ, Пакта за стабилност в ЮИЕ, инициативите в Черноморската зона и др.) продължава да съдейства за разрешаване на проблемите на региона, включително в областта на сигурността.

Налице е тенденцията за:

- Утвърждаване ролята на България като източник на сигурност и стабилност в региона;
- Подпомагане процесите на интеграция в страните от ЮИЕ, ЕС и НАТО;

➤ Преодоляване на негативните представи за региона като зона на кризи и конфликти чрез укрепване на доверието, стабилността и сигурността и прилагане на европейски стандарти в международните отношения.

Като цяло обстановката в Западните Балкани запазва своя динамичен характер с възможности за усложнения и кризисни ситуации, а за трайното ѝ стабилизиране се изисква време и ангажиране на международната общност в политически, икономически и военен план.

Неразрешените конфликти в Черноморския регион продължат да са основен проблем не само за сигурността, но и за политическото, икономическото и социалното развитие на страните от региона, включително на Република България. В краткосрочен и средносрочен план сигурността в страната ще се намира под влияние и на процесите, протичащи в Централна Азия, Близкия изток и Северна Африка. Основните рискове произтичат от високото ниво на политическо, социално, икономическо и религиозно напрежение, вътрешните и международните конфликти, производството и разпространението на наркотици и свързаната с тях организирана престъпност, а не на последно място и бежанският поток.

Приоритетните задачи за нашата страна в областта на регионалното сътрудничество са:

➤ Поддържане на активната политика за укрепване на доверието, стабилността и сигурността и утвърждаване на европейски стандарти в отношенията между държавите от региона, съчетана с оказване на конкретно съдействие на страните за подпомагане и отстояване на тяхната европейска и евроатлантическа перспектива;

➤ Повишаване значението на България като важен външнополитически фактор и източник на стабилност, като страна-членка на НАТО, член на ЕС и държава-участничка в глобалните международни организации и режими;

➤ Въздействие върху променящата се рамка на регионално сътрудничество в съответствие с приоритетите на страната;

➤ Разширяване на диапазона от конкретни съвместни дейности с траен обвързващ характер в региона;

➤ Инициране на конкретни действия по реализация на транспортните, енергийните и телекомуникационните инфраструктурни проекти, касаещи България;

➤ Развитие на икономическото, социалното и културното сътрудничество^{8,9}.

Във външен план за националната сигурност на България продължават да оказват влияние:

➤ Глобализацията остава водеща тенденция, която ще продължи да влияе върху цялостното развитие на външната среда за сигурност. Освен нея основни фактори на промяната ще бъдат евентуалното изместване на центъра на икономически растеж от Запад на Изток, засилващото се въздействие на недържавни структури, в т.ч. икономически и религиозни, а също и процеси в сферата на енергетиката, миграцията, проблемите на бедността и развитието, промяната на климата.

➤ Членството на Република България в НАТО и ЕС и обстоятелството, че нито една от съседните държави не я разглежда като потенциален противник, са определящи фактори за външната ѝ сигурност и ще възпрепятстват появата на пряка военна заплаха за суверенитета и териториалната ѝ цялост в дългосрочна перспектива.

⁸ Стратегия за национална сигурност на Република България, С., 2011 г.

⁹ Бяла книга за отбраната, МО на РБ, София, 2010

➤ Развитието на интеграционните процеси в ЕС и трансатлантическото сътрудничество имат важно значение за уреждане на основните международни въпроси. С инициативите и действията си ЕС и НАТО все повече се утвърждават като определящи фактори в укрепването на международната сигурност.

➤ Асиметричните заплахи (особено международният тероризъм и разпространението на оръжия за масово унищожение (ОМУ), регионалните конфликти, киберпрестъпността и трансграничната организирана престъпност оказват съществено влияние върху средата за сигурност в глобален и регионален мащаб.

➤ Тероризмът е сериозна заплаха за глобалната сигурност. Регионалните конфликти, икономическите и финансовите кризи изострят допълнително тази заплаха. Терористичните организации децентрализират структурите си, разнообразяват начините на действие и умело се инфилтрират в демократичното общество, което затруднява тяхното неутрализиране. Възможностите за използване на радиоактивни материали, токсични вещества и биологични агенти, както и за достъп до информационни бази от данни и технологии за терористични цели се увеличават.

➤ Рисковете от разпространяване на ОМУ нарастват вследствие на засиления интерес към придобиването им от различни държави. Запазват се рисковете, свързани със съхраняването на съществуващото ядрено оръжие и радиоактивни материали в отделни страни.

➤ Трансграничната организирана престъпност е една от главните заплахи за сигурността на гражданите и демократичните основи на обществото. Тя включва дейности, свързани с икономически престъпления, производство и трафик на наркотици, трафик и експлоатация на хора, контрабанда, производство и разпространение на неистински парични знаци и документи, киберпрестъпления, пране на пари и други. Организираната престъпност създава предпоставки и се възползва от корупцията.

➤ Киберпрестъпността е глобална и анонимна заплаха за информационните системи. Деструктивните въздействия върху информационните системи и мрежи могат да доведат до криза чрез затрудняване и/или блокиране нормалното функциониране на важни за икономиката, финансовата система и държавното управление системи или отделни компоненти.

➤ Сериозен проблем за международната сигурност са страните със слаба държавност, които не са способни да гарантират сигурността, правата и свободите на своите граждани, да управляват обществените отношения и да изпълняват международните си задължения.

➤ Ново тревожно явление е пиратството и отвличането на екипажи на търговския флот предимно в морските води край бреговете на Африка и Югоизточна Азия. Липсата на ефективно противодействие на този странен за 21-ви век феномен го прави източник на сериозни заплахи за световната търговия и транспортни комуникации, както и за сигурността на екипажите и пътниците.

➤ Нестабилната икономическа и политическа обстановка и ниският стандарт на живот в държави и региони от "третия свят" генерират миграционен натиск върху страната като външна граница на ЕС.

➤ Рискове за екологичната сигурност произтичат от промишлени аварии с изпускане на вредни емисии, трансгранично замърсяване на въздуха, водите и крайбрежната ивица, както и от заплахата за терористична дейност с използване на вещества, които са особено опасни за природната среда. Защитата на корпоративни

икономически интереси забавя предприемането на реални стъпки за разрешаване на тези проблеми в широк международен контекст.

➤ Реализирането на стратегически международни транспортни и енергийни проекти повишава степента на определеност на средата за сигурност. Това не гарантира еднозначно повишаване състоянието на сигурност и изисква изграждане на способности за защита на критичната инфраструктура.

➤ Глобализирането на транспортните връзки способства за бързото разпространяване на инфекциозни заболявания и епидемии в световен мащаб, излага на риск държавите и техните граждани, включително формированията на въоръжените им сили, участващи в международни мисии и операции в сложни природни условия.

➤ Енергийната сигурност е елемент на националната сигурност и предпоставка за икономическа стабилност. Задълбочава се зависимостта на държавите от жизненоважни ресурси - енергийни, водни, суровинни и хранителни, което повишава риска от възникване на кризи. Проблемите в тази област се превръщат в един от най-сериозните рискове за всички страни независимо от степента на икономическото им развитие и ресурсната им осигуреност.

➤ В Югоизточна Европа водеща е тенденцията към по-нататъшно стабилизиране и пълноценно включване в евроатлантическото и европейското пространство. За това допринасят намаляването на военните способности на държавите, разширяването на двустранното и регионалното сътрудничество, на регионалния пазар и съвместните проекти в различни области. В основата на засилването на тенденциите на сътрудничество и добросъседство са членството на държави от региона в НАТО и ЕС и процесът на постепенно интегриране на държавите от Западните Балкани в европейските и евроатлантическите структури. Силен стабилизиращ ефект за целия регион има присъединяването на България и Румъния към НАТО и ЕС.

➤ В Западните Балкани преобладават положителните тенденции благодарение на активното ангажиране на международната общност с разрешаването на традиционни и нововъзникващи проблеми. Важна стъпка по пътя на трайното стабилизиране на региона е присъединяването на Албания и Хърватия към НАТО през 2009 г. и запазването на перспективата за последващо присъединяване и на други държави от региона. Същевременно се запазват някои сериозни рискове пред демократичното и устойчивото развитие на държавите в региона. Продължават опитите за възпроизвеждане на стереотипи от миналото, породени от специфичната регионална среда и създаващи рискове за сигурността.

➤ Република България разглежда Черноморския регион в широк европейски и евроатлантически контекст с цел развитие на сътрудничеството между страните в сферата на икономиката, търговията и сигурността. Особено голямо значение този регион придобива в контекста на развитието на мрежата на пренос на основни енергоносители, свързващи държавите производителки с енергийните пазари в Европа. Значението на региона нараства предвид активната роля на страната ни за поддържане на международния мир, както и ангажиментите по охраната на външните граници на НАТО и ЕС.

➤ Тенденциите в Близкия и Средния изток чертаят несигурно бъдеще на региона и началото на период на продължителна трансформация. Ситуацията и перспективите в региона поставят пред сериозни предизвикателства страните от Евро-

пейския съюз и НАТО. Възможни са промени, които могат да доведат до демократично управление и балансирано икономическо и социално развитие. Същевременно съществуват очевидни рискове от увеличен миграционен натиск, засилване на влиянието на радикални движения и активиране на международни терористични мрежи в непосредствена близост до Европа. Стремещът на някои държави да развиват ядрени и/или ракетни програми създава допълнителни рискове от усложняване на обстановката. Неутрализирането на рисковете и едновременно с това поддръжката на положителните тенденции в държавите от региона следва да бъде ядро на новата евроатлантическа стратегия, в изготвянето на която България ще участва активно и конструктивно, като отчита специфичните си национални интереси.

➤ НАТО и ЕС имат съществени отговорности за осигуряването на устойчива и дълготрайна стабилност в Афганистан; тази задача изисква едновременното решаване на комплекс от разнородни проблеми - политическо и икономическо стабилизиране на региона, борба с тероризма и радикалния ислям, противодействие на производството и на трафика на наркотици и на хора¹⁰.

Във вътрешен план за националната сигурност на България продължават да оказват влияние:

- Рисковата миграция през територията на страната;
- Незаконният трафик на хора, наркотици и оръжие;
- Търговията с общоопасни средства и стоки с възможна двойна употреба;
- Дейността на организирани престъпни групи;
- Корупцията и др.^{11, 12}.

Въпреки че корупционната практика остава реално „рисково“ явление, с усъвършенстването на нормативната база, подобряването на дейността на правоохранителните органи и взаимодействието между държавните институции се повишават възможностите за нейното пресичане.

Не може да се изключи и възможността от евентуални терористични заплахи срещу страната ни, поради участието на български войскови подразделения в многонационални контингенти на НАТО, Европейския съюз и под егидата на ООН.

През следващите години се очертава излизане от икономическата криза и тенденцията за развитие на макроикономическа среда с функциониращи пазарни механизми, което е предпоставка за подобряване на националната икономика. Едновременно с това глобалната икономическа среда и в бъдеще ще продължи пряко да влияе върху развитието на българската икономика.

България има интерес да продължи да развива военнопромишленото си сътрудничество и коопериране на двустранна и многостранна основа в рамките на НАТО и ЕС, включително чрез участието си в процеса на формирането на единен Европейски пазар на отбранителни продукти и материали.

В сферата на отбранителната политика е необходимо да продължи реорганизацията на командната структура на Въоръжените сили; подготовката на декларираните сили и средства за участие в операции в „отговор на кризи“; изпълнението на приетите цели на въоръжените сили; реализиране на проектите за модернизация.

⁷ Стратегия за национална сигурност на Република България, С., 2011 г.

¹¹ Национална отбранителна стратегия, МО на РБ, София, 2016

¹² Доктрина на Въоръжените сили на Република България, С., 2011 г.

Необходимо е да се работи за осигуряване на благоприятна социална среда. Българската държава трябва да разширява защитата на правата и интересите на българските граждани, включително на тези в чужбина.

Социално-икономическата сигурност на населението в страната трябва да се гарантира чрез последователно провеждане на политика за осигуряване на максимална заетост, поддържане на по-висок жизнен стандарт, работещо здравеопазване, конкурентна образователна система и ефективна система за социално осигуряване.

Във вътрешнодържавен план средата за сигурност трябва да се формира чрез:

- Извеждане на стратегическите цели на политиката за сигурност на Република България като основен фактор за защита на националните интереси.

- Сътрудничество и координация между структурите за сигурност на Република България с тези на страните от НАТО, Европейския съюз и съседните държави.

- Изграждане на политическата стабилност с демократични институции, спазване върховенството на закона, ефикасна защита на правата на човека и ефективна пазарна икономика.

- Икономически просперитет, ефективна социална политика, усъвършенстване на националната образователна система, научни изследвания в областта на сигурността.

- Формиране поддържането на национален консенсус по приоритетни въпроси, гарантиращи сигурността и националните интереси на държавата¹³.

Националните интереси имат основна, целеполагаща роля в политиката по сигурността и по-специално в областта на отбраната.

Националните интереси са потребностите и желанията на нацията в контекста на международната обстановка. Националните интереси на държавата и нацията определят нейното участие като суверен на световната сцена. Те са основа за определянето на националните цели и формирането на политиката, включително в областта на сигурността.

От гледна точка на националната сигурност националните интересите се класифицират по категории в зависимост от техния характер и по приоритети. Важността на интересите е средство за определяне на приоритетите. Без определянето на приоритетите на интересите съществува опасност от възникване на несъответствие между целите и ресурсите.

Ролята на въоръжените сили е да допринася за осъществяване на националните интереси, гарантиране на териториалната цялост, независимостта и сигурността на страната, заедно с войските на съюзниците да възпират и да побеждават вероятни противници, да допринасят за задържане на заплахите далеч от границите на страната за запазване на международния мир и сигурност.

Външната среда за сигурност, която ще оказва влияние върху състоянието на националната ни сигурност, ще се характеризира с асиметрична многофакторност, висока динамика, неопределеност, нееднозначни и сложни за прогнозиране процеси.

Тенденциите в средата за сигурност показват, че в бъдеще може да възникнат нови конфликтни и кризисни ситуации в различни части на света, което ще налага рисковете и заплахите за националната сигурност и интересите на Република Бъл-

гария да бъдат посрещани извън територията на страната като част от съюзните усилия в рамките на НАТО и ЕС.

Нито една държава няма да може да се справи самостоятелно с рисковете и заплахите. Това налага търсенето на многостранни подходи при уреждане на важни проблеми на развитието и сигурността и засилва взаимозависимостта между политиките, предприемани на национално и международно равнище.

ООН, НАТО, ЕС, ОССЕ и други международни организации имат важна роля в областта на превантивната дипломация, управлението при кризи, следконфликтното стабилизиране, укрепването на демокрацията, спазването на правата на човека и върховенството на закона. Международните финансови, икономически и търговски организации разширяват своето влияние, което се отразява и върху средата за сигурност.

В условията на нарастващо влияние на външните фактори вътрешните фактори ще продължават да запазват своето решаващо значение за състоянието на националната сигурност.

Изводи:

➤ Съществените и динамични промени в стратегическата среда на сигурност изискват адаптиране и трансформиране на системите за сигурност и отбрана към реалната глобална и регионална обстановка.

➤ Членството на Република България в НАТО и ЕС и конструктивното участие в многостранни формати на регионално сътрудничество и развитие на добросъседски двустранни отношения на базата на реализация и защита на националните ни интереси са определящи за националната сигурност и отбраната на страната. Те възпрепятстват появата на пряка военна заплаха за суверенитета и териториалната цялост на Република България в средносрочна перспектива. Разрастването на мащабите на регионалните конфликти, стремежът за налагане на политически и икономически интереси от държавни и недържавни фактори, както и природните бедствия могат да изправят страната ни пред сериозни предизвикателства, като засилен бежански натиск, прояви на насилствен радикализъм и тероризъм, кибератаки, активизиране на каналите на международни криминални групировки, финансово-икономически престъпления, енергийни и екологични проблеми.

➤ Тенденциите в стратегическата среда на сигурност показват, че и в бъдеще е възможно да възникват конфликти и кризисни ситуации, което налага рисковете и заплахите за националната сигурност и отбраната на Република България да бъдат неутрализирани, включително извън територията на страната. Това поставя изисквания към въоръжените сили за приоритетно изграждане и развитие на способности за участие в мисии и операции на НАТО, ЕС, ООН, ОССЕ и други международни организации, както и за тяхното хармонизиране с гражданските и обществените усилия и нагласи.

➤ Ангажиментите на Република България за гарантиране на международната сигурност поставят военните ни формирования, участващи в мисии и операции извън територията на страната, под потенциалната заплаха от терористични атаки и въоръжени нападения, както и от други недобронамерени действия на противостоящите сили.

➤ В политико-военната област дълготрайният ефект от украинската криза и влошаването на отношенията на Русия с НАТО съдържат потенциал за развитие на

тенденцията на завръщане към „политика от позиция на силата“ в Европа.

➤ Динамичната и сложна геостратегическа среда повишава отговорностите на всички видове разузнаване за ранно предупреждение за рисковете и заплахите за сигурността и отбраната на страната, за своевременно информационно осигуряване на държавното и военното ръководство, за разузнавателна поддръжка на военните формирования от въоръжените сили на Република България и за изпълнение на ангажиментите към НАТО и ЕС.

➤ Военностратегическата среда продължава да се развива и влияе от непредвидимите и динамични политически, икономически, социални, научно-технологични и военни процеси. Възможните бъдещи кризи и конфликти се очаква да бъдат сложни и трудни за прогнозиране и управление. Това изисква гъвкаво и адекватно развитие на политиката, организацията и планирането на отбраната, на доктриналните документи, концепциите и планове за операции и преди всичко на отбранителните способности, на бъдещата структура и системата за ръководство, командване и управление на въоръжените сили.

➤ Съчетанието между демографската криза, ниската мотивация за образование, професионална подготовка и реализация на определени слоеве от населението и забавения икономически растеж е предизвикателство пред сигурността и отбраната на страната.

Литература:

1. Стратегия за национална сигурност на Република България, С., 2011 г.
2. Бяла книга за отбраната, МО на РБ, София, 2010 г.
3. Национална отбранителна стратегия, МО на РБ, София, 2016 г.
4. Доктрина на Въоръжените сили на Република България, С., 2011 г.
5. Визия: България в НАТО и Европейската отбрана 2020, София 2014 г.
6. Европейска стратегия за сигурност „Сигурна Европа в един по-добър свят” - [http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIBG .pdf](http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIBG.pdf)
7. Национална програма „България в НАТО и в Европейската отбрана - 2020”, октомври 2014 година.
8. Закон за отбрана и въоръжените сили на Република България.

МЕЖДУНАРОДНОТО ХУМАНИТАРНО ПРАВО – ФАКТОР В СЪВРЕМЕНИТЕ ВОЕНИ КОНФЛИКТИ

Калоян А. Илиев

“Vasil Levski” National Military University, “Artillery, Air-defence and Communication and Information Systems” Faculty, “Organization and management of the Field Artillery tactical formations” Department; town of Shumen.

INTERNATIONAL HUMANITARIAN LAW FACTOR IN MODERN MILITARY CONFLICT

Kaloyan A. Iliev

ABSTRACT: International humanitarian law is rooted in the norms established by the ancient civilizations on the conduct of hostilities. In many military conflicts have always existed certain rules and customs that are not always respected, but have always been the attention of military leaders.

International humanitarian law (the legal rules governing the conduct of the parties involved in armed conflict) covers all aspects of the conduct of the parties during the hostilities and the protection of victims of war, it is part of international law, the main sources of the latter are international treaties concluded by countries with customary rules and general principles of international law.

KEY WORDS: International humanitarian law, military actions, contemporary conflicts, armed forces, local conflict.

Международното хуманитарно право е част от международното право, а основни източници на последното са международните договори, сключвани от държавите, обичайните норми и общите принципи на международното право. Международното хуманитарно право се прилага към въоръжени конфликти – то не урежда въпроса дали една държава може да използва сила. Въпросите относно използването на сила от държавите са уредени в Устава на ООН^{14, 15, 16}.

Кодификацията на международното хуманитарно право започва през XIX в. От тогава държавите възприемат норми, основаващи се на опита във водене на военни действия. Тези норми целят да намерят баланса между хуманитарната необходимост и изискванията за удовлетворяване на военните нужди на държавите.

С увеличаването на международната общност все по-голям брой държави съдействат за развитието на тези норми. Международното хуманитарно право е универсално признато днес.

Същността на международното хуманитарно право може да бъде изразена най-ясно в четирите основни принципа:

¹⁴ Петко, Р. Женевските конвенции от 1949 г. за защита на жертвите на войната. София, Акад. издат. „Марин Дринов“, 1959.

¹⁵ Пашовски, С. Международното хуманитарно право – граница на насилието във въоръжените конфликти. София, Унив. издат. „Св. Климент Охридски“, 1990.

¹⁶ Каменова, Ц. Международното хуманитарно право (предизвикателства в началото на 21 век), Дисертация, БАН 2014.

(1) Военна необходимост – изразяващ се в нападения само върху военни цели;
(2) Хуманност – изразяващ се в забраната да бъдат нападани защитени лица;
(3) Пропорционалност – изразяващ се в забрана за използване на прекалена военна сила;

(4) Ограниченост – касаещ се за ограничаване на средства и методи за водене на военни действия^{17, 18}.

Тези основни принципи на международното хуманитарно право се приемат като критерии, от които военните командири са длъжни да се ръководят при планирането и провеждането на военни операции. Тези принципи трябва да се прилагат при всички видове военни конфликти – както при международните, така и при не международните. През изминалото десетилетие Европейският съюз ревизира политиката си по отношение на международното хуманитарно право, като престана да го третира като част от правата на човека, а започна да го третира като норми, които трябва да бъдат преценявани наред с правата на човека и все по-често се произнася във връзка с прилагането на хуманитарни норми по отношение на не международни въоръжени конфликти. Европейският съюз не се ограничава до „декларативната си практика“ по отношение на международното хуманитарно право, но се включва в граждански и военни операции по време на въоръжени конфликти. Цел на приетите насоки от Европейския съюз за съобразяване с принципите на международното хуманитарно право е да се формулират някои основни указания за Европейския съюз и неговите институции и органи за съгласуваност с международното хуманитарно право.

Проблемите, свързани с отговорността за нарушаване на международното хуманитарно право, придобиха първостепенно значение. Въоръжените конфликти не намаляха, нещо повече – в сърцето на Европа, в бивша Югославия, близо десетилетие (от 1991 до 1999 г.) се водиха ожесточени военни действия. Такива конфликти имаше и на други континенти: в Руанда, Сiera Леоне, Камбоджа, Източен Тимур и на много други места.

През последните десетилетия Международният съд на ООН в редица свои решения също се произнесе по проблеми на международното хуманитарно право. През периода 1995 – 2005 г. за първи път бяха положени основите на кодифицирането на обичайното международно хуманитарно право. Увеличиха се възможностите и ролята на мироопазващите сили на ООН, изпращани в горещи точки на земното кълбо за предотвратяване разрастването на вътрешни и международни въоръжени конфликти. Етническите конфликти са тлеещи конфликти, които сравнително лесно могат да прераснат във въоръжени конфликти.

Днес отново сме изправени пред аналогична ситуация. Нашата страна отново е заобиколена от въоръжени конфликти. На първо място е въоръженият конфликт, започнал в Сирия, разрастването му и провъзгласяването на т.нар. „Ислямска държава в Ирак. На второ място, не можем да игнорираме вътрешния въоръжен конфликт в Източна Украйна, който стана повод за все по-категоричното убеждение за това, че е поставено началото на нова Студена война между великите сили и ново блоково разделение на света. Ако конфликтът на територията на Сирия преди три или четири години ни се струваше твърде отдалечен от нашите граници, днес по-

¹⁷ Пашовски, С. Международното хуманитарно право – граница на насилието във въоръжените конфликти. София, Унив. издат. „Св. Климент Охридски“, 1990.

¹⁸ Каменова, Ц. Международното хуманитарно право (предизвикателства в началото на 21 век), Дисертация, БАН 2014.

токът от бежанци заплашва пряко българската национална сигурност. Не само българското общество, но и българските институции се оказаха неподготвени и не добре запознати със съществуващата международноправна уредба. Достатъчно е да споменем, че няма достъпен превод на български език на основните договорни източници на международното хуманитарно право.

Анализатори от различни държави предвиждат, че конфликтът в Украйна ще продължи с различна интензивност през следващите години и ще приключи най-рано през 2020 г.

Може без преувеличение да се каже, че този именно конфликт е повод за остри взаимни нападки между ръководителите на САЩ и на Руската федерация, той може да бъде посочен като една от причините за очертаващото се ново блоково разделение в света, което ще пречи за колективен отпор срещу т.нар. Ислямска държава.

Също така се констатира, че съществуването на въоръжен конфликт има значителни последици за действието на международното право – освен добре известния факт, че по време на въоръжен конфликт ще намират приложение нормите на международното хуманитарно право, държавите – участници във въоръжен конфликт, могат да имат правото да дерогират някое от своите задължения, произтичащи от нормите, които уреждат закрилата на правата на човека. Освен това държавите, даващи убежище на лицата, които се стремят да се избавят от насилието по време на въоръжен конфликт, имат задължение да сторят това; могат да бъдат засегнати договорни задължения или споразумения за контрол върху оръжията. Силите на ООН, включени във въоръжен конфликт, ще имат права и задължения, които не се прилагат при операции във въоръжен конфликт. Това са само някои от областите на международно право, които са повлияни от избухването на въоръжен конфликт. Ясно е, че съществуването на въоръжен конфликт е важен факт в международноправната система, но въпреки това не се констатира наличието на широко възприета дефиниция за въоръжен конфликт в нито един договор. Констатирано беше, че международната общност има общо разбиране за понятието въоръжен конфликт. Всеки въоръжен конфликт има някои минимални определящи характеристики, които го отличават от ситуациите на невооръжен конфликт или мирновременни ситуации. При отсъствието на такива характеристики, държавите не могат в съответствие с международното право да обявят, че една ситуация е или не е въоръжен конфликт.

Най-малко две характерни черти са типични за всички въоръжени конфликти:

- Съществуване на организирани въоръжени групи.
- Въоръжени групи, които са ангажирани в сражения с някакъв интензитет¹⁹.

Като допълнение към тези минимални критерии международното хуманитарно право добавя някои допълнителни критерии, за да класифицира конфликтите като международни или немеждународни.

Следователно въоръженият конфликт е едно съществено понятие в международното право, но дали съществува въоръжен конфликт зависи от това дали са налице обективни критерии. Определянето на тези критерии е било винаги предизвикателство в международното право. Това предизвикателство се увеличава през последните години със сблъсъка между привържениците на по-ясното разбиране

¹⁹ Каменова, Ц. Международното хуманитарно право (предизвикателства в началото на 21 век), Дисертация, БАН 2014.

на понятието въоръжен конфликт, което предоставя на държавите права на воюващи страни, и привържениците на тясна дефиниция, която защитава по-добре отделните лица. По време на въоръжен конфликт държавите имат особени права – да убиват без предупреждение, да задържат без съдебен процес и да дерогират договорни и други свои задължения. Отделните лица могат да имат право на живот, право на справедлив процес и други важни права, които обаче биват ограничени при въоръжен конфликт. Следователно, съществуването на въоръжен конфликт не само води до прилагане на международното хуманитарно право, но също така може да има влияние върху действието на международноправни норми, регулиращи отношенията между държавите^{20, 21}.

Международният комитет на Червения кръст последователно настоява правилствата да признаят воденето на сражения за въоръжен конфликт и да прилагат международното хуманитарно право. Но истински натиск за изясняване на проблема се появи след обявяването на „глобална война” и претенциите на САЩ да упражняват определени права, типични само за въоръжен конфликт, като например правото да убиват воюващи лица без предупреждение, да задържат без съдебен процес, да претърсват съдове в открито море и да конфискуват товари. Впоследствие държавите членки на Европейския съюз също се занимаха с понятието въоръжен конфликт, когато приемаха Директивата на Европейския съюз, предоставяща право на убежище на лица, бягащи от въоръжен конфликт. Ясно е, че съществува необходимост да се уточни различието между въоръжен конфликт и мирновременното състояние. Прилагането на международното хуманитарно право, на нормите за правата на човека, правото за търсене на убежище, както и на други международноправни принципи, зависи от разбирането на понятието въоръжен конфликт.

Друг аспект, на който трябва да се обърне внимание е съвременното технологичното развитие в областта на оръжията в началото на 21 век. Разглеждането и регулирането му трябва да бъде преценявано през призмата на чл. 36 от Допълнителния протокол I към Женевските конвенции. Този текст от цитирания акт гласи: При проучването, разработването, придобиването или приемането на въоръжение на нови видове оръжия, средства или методи за водене на война всяка високо договаряща страна има задължението да определи дали тяхната употреба, при някои или при всички обстоятелства, би попаднала под забраните на този протокол или на друга норма на международното право, приложими по отношение на високо договарящата страна.

Тъй като оръжията стават все по-сложни, спазването на това, на пръв поглед изглеждащо просто изискване на международното хуманитарно право става все по-трудно за изпълнение. Съвременните оръжия и функционирането им трудно могат да бъдат разбрани от неспециалист.

Едни от общите принципи, които са посочени в Международното хуманитарно право са Принципът на избягване на ненужни страдания и Принципът на разграничаването (discrimination). Принципът, закрепен в чл. 35 ал. 2 от Допълнителен протокол I, гласи: „Забранено е да се използват оръжия, снаряди и вещества като

20 Пашовски, С. Международното хуманитарно право – граница на насилието във въоръжените конфликти. София, Унив. издат. „Св. Климент Охридски”, 1990.

21 Каменова, Ц. Международното хуманитарно право (предизвикателства в началото на 21 век), Дисертация, БАН 2014.

методи за водене на война, които биха могли да причинят прекалено големи поражения или ненужни страдания^{22, 23}.”

Този принцип може да се разглежда като част от по-общия принцип на военната необходимост. Той се прилага както по отношение на оръжията, така и по отношение на методите за водене на военни действия. Принципът на разграничаването забранява използването на произволни оръжия, или по-скоро произволното използване на всяко оръжие.

Този принцип, от своя страна, включва три компонента:

– Първи - забранено е нападението над цивилни лица и граждански обекти, т.е. трябва да се спазва принципът на различаването (*distinction*);

– Втори - даже ако целта е легитимна военна цел, според принципа на пропорционалността е забранено нападението да бъде извършено, ако то заплашва да причини загуба на живота на цивилни лица или щети, които биха били прекалени във връзка с конкретните предвидими военни предимства;

– Трети - необходимост от вземане на предохранителни мерки.

Правните норми, относно използваните видове оръжия, имат за цел да уредят както средствата, така и методите на т.нар. „Право на войната”. Но често те се характеризират, като най-малко ефективни. Тук трябва да отбележим, че значителният прогрес в развитието на средствата и методите за водене на военни действия през 20-ия век трудно може да бъдат догонени от развитието на правото. Резултатът от това е, че голям брой правни норми както и правната литература в тази област оставят впечатление за анахронизъм. Например, забраната да се използват оръжия, причиняващи прекомерни страдания, бе установена за първи път преди цяло столетие, но тази забрана е част от действащото право и бе взета пред вид от Международния съд на ООН, за да се произнесе за законността на ядреното оръжие. Към края на 20-ия международната общност стана свидетел на безпрецедентна дейност за забрана на някои видове оръжия. Приети бяха договори, забраняващи използването на заслепяващи лазерни оръжия, на антиперсонални мини, както бе създаден и универсален договор, забраняващ използването на химически оръжия.

Най-важното развитие през последното десетилетие на 20 век относно правните норми при различните видове оръжия, е приемането на Конвенцията за забрана на разработването, производството, натрупването и употребата на химическо оръжие и за неговото унищожаване. Тази конвенция бе приета през 1993 г. и в литературата се нарича „Новата конвенция за химическите оръжия”. Почти всички държави са ратифицирали тази конвенция. Тя е един от най-добре разработените международно правни актове за забрана и контрол на въоръжението. Тя е първият многостранен договор за разоръжаване, който има за цел да ликвидира една цяла категория оръжия за масово унищожаване.

Прегледът на постигнатото до момента в правното регулиране на различните видове оръжия в края на 20 и началото на 21 век показва, че тази част от международното хуманитарно право, въпреки че не може да бъде характеризирана като най-ефективно действаща, не може също така да бъде игнорирана като анахронизъм. Приемането на нови договори за оръжия, които имат голямо военно значение (напр. химическите оръжия и сухопътните мини) показва, че е възможно да се

22 Пашовски, С. Международното хуманитарно право – граница на насилието във въоръжените конфликти. София, Унив. издат. „Св. Климент Охридски”, 1990.

23 Каменова, Ц. Международното хуманитарно право (предизвикателства в началото на 21 век), Дисертация, БАН 2014 г.

развиват правни режими, които имат значително влияние за защитата на ценностите, защитавани от международното хуманитарно право. Съвещателното мнение на Международния съд по делото за ядрените оръжия показва, че общите принципи на правото могат да бъдат прилагани към нови видове оръжия.

Правното регулиране на използваните оръжия е част от международното хуманитарно право и поради това то отразява целите на международното хуманитарно право като цяло. Целта на международното хуманитарно право е на първо място да се съхранят, доколкото е възможно, някои хуманитарни ценности по време на враждебни действия. То няма за цел да предотврати или да откаже държавите да използват сила и ограниченията, които то налага, не трябва да бъдат несъвместими с ефективното водене на враждебни действия. Всяка държава има право на самозащита според международното право и има право да използва сила при осъществяване на самозащитата си.

Международното хуманитарно право налага ограничения относно това, какво може да извърши държавата, упражнявайки това право, но неговата цел не е да предотврати ефективното упражняване на правото. Международното хуманитарно право се основава на предположението, че държавите, ангажирани във въоръжен конфликт, по необходимост ще причиняват смърт и нараняване на физически лица и разрушаване на собственост. То цели да ограничи тези последици като предотвратява изключителните страдания и разрушения, които не са необходими, тъй като не преследват полезна военна цел. Правото изисква даже когато разрушенията имат военна цел, да се търси и намира баланс между постигането на тази цел и на други ценности, като например запазване живота на цивилни лица.

Правните норми забраняват нападения, при които военното предимство, очаквано от тях, е значително по-малко от уврежданията, с които ще се нарушат тези ценности. Основната цел на правните норми, уреждащи използването на различни видове оръжия, е защитата на тези ценности. Хуманитарните цели на тези правни норми често се смесват със загрижеността за разходите за въоръжението.

Изводи:

➤ Международното хуманитарно право има задължителен характер във всеки един въоръжен конфликт то принуждава държавите да изпълняват определени принципи за прилагане на сила, като търсят баланса между хуманитарната необходимост и удовлетворяване на военните нужди на държавите.

Литература:

1. Петко, Р. Женевските конвенции от 1949 г. за защита на жертвите на война. София, Акад. издат. „Марин Дринов“, 1959.
2. Пашовски, С. Международното хуманитарно право – граница на насилието във въоръжените конфликти. София, Унив. издат. „Св. Климент Охридски“, 1990.
3. Каменова, Ц. Международното хуманитарно право (предизвикателства в началото на 21 век), Дисертация, БАН 2014.

НАЦИОНАЛНИТЕ СЪВМЕСТНИ СИЛИ - ГАРАНТ ЗА СИГУРНОСТ

Калоян А. Илиев

“Vasil Levski” National Military University, “Artillery, Air-defence and Communication and Information Systems” Faculty, “Organization and management of the Field Artillery tactical formations” Department; town of Shumen.

NATIONAL JOINT FORCES - SECURITY GUARANTEE

Kaloyan A. Iliev

ABSTRACT: The end of the Cold War symbolically terminate block opposition and reduce the risk of a global world war with unpredictable consequences. But he put the beginning of a number of local military conflicts in a peculiar way marked the last 20 years. They became the scene of serious political oppositions and all were solved using military force. While generated and catalyzed by different reasons in different geographical areas for solving them they were used national and multinational joint forces which had participated soldiers of the Bulgarian Army.

National joint forces are national (unified) combined from all kinds of armed forces operational (tactical) organized group formed to perform tasks that require a command and control headquarters of national joint forces.

KEY WORDS: National joint forces, military conflicts, armed forces, local conflict, military operations model for European security.

Въоръжените сили на държавите членки на НАТО могат да формират от своя състав национални или многонационални съвместни сили. Това правило не изключва и възможността в техния състав да могат да се включват и елементи от страни партньори, които не са членки на Алианса. Това показва, че операцията следва да се провежда под егидата на международни организации като например от ООН и Организация за сигурност и сътрудничество в Европа или Европейския съюз. Те следва да извършват политическия контрол за провеждане на операцията с мандат по глава 7 от Устава на ООН, за което съществуват два начина:

- Първият – операцията се ръководи от Съвета за сигурност на ООН;
- Вторият – като оторизирана операция^{24 25}.

Оторизираните операции се разглеждат като такива след приемане на резолюция от Съвета за сигурност на ООН, за провеждане на конкретна операция и възлагане на мандат на съответната международна организация, съюз, нация или коалиция от държави. Самото ръководство, планиране и провеждане на операцията, както и дейностите по предоставяне на войски и ресурси се извършва в съответствие с дадения мандат на създадената коалиция. Самото структуриране на формиранията, развърщането на силите, а и всички действия на войсковите формирова-

²⁴ Доктрина на съвместните операции. ГЩ на БА 2001г.

²⁵ Доктрина на съвместните операции на съюзническите войски (АJP – 01 (А). 2001

ния по провеждане на операцията може да се повери и на регионална организация или държава (нация).

Стремежът на НАТО в последните години е бързо да реагира и адекватно да отговори на продължаващите промени в областта на сигурността.

За да отговори на новите предизвикателства пред сигурността в световен мащаб през 1994 г. се въвежда военната концепция за многонационални съвместни сили (МСОС) – Combined Joint Task Force (CJTF). В същото време концепцията и свързания с нея модел за европейска сигурност поставят важни въпроси пред България като страна вече член на НАТО и като отговорен участник в развиващата се система за Европейска сигурност. Идеята е да се предостави на НАТО гъвкав инструмент за провеждане на оторизирани операции, включително операции съвместно с държави извън съюза, като се подобри способността на НАТО в кратки срокове да развърне национални и многонационални съвместни сили, включващи компоненти от различните родове войски, създадени за конкретни военни задачи като хуманитарни и мироопазващи действия. Към настоящият момент Северноатлантическият съюз се явява и единствената международна военнополитическа организация с възможност и готовност за провеждане на такива операции. Точно за това командната структура и управленските процедури са близки до възприетите в Северноатлантическия договор. За провеждането на операциите се използват развърнатите съюзни съвместни командвания със съответните им компоненти, като допълнително се привличат и други държави. В резултат, командната структура е комбинирана, като силите от държавите, членки на НАТО, реализират интегрирана командна структура, а тези от другите нации се включат в паралелни структури^{26, 27}.

Много от характеристиките на концепцията за многонационални съвместни сили се прилагат при мироопазващите операции на Балканите под командването на НАТО. Концепцията предвижда създаването на отделими, но не постоянно отделени, военни сили, които да се използват от НАТО или при определени обстоятелства от Европейския съюз. Тези сили служат като основа за формирането на многонационалните съвместни сили, които по своята същност са многонационални формирования от видовете въоръжени сили, родовете войски и служби, сформирани за изпълнение на определена мисия, подготвени за участие в пълния спектър от военни задачи на Алианса, отговарящи на изискванията за многонационално командване и управление.

Националните съвместни сили постигат и поддържат необходимото равнище на оперативна съвместимост с цел осигуряване на възможност за участие в коалиционни сили за отбрана в контекста на приоритетната цел за членство в НАТО и ЕС.

Националните съвместни сили под формата на свързани помежду си щаботе и формирования имат способност за бързо и ефикасно въвеждане в и извън територията на страните членки на Алианса, включително и в зони с ограничено или липсващо сътрудничество и поддръжка на домакинстваща нация. Първостепенна мисия на националните съвместни сили е водене на операции в отговор на кризи

²⁶ Доктрина на съвместните операции. ГЩ на БА 2001г.

²⁷ Доктрина на съвместните операции на съюзническите войски (АЖР – 01 (А). 2001

извън обхвата на член 5. Въпреки това, не е напълно изключено създаване и използване на такъв вид сили и за операции по член 5²⁸.

В структурата на НАТО границите за провеждането на операциите от национални съвместни сили зависят от развитието на обстановката и характера на мисията. Те трябва да се използват така, че да повишават гъвкавото и нелинейно очертаване на зоните, ограничени от определени показатели и параметри като време и обсег. С изключение на границите на секторните и регионалното командване (Командване на НАТО за Европа), всички останали граници се обуславят и зависят от мисиите и се ограничават от определени съгласувани параметри (време, обсег и др.).

Операциите на националните съвместни сили²⁹ се ръководят, планират и провеждат на три нива. Те се ръководят от стратегическия командващ, а се планират и изпълняват на оперативни и тактическо ниво. Действията се определят като: стратегически, оперативни и тактически, базирани на влиянието им или приноса за постигане на поставените цели^{30, 31, 32}.

На стратегическото ниво, въоръжените сили се развърщат и използват в съответствие с политическата рамка и в синхрон с други невоенни инициативи (например дипломатически или икономически), с цел да се достигнат стратегическите цели на Алианса в колективната система за сигурност.

На оперативни ниво и в определената зона за съвместни операции, въоръжените сили се развърщат и използват в съответствие със стратегията на кампанията за постигане на стратегическите цели. Обикновено това включва непрекъснати операции с едновременни или последващи действия на съюзни сили.

На тактическо ниво, силите се използват, за да изпълняват бойни задачи и да постигат военни цели. Успешното постигане на тези цели е предпоставка и основен принос за успеха на оперативните и стратегическите нива.

В операциите на съвместите сили може да има основни (ведещи) и поддържащи операции, които се провеждат от компонентите. В зависимост от фазата на операцията на съвместните сили водещата операция може да бъде на сухопътния, военновъздушния или военноморския компонент, при което операциите могат да бъдат сухопътни, въздушни и морски. Когато единият от компонентите провежда основна операция, другите провеждат поддържащи операции в негов интерес^{33, 34, 35, 36}.

Сухопътни операции. Сухопътната операция в много от случаите е основа за изпълнението на мисията от съвместните сили при разрешаване на кризата. Тя може да се проведе като водеща и да е в началото или в завършващия етап от операцията на съвместните сили. В зависимост от условията за постигане на целите на съвместната операция сухопътна операция може и да не се провежда. Когато се провежда, тя най-често е съвместна и в нея участват и останалите компоненти на съвместните сили. Сухопътните операции обикновено включват удържане на позиции, унищожаване на противникови сили и връщане на загубени територии. За

28 Ръководство за планиране на операциите, МО на РБ, 2011

29 По надолу в дисертационния труд всяко казано за съвместни оперативни сили се отнася за национални съвместни оперативни сили, ако изрично не е указано друго. Затова се използва обобщеното понятие съвместни оперативни сили.

30 Ръководство за планиране на операциите, МО на РБ, 2011

31 Доктрина на съвместните операции. ГЩ на БА 2001.

32 Доктрина на съвместните операции на съюзническите войски (АJP – 01 (А). 2001

33 Ръководство за планиране на операциите, МО на РБ, 2011

34 Доктрина на съвместните операции. ГЩ на БА 2001г.

35 Доктрина на сухопътните войски – част 1, 2001.

36 Доктрина на съвместните операции на съюзническите войски (АJP – 01 (А). 2001

да осигурят тези ключови възможности, основните сухопътни части от обединените сили трябва да включват бронирани, механизирани и ударни авиационни сили, които се характеризират с високо ниво на бойна мощ, маневреност, способност за оцеляване, издръжливост и мобилност³⁷.

За изпълнение на поставените цели в операциите сухопътните сили провеждат отбранителни и настъпателни операции.

Успехът при сухопътните операции може да зависи от изхода на действията, проведени от другите формирования, като например - да се подготви бойното поле и да се намалят силите за съпротива у противника още преди началото на сухопътната операция. За провеждането и се използват огневи удари по цели, които ще оказват съществено влияние при провеждането на сухопътната операция.

Въздушни операции. Военновъздушният компонент заема основно място в състава на съвместните сили. Той се сформира на базата на Военновъздушните сили на страните – участнички в съвместните сили и играе важна роля в борбата за завоюване и удържане на огнево превъзходство.

Основни въздушни операции в рамките на операции, провеждани от съвместните сили, са:

- Противовъздушни операции
- Изолиране зоната на операциите
- Непосредствена авиационна поддръжка
- Разузнаване и наблюдение
- Въздушен транспорт
- Специални действия

Въздушните операции в началото на операцията се провеждат от авиационните средства за поразяване на военновъздушния и военноморският компонент, като осигуряват и поддържат в желаната степен контрол върху зоната на бойните действия. Мероприятията и действията, свързани с непосредствена авиационна поддръжка на маневрените формирования, зависят от цялостната стратегия на операцията и конкретната обстановка, действията на групировките на противника, фазата на операцията, степента на въздушния контрол и от потребностите на маневрените формирования.

Морски операции. Морските операции се провеждат от военноморския компонент от състава на съвместните сили и включват всички действия, извършвани от силите на, под или над морската повърхност, за установяване или упражняване на господство на море, контрол на морските пространства или лишаване от достъп до морските пространства в зоната на морските операции.

Морските операции във висока степен се отличават от сухопътните. Основна причина за това е, че съгласно нормите на международното законодателство, преобладаваща част от морето и прилежащото му въздушно пространство остават по същество неутрални и не обитавани. Морето не може да бъде „притежавано“ така, както сушата.

Спецификата на морските операции се усложнява допълнително от факта, че държавите могат да тълкуват и прилагат международноправните норми, акцентирайки върху различни „нюанси“ на заложените в законите идеи.

Независимо от обширните морски пространства, действията на военноморския компонент най-често се провеждат в близост до брега, където морската среда рязко

37 Доктрина на сухопътните войски. Част втора. Тактическа доктрина на Сухопътните войски. София. 2001

се различава от обичайната и се ограничава маневреността на силите. Това налага той да решава задачите си в тясно взаимодействие с другите видове въоръжени сили в рамките на съвместните сили.

Основната цел на морските операции е да се осигури открита, продължителна и неограничена подкрепа на националните, респективно съюзните интереси в морските пространства.

Основни (водещи) морски операции са преди всичко тези, които са свързани с решаване на задачи в чисто морско направление, като нарушаване на противникови и защита на свои комуникации, унищожаване на ударни групировки на противника и отразяване на удари по своите сили. Такива операции са: господство на море; контрол на морските пространства; лишаване от достъп до морските пространства; използването на морска мощ (проекция на морската мощ); налагането на морска блокада.

Специални операции. При провеждането на операциите от съвместните сили се формира и компонент от силите за специални операции, който компонент играе съществена роля в борбата за завоюване и удържане на огневото превъзходство над противника.

Маневрените формирования по принцип не са обучени, екипирани или организирани да провеждат специални операции. Всяка по голяма промяна на задачите им би могла да ограничи техните способности да изпълняват основните си задачи.

Специални операции са военни дейности, провеждани от специално предвидени, организирани, тренирани и оборудвани сили, използващи нетипични за конвенционалните сили оперативни техники и начини на действия.

Необходимостта в борбата за огнево превъзходство да се търсят и поразяват стратегически или оперативни цели с малки формирования, да се определят координати на цели, да се насочват удари и огън по важни цели в дълбоките операции е наложило създаването на специални формирования с определени специални възможности. Ето защо тези формирования имат основната и важна задача да провеждат специални операции. Понякога, при определени обстоятелства, маневрени формирования могат да бъдат назначавани за провеждане на специални операции.

Използването на силите за специални операции зависи от много и различни фактори и обстоятелства. Въпреки, че силите за специални операции често използват усъвършенствани и нетрадиционни методи и оборудване, ключът към успеха им е в индивидуалните способности на личния състав. Затова е много важно плановете и процедурите, които управляват използването им, да бъдат прости и недвусмислени, с цел намеренията на командването да могат да бъдат лесно разбираени.

Борбата с разпространението на оръжия за масово унищожаване се заключава в локализиране, отнемане и пленяване на оръжията. Главните цели на операциите са пресичане на пътищата за сдобиване с оръжия и носителите за тях и предотвратяване на тяхното използване. Продължаващото разпространение на технологиите за производство на оръжия за масово унищожаване може да разпали регионални политически противопоставяния и в ръцете на терористите да попаднат нови и мощни оръжия.

Сили за психологически операции. Психологическите операции се определят като „планирана психологическа активност, предназначена за въздействие върху начина на мислене и поведение за изпълнение на политическите и военните

задачи”. Те спадат към несмъртоносните средства за поразяване и играят определена важна роля в борбата за огнево превъзходство. Психологическите операции включват: стратегически психологически действия; укрепващи психологически действия; психологически действия на бойното поле и мироподдържащи психологически действия. На оперативен и тактическо ниво, психологическите действия на бойното поле и мироподдържащи психологически действия, обикновено включват военни сили, участващи в разрешаването на конфликти и операции в отговор на кризи.

Във всяка операция главната мисия на контингента на силите за психологически операции е да поддържа информационната операция, провеждана от съвместните сили, гражданско-военното сътрудничество и силите за специалните операции.

Психологическите действия в зоната на съвместните операции се планират и ръководят като неразделна част от борбата за завоюване и удържане на огневото превъзходство. Те са насочени към противника за снижаване на бойната му мощ, чрез деморализиране на войските. Планират се предварително в мирно време и се изпълняват като елемент на операциите в хода на военните действия. Психологическите дейности, проведени в правилния момент, могат значително да намалят влиянието на използването на сила в операциите.

Предимствата на психологическите операции трябва да бъдат използвани пряко за получаване на подкрепа на гражданско-военното сътрудничество, за да се дава гласност на провежданите дейности и се пропагандират успехите. Те значително могат да подсилат увереността на местното население за координирани действия срещу противникови усилия за разрушаване на единството в зоната на операцията.

Информационните операции се провеждат в тясно взаимодействие с психологическите операции. Информационните операции от своя страна представляват акции, провеждани с цел ограничаване възможностите на противниковия информационен поток и информационни системи, като в същото време се защитават собствените такива. Те могат да се провеждат през всички фази на дадена операция, в рамките на няколко операции или през всичките фази на войната. Информационните операции включват възможност за провеждане на редица действия: операции засягащи компютърните мрежи, електронна война, оперативната сигурност, психологически операции и въвеждане на противника в заблуждение^{38, 39, 40}.

Изводи:

➤ Командващият на Съвместното командване на силите има пълното командване над подчинените му структури, войски и сили в мирно време и при кризи. Той осъществява правомощията си чрез подчинените му командващи.

➤ В операциите на съвместните сили всеки компонент има определен принос за изпълнение на общата мисия и допринася за реализирането на желаните ефекти от старшия щаб. За постигане на исканите (желаните) ефекти в операцията на съвместните сили трябва да се интегрират усилията на всички средства за разузнаване и въздействие, като в основата на въздействието следва да бъде съвместната огнева поддръжка.

38 Доктрина на съвместните операции. ГЩ на БА 2001г.

39 Доктрина на сухопътните войски – част 1, 2001.

40 Доктрина на сухопътните войски. Част втора. Тактическа доктрина на Сухопътните войски. София, 2001

Литература:

1. Доктрина на съвместните операции. ГЩ на БА 2001.
2. Доктрина на съвместните операции на съюзническите войски (АJP – 01 (А). 2001.
3. Ръководство за планиране на операциите, МО на РБ, 2011.
4. Ръководство за планиране на операциите, МО на РБ, 2011.
- 5 Доктрина на сухопътните войски – част 1, 2001.
- 6 Доктрина на сухопътните войски. Част втора. Тактическа доктрина на Сухопътните войски. София. 2001.

МОДЕЛ ЗА УПРАВЛЕНИЕ НА ОПЕРАЦИЯ ЗА РЕАГИРАНЕ ПРИ КРИЗА, ВЪЗНИКНАЛА ВСЛЕДСТВИЕ НА БЕДСТВИЕ ИЛИ АВАРИЯ

Христо А. Христов

*Шуменски Университет „Епископ Константин Преславски”, Шумен
Факултет по технически науки
e-mail: hristov63@abv.bg*

A MODEL ON CONDUCTING AN OPERATION ENABLING REACTION TO CRISES CAUSED BY DISASTERS OR ACCIDENTS

Hristo A. Hristov

ABSTRACT: *Elaboration of the model provides the connection between the new-coming situation and the ultimate wanted condition of the crisis. The model allows through a series of consecutive actions to accomplish a result in regard to current goals' realization, to decrease the risk level and to attain one acceptable condition for the existing crisis. Defining critical elements of this activity turns out to be the main step which elements should be influenced on and chronologically attached to activities' aims.*

KEY WORDS: *Governor, Risk assessment, operational center, Regional Directorate of the Interior Ministry, Regional Directorate „Fire Safety and Population Protection”, Ministry of Defense*

Въведение

Предложеният модел за управление на операция за реагиране при криза, възникнала вследствие на бедствие или авария, включва няколко етапа. Първи етап се явява оценка и анализ на ситуацията. Този етап подпомага оценката на риска от операцията, определянето на необходимото количество сили и средства и ангажирането на допълнителни сили, синхронизацията на различните операции.

Целта на етапа е събиране и анализ на наличната информация за обща оценка на ситуацията и събитието. Извършва се мониторинг на текущата обстановка, организира се наблюдение и диагностика на кризисните показатели, определя се промяната в степента на риска, определят се границите на развитие на събитието и евентуалните граници на операцията, оценява се степента на развитие на ситуацията и заплахата от превръщането ѝ в криза [10].

В дейностите участват представители на Областна дирекция на МВР, Областна дирекция на ПБЗН, МО, външни представители на елементите на критичната инфраструктура от местно и регионално ниво. С началото на етапа се развързва Оперативният център [1].

Изложение

Същност на дейностите:

- Областен управител (или негов представител) определя зоната на аварията, бедствието;
- Аналитични групи от експерти (от общините, Областна Дирекция ПБЗН) определят нивата на настоящите рискове и промяната в нивата на допустимост;
- Формулират се новопоявили се рискове от:
 - наводнения, разширяване на огнища от пожари;
 - повреди по електрическите, ВиК и газопреносни системи;
 - второстепенни заплахи от химическо заразяване;
 - хуманитарни бедствия;
 - заплахи от проява на тероризъм и мародерство.
- разпределят се групите от участници, при необходимост се създава изнесен щаб в района на бедствието (временен оперативен щаб).

Всеки участник предоставя анализ на информацията от своя ресор и изпълнението на предприетите мерки. Оценяват се:

- социалните фактори (пострадали, защитеност на населението);
- икономически фактори (размери на щетите и перспективи за тяхното количество);
- инфраструктурни фактори (съоръжения и инсталации в зоната и тяхната важност за нормалното функциониране на живота на населението);
- информационни фактори (елементи, които съхраняват, натрупват и имат право да разпространяват информация, медии, интернет и др.).

Анализът на ситуацията се извършва от експертите и членовете на кризисния щаб по следните показатели:

- развитие на ситуацията, произход, инициращи причини, превърнали заплахата в бедствие;
- основни координиращи взаимовръзки;
- динамика на ситуацията в момента на работа и фактори, влияещи за стабилизация или ескалация на бедствието;
- приложени към момента части от планове за защита и тяхната ефективност;
- недостиг от информация и пътища за нейното натрупване;
- необходими средства и сили за активиране от незасегнати райони, на централно подчинение, техника от частни фирми и др.

Втори етап на предложения модел – обща оценка на ситуацията. Етапът позволява в първата част да се обобщят изводите за ситуацията, а с втората част насочва екипа към вариантите за провеждане на операцията.

Същността на действията има за цел да се формулира оперативна оценка за събитието и разпределение за разработване на вариантите. Желаният краен резултат са целите, които се постигат с операцията при наложените ограничения и критерии за постигане на целите на операцията [8].

Етапът преминава през стъпките:

- активиране – активират се обектови и регионални сили, осъществява се окончателната връзка с други агенции и организации, актуализиране на информацията и увеличаване на разузнавателните усилия;
- оценка – уточнява се точното време на събитието, определя се времето до неговата кулминация или преустановяване на активността му, набелязват се потенциалните задачи и се определят искванията, насочени към централния щаб;
- указания на областния управител – увеличаване на групата при необходимост, изисквания за външно сътрудничество, времеви график за формиране на решението, необходимост от съдействие, критерии за успех и съображения за поемания риск;
- анализ – извършва се комплексен анализ на възникналата ситуация, в който се преценява съпоставимостта ѝ със ситуации, за които има разработени планове, необходимата им корекция и привеждането им в действие. Тази стъпка може да доведе до приемане на ускорено решение и прилагането му в неутрализиране на ситуацията.

В резултат на този анализ областният управител може да издаде заповед за извънредно положение, да уточни готовността на силите и средствата и след адаптация, да пристъпи към прилагане на предварителен план за провеждане на операцията.

Развитието на кризата се определя, като се оценяват основни аспекти, влияещи върху нейната динамика:

- среда (сезон, хидрография, релеф и др.);
- съпътстващи заплахи (следствени бедствия и допълнителни опасности);
- икономически аспекти на бедствието (застрашени производства, търговия, разпространение на стоки);
- социални аспекти (здравеопазване, опасности от епидемии, бежански потоци);
- инфраструктурни аспекти (пътна мрежа, енергоразпространение, комуникации);
- влияние на всички участници в операцията (структури, имащи решаващ принос към овладяване на кризата);
- медийна комуникация.

Способностите за оценка за постигане на крайното състояние зависят и могат да се оценят по:

- оценката на силите и средствата (способностите на силите с най-висока готовност, времето за подготовка на останалите сили, необходимост от нарастване на участниците в операцията);
- оценката на наличните ресурси (транспорт, логистика, медицинско осигуряване, КИС);

- оценката на риска и изпълнимостта на крайното състояние.

Като трети етап на изследвания модел се явява ориентирането на екипа. Целта на етапа е анализ на задачите, които предстоят да се решават за постигане на успех в специфични условия и ключови фактори.

Дейностите, в зависимост от времевите параметри и степента на развитието на кризата, обхващат анализ на общата обстановка и факторите, влияещи върху нея, анализа на средата (време, географски и хидрографски особености), ограничения в действията, необходимо взаимодействие.

Краен резултат от този етап са задачите и организирания условия за тяхното изпълнение, целите на операцията, необходимите способности на изпълнителите, системата от елементи (инициатори) на кризата, върху които трябва да се действа приоритетно и координацията на действията между участниците.

Същността на дейностите има определена последователност, която може да се променя в зависимост от условията и наличното време. Тя обхваща:

Начало: Областният управител отбелязва основните събития, причинили кризата, необходимостта от преценка за приложимост и адаптация на съществуващите планове, действията на участниците в ликвидиране на кризата, техните ръководители и координатори.

Условия: Обобщават се нивото, обхватът и динамиката на създалата се ситуация, ключови фактори, налични участници за разрешаване на кризата, заплахи за региона от екологично естество, за граничните райони – възникнали международни ангажименти, състояние на общественото мнение.

Анализ на среда и участници: Анализът на средата определя външните условия, при които ще се провежда операцията. Той обхваща няколко елемента:

- Зона на операцията – размери, част от територията в проценти, разстояния, възможен достъп, налични бази от ресурси в зоната.
- География – релефът на месността, хидрография, пътна мрежа, възможни препятствия.
- Демография – пострадали, миграционни потоци, население в риск и необходимост от хуманитарна помощ.
- Икономика – заплахи за енергийна изолация, промишленост, застрашена от бедствието, застрашени източници на храна и вода.
- Социална обстановка – заплахи от екстремизъм и доминиращи групи население.
- Инфраструктура – зони за преминаване на транспорти, пътни съоръжения, складове, ГСМ и възможности за заплахата им.
- Здравеопазване – рискове от епидемии, пострадали, ранени, смъртни случаи.
- Информация и медии – обществен достъп до информация и периодична осведоменост.

Оценката на участниците се определя от етапа на развитие на кризата, състоянието на силите и средствата, които участват в редуцирането на кризата и тяхното нарастване във времето и възможните действия за овладяване на кризата със собствени, регионални и национални сили.

Анализ на задачата: Той обхваща четири страни, при които се анализират:

- времеви параметри на кризата (времетраене от началото ѝ до евентуален край, време за нарастване на количествата сили и средства, рискове при ограничаване във времето);

- район на кризата (изменения в релефа, райони за разполагане на силите, опасни райони);

- участници в овладяване на кризата (количества и техните възможности, модулни способности, рискове за участващите, допустими нива на критични способности);

- изисквания (предпоставки за успех и приоритетни направления);

- ограничения;

- рискове за успеха.

Анализ на елементите от кризата, подлежащи на въздействие: Дейността се извършва последователно от всеки участник в заседанието на съвета, според ред, определен от областния управител. Анализът служи за определяне на действията, от които кризата ще се забави или предотврати и способностите на силите, които имат най-силно влияние върху бедствието. Редът за извършване на анализ включва: елемента, към който да се въздейства с минимални последствия, кой и с какво може да въздейства (хора и техника), какво трябва да се направи, какви способности да се изграждат в силите за въздействие.

Оценка на условията. Окончателно областният управител определя целите на операцията, критериите за успех и показателите за постигане на ефективност.

Разработването на модела осигурява връзката между създалата се ситуация и желаното крайно състояние на кризата. Моделът дава възможност с ред последователни действия да се постигне резултат, в изпълнение на текущите цели, намаляване на риска и достигане на приемливо състояние на възникналата криза. Основни стъпки в тази дейност се явяват определянето на критичните елементи, върху които трябва да се въздейства и хронологичното им обвързване с целите на действията.

Следващата стъпка е оглед на района на бедствието, което може да стане визуално, по карта или с използване на съвременни безпилотни средства. Използването на интерактивни методи, като интернет-базирана система за регистрация, визуализация и ползване на данни и анализи с RFMEA, методи за мониторинг и превантивно ресурсно управление на риска от природни бедствия, данни от ЦАН и Българска инфраструктура за пространствени данни, допълнително улеснява дейността на ръководителя.

Крайна стъпка са указанията на ръководителя (областния управител) до изпълнителите, свързани с:

- вероятност за ескалация на бедствието;

- времеви параметри на дейностите;

- целта, която трябва да се постигне и вариантът за разработване;

- обвързаност на действията с националните органи за управление;

- необходимост от помощ и усиление;

- критерии за успеха.

Целта на етапа, разработване на план за провеждане на операцията, е да се определи най-ефективният начин за провеждане на операцията. В преминатите етапи са определени условията за провеждане на дейностите: известни са оценките и анализът на ситуацията, определени са целите на операцията, фиксиран е моделът на операцията и са определени критериите за успех. Дейностите преминават последователно в няколко стъпки.

Анализ на възможното развитие на кризата. Тук се обобщават последните данни за кризата, определя се стадият на бедствието и възможната ескалация, определят се критични точки и зони, които да се овладеят с цел недопускане на разрастване или намаляване скоростта на развитие, оценяват се условия, които ще намалят ефективността на силите, търсят се алтернативи за действие.

Разработване на частни варианти за действие. Те се развиват от специалисти от ОДПБЗН, МЗ, МО, специалисти по ОМП в областта и други експерти по специфичните направления. В разработените варианти се отбелязват: последователността на въздействията върху критичните точки и очакваните резултати от това, силите, участващи в действията и евентуални допълнителни действия.

Анализ на вариантите. Екипът анализира вариантите по определените критерии, свързани със социалната значимост на кризите от подобен характер: приемливост, изпълнимост, максимална защита на населението, минимална загуба на хора и техника и завършеност. В процеса на анализа се сравняват необходимите сили и способности за всеки вариант (готовност, как ще се използват и необходимост от допълнителни сили) и развърнатите сили до момента (колко, транспорт за прехвърляне на специална техника, международно участие и др.).

Сравняване на вариантите. Съпоставянето се извършва по критериите за анализ на вариантите, максималното използване на силите, предимства и недостатъци и количество на риска във всеки вариант и за всеки източник. Тази стъпка определя и необходимото въздействие върху риска (пълно неутрализиране, редуциране или ограничаване на последствията) в зависимост от неговата степен (неприемлив, условно приемлив и приемлив).

Избраният вариант (по числени стойност или по предпочитане) е решението на областния управител, по което се изготвя планът за операцията или се пристъпва към разработване на нов анализ и решение.

Разработване на плана. Целта е да се детайлизира избраният вариант, да се уточнят действията на силите, тяхната всеотпадна поддръжка и взаимодействие. За осъществяването на планирането са изпълнени началните условия: известен е вариантът, количеството сили и тяхното нарастване, определени са крайните условия на операцията. Действията имат определена последователност.

Актуализиране на информацията за развитие на кризата и адаптиране на предварително планираните дейности към създалата се конкретна обстановка. Планиране на активирането на допълнителните сили и нарастване на техните способности до необходимото ниво и изпращане на указания до тях. Планиране на развърщането на комуникационните канали.

Определяне на разпределението на районите и зоните за действие на участниците и координиране на действията от различните участници.

Областният управител разпределя отговорностите по изготвянето на отделните части и анекси на плана между членовете на щаба и определя общия отговорник (експерта по ОМП). През време на неговото изготвяне координира действията на екипа и синхронизира дейността. След изготвянето плана се обявява и се изпраща до изпълнителите [1].

Същността на планирането е да определи точно и ясно:

- реда за използване на силите, рамката на ограниченията за прилагане на влияние върху елементите на кризата;

- обема и последователността на задачите и факторите, които могат да попречат на тяхното изпълнение;

- синхронизирането на изпълнението на задачите: придвижване и подход в зоната на операцията, взаимодействие между участниците, формиране на резерви, логистика, евакуация на пострадали и снабдяване на гражданите с вода, храна, електричество, медицински услуги и др.

Планира се и работата на системата за управление:

- Необходими сили и средства, организация на дежурни в кризисния щаб.
- Места за развърщане на органите за управление, необходимост от щаб на място и комуникацията с него.
- Способи за изграждане на комуникационната структура и ред за нейното функциониране.

Извършва се планиране на логистичната поддръжка на силите в зоната на операцията, финансовото осигуряване на операцията и следоперационния период.

За операцията се планират:

- мероприятия по сигурността и защитата на силите и гражданите и сили за тази дейност;
- ограниченията и правилата за придвижване в зоната.

Прилагане на решението и оценка. Прилагането на плана става със заповед на областния управител в хода на операцията за поставяне на специфични задачи или при промяна на ситуацията с разпореждания.

Този етап периодично диагностицира решението и валидира разработения план за операцията. Оценката се извършва по степента на изпълнение на определените дейности, тяхната ефективност и измененията, които настъпват с последствията от събитието. Въз основа на резултатите от тази диагностика, планът може да се адаптира за постигане на окончателните крайни цели, поставени с операцията [10].

Преход. Деескалацията на кризата изисква в посткризистния период управлението на операцията да се предаде на други органи на местна власт, ръководители на нестопански организации и фирми. Постигнатите цели и крайно състояние осигуряват ниския риск и стабилност в района. Експертите трябва периодично да наблюдават показателите в зоната на бедствието и да възпрепятстват следваща ескалация. В този етап се извършва оценката на човешките загуби и загубите на материални средства, координират се действията по установяване на правен ред, охраната на обектите, здравеопазване, хигиена и регулирането на бежанските потоци. При необходимост се осъществяват и координационни отношения с ЕС и други международни институции за оказване на помощ във възстановителните процеси.

Заключение:

Моделът за управление на операция за реагиране при криза, възникнала вследствие на бедствие или авария, осигурява обективна прогноза за развитието на кризата и способностите на силите и средствата за достигане на крайни устойчиви резултати, определя варианти за овладяване и разрешаване на кризата. Те се съдържат в условията за постигане на успех, граничните способности на наличните сили, възможностите на инфраструктурата да обслужва операцията, способностите на системата за управление да ръководи и транслира сигнали и възможностите на националната система да взаимодейства и да поддържа операцията.

Благодарности

Този доклад е подкрепен по Проект № РД-08-144/08.02.2016 г. “Ситуационен център за управление на кризи и реагиране при бедствия ”, финансиран от ШУ „Епископ Константин Преславски“.

Литература:

1. Закон за защита при бедствия, изм. ДВ. бр.81 / 20.10.2015.
2. Закон за администрацията, изм. ДВ. бр.27/25.03.2014.
3. Закон за опазване на околната среда, изм. ДВ. бр.101 / 22.12.2015.
4. Инструкция № 8121з-953 за условията и реда за осъществяване на химическа, биологическа и радиационна защита при пожари, бедствия и извънредни ситуации, изм. ДВ. бр.104 / 16.12.2014.
5. Национален доклад за състоянието и опазването на околната среда. София, 2015.
6. Национален аварийен план за борба с нефтени разливи в Черно море. МС София, 2011, Приложение № 10.
7. Национален план за защита при бедствия, МС София, 2010.
8. Национална програма за защита при бедствия 2014 – 2018. МС София, 2013.
9. Ръководство за класифициране на предприятия и съоръжения. <http://www.chemicals.moew.government.bg/chemical/site/File/manuals/Classification_guidance.pdf> (03.02.2016).
10. Сандев, Г. Лекции по Гражданска защита. Шумен, 2014.

КООРДИНАЦИЯ, ВЗАИМОДЕЙСТВИЕ И СЪТРУДНИЧЕСТВО ПРИ ПРЕОДОЛЯВАНЕ НА КРИЗИ, ПОРОДЕНИ ОТ БЕДСТВИЯ И АВАРИИ

Христо А. Христов

*Шуменски Университет „Епископ Константин Преславски”, Шумен
Факултет по технически науки
e-mail: hristov63@abv.bg*

COORDINATION, INTERACTION AND COLLABORATION IN THE PERIOD OF OVERCOMING CRISES ENGENDERED BY DISASTERS AND ACCIDENTS

Hristo A. Hristov

ABSTRACT: *Crisis management is a difficult process with many components that are the basis of achieving more efficiency in coordination and interrelation among authorities of the administrative apparatus of the country incises. In order to coordinate and interrelate effectively defining priorities is the main process task because of the evolving mechanisms that favorably influence on effectiveness of the coordination and interrelation under conditions of crisis.*

KEY WORDS: *Governor, Risk assessment, operational center, Regional Directorate of the Interior Ministry, Regional Directorate „Fire Safety and Population Protection”, Ministry of Defense*

Въведение

Прилаганите процедури, материална, комуникационна, информационна база, държавните органи, които ги осигуряват и използват, както и силите и ресурсите, формират механизъм за управление при кризи. Ефективността на механизма зависи от организацията за провеждане на незабавен и непрекъснат процес на координиране и взаимодействие, както между компетентните държавни ведомства, органите и силите за реагиране така и с ЕС, ООН и нейните агенции, ОССЕ и с отделни държави.

Дейността по организиране на координацията и взаимодействието в условията на кризи в настоящия момент е затруднена, поради все още липсващата пълна законова регламентация на дейността на ведомствата и органите в условията на кризи. Проблемите са много, но те биха могли да се решат единствено при ясна и точна координация между всички структури, които са елемент от Националната система за управление при кризи. Основните изпълнители са централните и териториални органи на изпълнителната власт, председателите на държавните агенции, държавните комисии, изпълнителните директори на изпълнителните агенции, ръководителите на държавни институции, създадени със закон или с постановление на Министерския съвет, които имат функции във връзка с осъществяването на изпълнителната власт. Във всички случаи при планирането и прилагането на спе-

циални мерки за реагиране при кризи решаваща роля и място имат оперативните центрове на ГДПБЗН на МВР, които координират дейността на основата на стандартни оперативни процедури. Спазването на законоустановения механизъм на управление трябва да гарантира принципа за получаване на изпреварваща информация в реално време и в еднакъв обем [10].

Изложение

Управлението при кризи е сложен процес с много компоненти, които са в основата за постигане на по-голяма ефективност в координацията и взаимодействието на органите в условията на кризи. Дефиниране на приоритетите за осъществяване на ефективна координация и взаимодействие и на тяхна основа, извеждане на механизмите, които оказват благоприятно влияние върху ефективността на координацията и взаимодействието в условията на кризи.

Координацията и взаимодействието, като термини, отразяващи единодействието на сложните социални системи, отразяват една важна управленска функция, чието значение расте екстремално с повишаването на управленското ниво. Те са основна функция, която се реализира на всички етапи от управленския цикъл.

Координацията, най-общо предполага предварителна договореност, изразяваща се най-често като принципна правна регламентация по определени стратегически въпроси, свързани с координацията: предметът ѝ; принципите; водещият орган в процеса; системността; договореността по формите; управлението и др.

Необходимостта от координация е обусловена от общността на целите, които стоят пред държавните органи – ефективно гарантиране на сигурността. Тя представлява предварително съгласуван ред между елементите в която и да е система. Тази съгласуваност се постига за сметка на подреждането в система, а това е главният ѝ признак, отличаващ я от взаимодействието.

Друго важно изискване при извършване на координацията и взаимодействието е пълното разкриване на системата от органи (държавни, обществени, отделни лица), между които трябва да се реализира взаимодействието за възможно най-пълно постигане на целите. Описването на тази система е сложен процес, тъй като тя има йерархична структура и различни подсистеми. Това означава, че за осъществяване на координацията и взаимодействието трябва да се вземе решение относно изграждането на специализирана организационна структура (звено), която ще планира, ръководи и отчита резултатите; кои ще бъдат формите на взаимодействие; какви документи ще се разработват за регламентиране на координацията и взаимодействието и т.н [3].

В теорията на социалното управление някои автори разглеждат координацията като управленска функция. „Съгласуване и установяване на целесъобразно съотношение в действията на различни органи и техните структурни подразделения за постигане на определена цел с най-малко загуби на сили и средства”.

Други автори разглеждат координацията като метод за управление на многостепенни и многоцелови системи, чиято същност е изработването и вземането на управленски решения. „Координацията се свежда до приемане на съответни решения от подсистемата за управление”, която е длъжна така да въздейства на относително самостоятелните нискостоящи подсистеми, че да бъде постигната целта, поставена пред цялата система”, в нашия случай – гарантиране на сигурността на обществото [10].

Основавайки се на анализа на горните схващания за координацията и приемайки, че тя е общоуправленска функция, проявяваща се при всички останали функции от управленския цикъл, можем обобщим, че координацията е съгласуване (установяване и поддържане) на действията на елементите на системата с цел поддържане на състояние на равновесие, чрез което по-ефективно да се постигнат поставените задачи, отнасящи се до сигурността.

Координацията, като дейност се свързва главно с управленската дейност, осигуряваща съгласуваността на практическото изпълнение. Тя може да се разглежда и като правомощие, според което на правото на координиращия орган съответства определено задължение на друг компетентен държавен, съдебен или орган на местното самоуправление и местната администрация за предприемане на необходимите действия. Като метод на управление, координацията може да се прилага и при прогнозирането, планирането, решаването, провеждането, отчета и контрола като съвкупност от функции, съставляващи дейността на органите на службите за сигурност и службите за обществен ред, за защита на националната сигурност и опазването на обществения ред.

Координацията се проявява по различен начин в зависимост от вида, обхвата и целите на системата и характера на нейното управление. В теорията на социалното управление, според характера на отношенията между координиращия и координираните органи, се различават множество модели на координация. Като отчитаме неопределеността и високия риск на кризите от невоенен характер, приемаме за основни вертикалния и хоризонталния модели на координация.

Вертикалната координация се осъществява в отношенията на висшестоящия орган с подчинените му органи на управление. При нея на практика се извършва съгласуване на интересите на отделния елемент (службата, отдела) или орган, с общите за организацията (операцията). Вертикалната координация подпомага и съдейства за реализиране на цялостната функция по управление на системата, като посредством нея се осъществяват единство и съгласуваност на действията по йерархичен път, който е характерен за този вид операции.

Хоризонталната координация се изразява основно под формата на съгласуване на действията между отделните звена и техните органи при осъществяване на съвместните дейности по изпълнение на планираните мероприятия. В практиката тя се изразява в планирането, организирането и провеждането на съвместните мероприятия, съгласуване на действията при провеждане операциите.

В теорията и практиката съществуват и други форми на координация: линейно-функционална, програмно-целева и консултативна. Общото и в трите форми на координация е, че те се прилагат в дейността на различаващи се по структура и компетенция органи, които като субекти на координацията имат собствена организационна и функционална обособеност, определеност и самостоятелност в дейността си, насочена към постигане на общата цел [10].

От тях съществено внимание следва да отделим на програмно-целевата форма на координация. Тя има ефект при съвместни програми и планове, които координират дейността на няколко структури по отделни направления на дейност, а също при създаване на целеви групи за постигане на общи цели – комплексно изпълнение на приоритетни или актуални задачи, свързани със защитата при бедствия, аварии и катастрофи. Прилагането на тази форма се определя от обективните потребности на обществото в условията на криза. При противодействието на посега-

телствата върху сигурността на страната, в условията на нарастващо напрежение, неяснота и бързопроменяща се обстановка, които изискват координираните усилия на всички национални, териториални и локални органи и служби. Такава форма на координация се осъществява на основата на стратегии и програми и е особено наложителна, когато се окаже изправени пред възникнала опасност за сигурността и обществения ред при природни бедствия, производствени аварии, земетресения и др., т.е. когато възникне необходимост от съвместни действия.

Координационни отношения се създават не само между отделните изпълнители, но и между различните подразделения на един и същ субект на управление. Когато управленските процеси и отношения в системата са между равнопоставени, те имат характер на „хоризонтални“ отношения, а когато са между неравнопоставени, са „вертикални“ отношения.

Координацията по своята функционална същност е определянето на реда между отделните елементи в системата, като самостоятелни социални подсистеми за реагиране на заплахите. Разглеждана като система, координацията се изгражда от няколко основни елемента: наличие на цел, диференцираща и интегрираща различните елементи от системата и процесът на внасяне на ред;

Разглеждана като процес, координацията винаги е дейност, отнасяща се до участие на съизпълнители, която се основава на обективни връзки и се реализира от субекта, който има властови функции. Разположеният най-високо в йерархическата стълбца субект на управление решава кога, в какви случаи и в какъв обем да се намеси в дейността на изпълнителите от структурите за сигурност и обществен ред.

В зависимост от целите за постигане, координацията се класифицира на два основни вида – предварителна и текуща. В общия смисъл тя се явява съгласуване на действията на изпълнителите в лицето на отделните структурни единици по време, място, цели и задачи и се осъществява от управляващите органи, като се базира и съобразява с инициативите на изпълнителите. Когато координацията е планово организирана, тя предполага съгласувателни мерки по предмет, принципи, водещ орган, договореност по формите на координация, управление и комуникационни връзки.

В съвременните условия в операциите от невоенен характер се осъществяват координационни отношения между силите за реагиране, включващи структури на различни министерства и ведомства. В ЗЗБ ясно са очертани основните сили за извършване на СНАВР и отговорникът за координацията, като е заложен вертикалният (йерархичният) модел на координация между участниците [1]. Координацията се провежда по планово-договорна форма чрез разработени стандартни оперативни процедури. Тяхното съдържание се отнася за провеждане на СНАВР и е продукт на процесите на предварително планиране. В процеса на провеждане на операцията и изпълнение на задачите възниква и необходимост от текущо координиране, иницирано от внезапно настъпили промени в обстановката или недостиг на ресурси (време, техника, личен състав или материални средства). Целесъобразно е тази дейност да се насочи към кризисния щаб и чрез прилагане на програмно целеви подход да се поддържа в необходимата актуалност. В съдържанието на тази координация трябва да се включат мерки за осъществяване на взаимодействие и с допълнителните сили и средства, привечдани в действие по искане на областния

управител или кметове. Резултатите от координационната дейност е целесъобразно да се разработят в текстуален вид и времеви график.

Между координацията и взаимодействието съществува динамична взаимовръзка, поради което в практиката двете понятия често се употребяват еднозначно. Трябва да се посочи, че координацията служи за основа на взаимодействието, а взаимодействието от своя страна е следствие на координацията. Като основни форми на взаимодействие могат да се посочат: взаимен обмен на информация; провеждане на съвместни мероприятия и операции; взаимодействие с оперативни сили и средства.

В основата на координацията и взаимодействието се застъпват принципи, които трябва да се спазват за постигане на общите цели. Към тях се отнасят:

- определяне и разграничаване на компетенциите на всеки субект, участващ в координацията и взаимодействието;
- необходимост от главно свързващо звено (кризисен щаб) или оторизиран представител на място (ГДПБЗН), към което да текат информационни потоци и йерархичната координация на всеки друг орган с него;
- съгласуване на частни планове и мероприятия при ясно определяне на възможностите на другите субекти за координация и взаимодействие;
- определяне на границите на организационна и тактическа самостоятелност на органите и участниците;
- самостоятелно делегиране на права за действия по избора на средства;
- постоянно осъществяване на контрол за паралелното етапно изпълнение на задачите в рамките на координацията.

Проблемът с координацията възниква при обединяването на усилията по преодоляване на кризата и има юридически аспект. Като се анализират детайлно и правните страни на проблема с координирането на операцията, е рационално да се приеме и тезата, че актът за прилагане на управленското решение е акт на управленско въздействие върху управляваните обекти, което по принцип е административен акт. За да бъде това действие законосъобразно, той следва да е издаден от овластен ръководител или орган, т.е. координацията на място трябва да е в съответствие с правните норми в държавата. Следователно ръководителят на място при провеждане на спасителни и неотложни аварийно-възстановителни работи се овластява с право да прилага координиращи мерки, като:

- забрани или ограничи влизането на лица в мястото на намеса;
- нареди временно извеждане на лица от мястото на намеса;
- разпорежи незабавно извършване и спиране на строежи, строителни работи, теренни преустройства или събаряне на сгради и съоръжения или части от тях с цел намаляване или отстраняване на рисковете от възникнало бедствие;
- поиска от юридически или физически лица предоставяне на лична или материална помощ;
- създаде временен оперативен щаб на ръководителя на място с представители на участващите екипи от единната спасителна система;
- раздели мястото на намеса на сектори или на участъци, да определи техни ръководители, да им възлага задачи, както и да разпределя сили и средства за тях.

Според критерия за организационно изграждане на структурите, координацията и взаимодействието могат да се разглеждат като два основни вида – вътрешно и

външно. Методът за неговото организиране се определя в зависимост от задачата, обстановката и най-вече от разполагаемото време.

Вътрешна координация и взаимодействие е съгласуваност, която се осъществява в границите и рамките на всяка отделна структура (система), пряко ангажирана с участие в операцията. Обикновено тя е предварително планирана, осигурена със съответните материални средства и съобразена с основните участници в действията. Това произтича от участието на ръководителя на структурата в подготовката на операцията, от ученията и тренировките, които са провеждани с екипите.

Външната координация и взаимодействие включват съгласувани действия между териториалните органи на МВР, МО, МЗ, агенции и др., независимо от това в кой етап от операцията участват и дали имат пряко подчинени структури. Тяхното включване е в отговор на стремежа за по-ефективно въздействие върху кризата и е целесъобразно те да се организират по видове операции. Те обхващат и връзките между общинските и областни щабове, както и тези на национално ниво.

В район на силно земетресение, ръководителят е длъжен да съгласува реда за придвижване на разузнавателните формирования, силите с общо и специално предназначение и действията им в зоната на бедствено положение; реда за преодоляване на зоните на разрушения, пожари и заразяване; дейността на силите по взаимното осигуряване подхода към местата за работа, устройване на проходи в затрупванията, разкриване на затрупани хора и извличане на поразените; в кои медицински учреждения да бъдат евакуирани пострадалите и т.н. Наред с това се организира взаимодействието с органите на централната власт (министерства и ведомства) за решаване на въпросите по настаняване, изхранване, обличане и медицинско обслужване на пострадалото население; лечението на пострадалите; борбата с мародерството; материално-техническото осигуряване на силите, извършващи СНАВР и редица други въпроси [8].

При хуманитарна операция взаимодействието се организира с цел да се осигури оцеляването на хората. От съществено значение е координацията с обединените граждански и военни елементи, действащи заедно или като национални гости и международни хуманитарни организации. При такива ситуации могат да се използват възможностите на специалисти в медицинското и инженерното осигуряване. Възможно е главният координатор на външната подкрепа за такива мисии да бъде от международна гражданска организация като Департамента по хуманитарните въпроси към ООН или Върховния комисариат на ООН за бежанците [4].

Взаимодействие може да се организира и по основните способности на отделните участници в преодоляването на кризата. Формированията от МВР съгласуват: охраната на държавните граници, промишлени, енергийни, свързочни и други важни обекти на територията на страната; издирването и залавянето на нарушителите, осигуряването на безопасността на движението и охраната на уязвими участъци по магистралите, пътищата и маршрутите за изнасяне на участниците; осигуряване на противопожарна защита и материални ресурси; охрана на стопански обекти, охрана на местата за подслон на евакуираните, мероприятия по защита на националното стопанство от диверсии и посегателства.

С министерството на транспорта и съобщенията се уточняват въпросите по техническото прикритие на транспортните комуникации, подготовката на транспортната система на страната и заявките за превоз на тежка техника. По линията на съобщенията се съгласуват трасетата на магистралните проводни линии и обектите

от националната свързочна система, строежът на нови обекти и възстановяването на обекти от съобщенията.

Заклучение:

Република България, като страна членка на ЕС, осъществява координация в съответствие със стратегическите цели и приоритети. Тя се реализира в рамките, определени от националното законодателство и международните договори, по които Република България е страна.

Международната дейност се реализира чрез комплекс от мерки в следните основни направления: Сътрудничество по линия на ЕС; Сътрудничество по линия на НАТО; Регионално сътрудничество; Двустранно сътрудничество.

Координацията и взаимодействието са главно условие за оптимизиране на дейността чрез съсредоточаване на сили и средства по определени направления и в определено време. За да се използват наличните възможности за изпълнение на задачите, които се предоставят от координацията и взаимодействието, е важно те да бъдат своевременно осъществени.

Благодарности

Този доклад е подкрепен по Проект № РД-08-144/08.02.2016 г. “Ситуационен център за управление на кризи и реагиране при бедствия”, финансиран от ШУ „Епископ Константин Преславски“.

Литература:

1. Закон за защита при бедствия, изм. ДВ. бр.81 / 20.10.2015.
2. Закон за администрацията, изм. ДВ. бр.27/25.03.2014.
3. Закон за опазване на околната среда, изм. ДВ. бр.101 / 22.12.2015.
4. Инструкция № 8121з-953 за условията и реда за осъществяване на химическа, биологическа и радиационна защита при пожари, бедствия и извънредни ситуации, изм. ДВ. бр.104 / 16.12.2014.
5. Национален доклад за състоянието и опазването на околната среда. София, 2015.
6. Национален аварийен план за борба с нефтени разливи в Черно море. МС София, 2011, Приложение № 10.
7. Национален план за защита при бедствия, МС София, 2010.
8. Национална програма за защита при бедствия 2014 – 2018. МС София, 2013.
9. Ръководство за класифициране на предприятия и съоръжения. <http://www.chemicals.moew.government.bg/chemical/site/File/manuals/Classification_guidance.pdf> (03.02.2016).
10. Сандев, Г. Лекции по Гражданска защита. Шумен, 2014.
11. Стратегия за национална сигурност на Република България, МС София, 2011.

ИНФОРМАЦИОННА СИГУРНОСТ

ОДИТ НА СИГУРНОСТТА НА ИНФОРМАЦИОННИ СИСТЕМИ, СВЪРЗАНИ С ИНТЕРНЕТ

Веселин Ц. Целков¹, Орхан А. Исмаилов², Мая Г. Божилова³

¹Комисия за защита на личните данни
София, 1592, бул. „Професор Цветан Лазаров” № 2

²Министерство на отбраната на Р. България
София, 1000, ул. „Дякон Игнатий” № 3

³Институт по отбрана “Професор Цветан Лазаров”
София, 1592, бул. „Професор Цветан Лазаров” № 2

SECURITY AUDIT OF INTERNET CONNECTED INFORMATION SYSTEMS

Veselin Ts. Tselkov, Orhan A. Ismailov, Maya G. Bozhilova

ABSTRACT: *Information System is an asset for organizations and should be well managed, protected and controlled. This paper presents an approach for information systems auditing. Based on international best practices and standards the questionnaire for evaluation of security of information systems is defined.*

KEY WORDS: *Information systems security, Information systems audit, Data protection, Internet security*

1. ВЪВЕДЕНИЕ

Информационната система е множество от човешки и капиталови ресурси, инвестирани в дадена организация, с цел събиране и обработване на данни, за да се получи информация, която да се използва при вземане на решение на всички управленски нива и при контролиране на дейностите в организацията [2]. Одитът е систематичен процес [3, 1] на оценяване и получаване на доказателства за дейности, събития или транзакции. В момента, одитните практики се развиват с бързи темпове в резултат на развитието на информационните технологии и одитът на информационните системи се фокусира основно върху оценката на правилното прилагане, управление и контрол на информационни системи и ресурси в рамките на организацията.

За извършване на преглед на сигурността на информационните системи, работещи в средата на Интернет е необходимо да бъдат извършени последователно следните действия:

- Дефиниране на изискванията за сигурност;
- Въпросник за преглед на сигурността на информационните системи, работещи в средата на Интернет;
- Отговор на въпросите от въпросника;
- Анализ и обобщаване на резултатите;
- Изводи и препоръки за подобряване на сигурността на публичните информационни системи.

2. ДЕФИНИРАНЕ НА ИЗИСКВАНИЯТА ЗА СИГУРНОСТ

Основните елементи при дефинирането на изискванията за сигурност включват основните стандарти за сигурност, които могат да бъдат използвани за систематична оценка, механизмите за идентификация на уязвимостите на активите (персонал, хардуер, софтуер, информация), автоматизирани процедури и процеси, свързани с дадената ИТ система, в следните области за сигурност:

- Управление на сигурността;
- Сигурност при експлоатацията (използването);
- Техническа сигурност.

2.1. Управление на сигурността

Управлението на сигурността включва:

- Назначение (разпределение) на отговорностите;
- Непрекъснатост на поддръжката;
- Способности за отговор (реакция) на инцидентите;
- Периодичен преглед на контролите за сигурност;
- Персонална сигурност и проучване;
- Оценка на сигурността;
- Обучение и тренировки за сигурност и използване на системата;
- Разделяне на отговорностите;
- Системно упълномощаване и преупълномощаване;
- План за сигурност на системно и приложно ниво.

2.2. Сигурност при експлоатацията (използването)

Тази област обхваща:

- Контрол на съдържанието на въздуха (дим, прах, химикали);
- Контроли за гарантиране на качеството на електрическото захранване;
- Достъп до носителите на данни и освобождаване;
- Външно разпределение на данни и етиктиране;
- Защита на съоръженията:
 - Център за данни;
 - Компютърните стаи;
 - Офисите;
- Контрол на влажността;
- Контрол на температурата;
- Компютри:
 - Сървъри;
 - Работни станции;
 - Преносими компютри.

2.3. Техническа сигурност

В техническата сигурност се включват:

- Комуникации;
- Криптография;
- Контрол на достъпа;
- Идентификация и автентификация;
- Откриване на нарушения;
- Системно наблюдение.

3. БАЗОВ ВЪПРОСНИК ЗА ПРЕГЛЕД НА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ СИСТЕМИ, РАБОТЕЩИ В СРЕДАТА НА ИНТЕРНЕТ

Въпросите свързани с прегледа на сигурността на информационните системи са базирани на добрите практики от стандартите на ISO и са разделени в десет основни направления, както следва:

- Политика за сигурност;
- Организационна сигурност;
- Класификация на активите и контролите;
- Сигурност на персонала;
- Физическа сигурност;
- Комуникации и оперативно управление;
- Контрол на достъпа;
- Разработка и поддръжка на системата;
- Управление непрекъсваемостта на бизнеса;
- Съответствие.

Представяне на компонентите

1. Политика за сигурност

Политика за информационна сигурност

1. Съществува ли документ за политика за информационната сигурност, който да е одобрен от ръководството, публикуван и съобщен на всички служители в касаещия ги обем, независимо дали политиката става ангажимент за тези служители ?

2. Дали е определен отговорник за преглед и оценка на политиката за информационна сигурност ?

3. Процесът гарантира ли преглед на политиката при евентуални промени, засягащи оценката на информационната сигурност? Напр.: Значителен инцидент със сигурността, нови уязвимости, промяна в организационната или техническата инфраструктура и др.

2. Организационна сигурност

Въпросите, свързани с организационната сигурност са групирани в три групи:

- Инфраструктура на информационната сигурност;
- Сигурност на достъпа на трети страни;
- Аутсорсинг (външни услуги).

Инфраструктура на информационната сигурност

4. Създаден ли е борд за управление за информационната сигурност?
5. Съществува ли система за координация на информационната сигурност в организацията?
6. Ясно и точно ли са разпределени отговорностите по информационната сигурност?
7. Съществува ли процес на разрешение относно ново оборудване?
8. Ползват ли се съвети на специалисти по информационна сигурност?
9. Съществува ли сътрудничество между организации (правоохранителни, регулаторни, и др.)?
10. Извършва ли се редовно независима проверка на сигурността на информацията?

Сигурност на достъпа на трети страни

11. Направена ли е идентификация на рисковете от достъпа на трети страни?
12. Дефинирани ли са изисквания за сигурността при договори с трети страни?

Аутсорсинг (външни услуги)

13. Дефинирани ли са изисквания за сигурността при договори за аутсорсинг (външни услуги)?

3. Класификация на активите и контролите

Класификацията на активите и контролите обхваща групите;

- Отчетност на активите;
- Класификация на информацията.

Отчетност на активите

14. Извършва ли се редовно инвентаризация на активите?

Класификация на информацията

15. Създадени ли са ръководства за класифициране на информацията?
16. Съществува ли набор от процедури за начините за етиктиране и обработка на информацията?

4. Сигурност на персонала

Сигурността на персонала обхваща;

- Сигурност при дефиниране на работата;
- Обучение на потребителите;
- Отговор на инциденти със сигурността и неизправности на оборудването.

Сигурност при дефиниране на работата

17. Включват ли се отговорности по сигурността в работата на персонала?
18. Осъществява ли се скрийнинг (предварителна проверка, наблюдение и др.) на персонала?
19. Сключват ли се споразумения за поверителност?

20. Съществуват ли допълнителни условия за работа в аспекта сигурност на информацията?

Обучение на потребителите

21. Извършва ли се обучение по сигурност на информацията?

Отговор на инциденти със сигурността и неизправности на оборудването

22. Съществува ли процедура за докладване на инциденти по сигурността?

23. Съществува ли процедура за докладване на слабости в сигурността?

24. Съществува ли процедура за докладване на софтуерни неизправности?

25. Съществува ли механизъм за създаване на изводи от инциденти?

26. Има ли наличен процес за дисциплиниране на потребителите?

5. Физическа сигурност

Въпросите се групират както следва:

- Охранявана зона (зони за сигурност);
- Сигурност на оборудването;
- Общ контрол.

Охранявана зона (зони за сигурност)

27. Има ли физическа сигурност на периметъра?

28. Съществува ли контрол на физическия достъп?

29. Има ли защита на офиси, стаи и съоръжения?

30. Извършва ли се работа в защитени зони?

31. Съществува ли изолиране на зоните за доставки и областите за зареждане?

Сигурност на оборудването

32. Има ли точно определено място за разполагане на оборудването?

33. Защитени ли са захранващите системи (UPS, генератори и др.)?

34. Съществува ли процедура за сигурност на кабелните системи?

35. Поддръжката извършва ли се по определена процедура?

36. Съществува ли процедура за защита на оборудването извън периметъра?

37. Дефинирани ли са мерки за спазване на сигурността при повторно използване на оборудване?

Общ контрол

38. Изградена ли е политика за “чисто бюро и чист екран”?

39. Възможно ли е да се приема отвън оборудване, информация или софтуер без съответното разрешение?

6. Комуникации и оперативното управление

Въпросите свързани с комуникациите и оперативното управление са групирани в четиринадесет групи:

- Оперативни процедури и отговорности;
- Система за планиране и одобрение;
- Защита от зловреден софтуер;
- Поддръжка на информацията;

- Управление на мрежите;
- Сигурност на устройствата за съхранение на информация;
- Обмен на информация и софтуер;
- Оперативни процедури и отговорности;
- Система за планиране и одобрение;
- Защита от зловреден софтуер;
- Поддръжка на информацията;
- Управление на мрежите;
- Сигурност на устройствата за съхранение на информация;
- Обмен на информация и софтуер.

Оперативни процедури и отговорности

40. Документират ли се оперативните процедури?
41. Изградена ли е система за оперативен контрол на промените?
42. Въведени ли са процедури за управление на инциденти?
43. Извършено ли е разпределение на задълженията?
44. Разделени ли са съоръженията за разработване и за реална експлоатация?
45. Съществува ли управление от трета страна на съоръжения и оборудване, обработващо информация на организацията?

Система за планиране и одобрение

46. Извършва ли се планиране на капацитетите?
47. Има ли система за одобрение?

Защита от зловреден софтуер

48. Въведени ли са контроли срещу зловреден софтуер?

Поддръжка на информацията

49. Поддържа ли се система за архивиране на информацията?
50. Водят ли се дневници на операторите?
51. Съществува ли водене на дневници на повредите?

Управление на мрежите

52. Въведени ли са контроли на мрежите?

Сигурност на устройствата за съхранение на информация

53. Съществува ли процедура за управление на преносимите носители на информация?
54. Създадена ли е система за унищожаване на носителите на информация?
55. Съществуват ли процедури за обработка на информация?
56. Защитена ли е системната документация?

Обмен на информация и софтуер

57. Има ли споразумения за обмен на информация и софтуер?
58. Дефинирана ли е процедура за защита на носителите на информация при транспортиране?
59. Съществува ли политика относно сигурността на електронната поща?

60. Съществува ли политика относно сигурността на електронните офис системи?

61. Съществува ли процес за одобрение при ползване на публично достъпни системи?

62. Има ли други форми за обмен на информация?

7. Контрол на достъпа

Обхваща следните групи:

- Бизнес изисквания за контрол на достъпа;
- Управление на потребителския достъп;
- Отговорности на потребителите;
- Контрол на мрежовия достъп;
- Контрол на достъпа до операционната система;
- Контрол на достъпа до приложенията;
- Наблюдение на достъпа и използването на системите;
- Мобилни компютърни устройства и работа от разстояние.

Бизнес изисквания за контрол на достъпа

63. Дефинирана ли е политика за контрол на достъпа?

Управление на потребителския достъп

64. Извършва ли се регистрация на всеки потребител?

65. Извършва ли се управление на привилегиите?

66. Съществува ли процедура за управление на паролите на потребителите?

67. Съществува ли процес за преглед на правата за достъп на потребителите?

Отговорности на потребителите

68. Има ли ръководство за създаване и използване на „силна” парола?

69. Запознати ли са потребителите с правилата за защита на оставено оборудване без надзор?

Контрол на мрежовия достъп

70. Съществува ли политика за използване на мрежови услуги?

71. Има ли контроли относно строго спазване на пътищата (рутиране между услуги и терминали)?

72. Има ли механизъм за автентификация на потребителите при външни услуги?

73. Автентифицират ли се връзките до отдалечени компютърни системи, външни за организацията?

74. Има ли използван механизъм за отдалечена проверка за диагностициране и защитата на портове?

75. Мрежите за достъп на трети страни разделени ли са с периметрови механизми за защита и сигурност, напр. защитни стени?

76. Съществува ли контрол на споделените мрежови връзки, които се простират извън организацията. Съществува ли контрол на мрежовото маршрутизиране?

77. При използването на публични или частни мрежови услуги, гарантира ли се ясно и точно използването на еднозначни механизми и атрибути за сигурност на мрежата?

Контрол на достъпа до операционната система

78. Използва ли се автоматична идентификация на терминала?

79. Съществува ли процедура за вход (log-on) в терминала?

80. Извършва ли се еднозначна идентификация и автентификация на потребителите?

81. Съществува ли система за управление на паролите?

82. Контролира ли се използването на системен и помощен софтуер?

83. Съществуват ли принудителни аларми (паник-бутони) за защита на потребителите?

84. Дефинирано ли е време за изчакване на терминала?

85. Съществува ли ограничаване на времето на свързаност?

Контрол на достъпа до приложенията

86. Има ли механизми за ограничаване на достъпа до информация?

87. Извършва ли се изолация на чувствителните системи?

Наблюдение на достъпа и използването на системите

88. Извършват ли се записи на събития?

89. Създадени ли са процедури за контрол на използването на информационните ресурси?

90. Извършва ли се синхронизация на времето?

Мобилни компютърни устройства и работа от разстояние

91. Съществува ли политика относно използването на мобилни компютърни устройства?

92. Има ли процедура за отдалечена работа?

8. Разработка и поддръжка на системата

В частта разработка и поддръжка на системата са специфицирани групите:

- Изисквания за сигурността на системите;
- Сигурност на приложните системи;
- Криптографски контроли;
- Защита на системните файлове;
- Сигурност и защита в процеса на разработване и поддръжка.

Изисквания за сигурността на системите

93. Дефинирани ли са изисквания за сигурността при анализа и специфициране на системата?

Сигурност на приложните системи

94. Извършва ли се проверка на входните данни?

95. Съществува ли контрол на вътрешната обработка?

96. Прилагат ли се контролни суми (хеш)?

97. Извършва ли се валидация на изходните данни?

Криптографски контроли

98. Има ли политика за използване на криптографски контроли?
99. Извършва ли се криптиране?
100. Използва ли се цифров подпис?
101. Въведени ли са услуги, свързани с невъзможност за отказ от авторство?
102. Съществува ли система за управление на криптографските ключове?

Защита на системните файлове

103. Съществуват ли контроли по отношение на системния софтуер?
104. Защитават и контролират ли се тестовите данни за системата?
105. Въведен ли е строг контрол на достъпа до изходния код на софтуерните библиотеки?

Сигурност и защита в процеса на разработване и поддръжка

106. Съществува ли процес за промяна на процедурите за контрол?
107. Съществува ли процес или процедура за тестване и проверка на приложните системи след промяна на операционните системи?
108. Съществуват ли ограничения по отношение промяната на софтуерните пакети?
109. Съществува ли процедура за проверка за „задни вратички“ и „Троянски коне“?
110. Съществуват ли контроли за проверка на външно разработвания софтуер?

9. Управление непрекъсваемостта на бизнеса

Аспекти на управлението на непрекъсваемостта на бизнеса

111. Съществуват ли управляеми процеси относно развитието и поддръжката на непрекъсваемостта на бизнеса в организацията?
112. Идентифицирани ли са събитията, които могат да доведат до прекъсване на бизнес процесите?
113. Създаден ли е план за възстановяване на бизнес операциите в рамките на определен срок след прекъсване или отпадане на бизнес процеси?
114. Съществува ли единна структура на плана за осигуряване непрекъсваемостта на бизнеса?
115. Тества ли се периодично плана за осигуряване на непрекъсваемост на бизнеса ?

10. Съответствия

Одитът за съответствие обхваща въпроси от групите както следва:

- Съответствие със законовите изисквания;
- Преглед на политиката за сигурност и техническото ѝ съответствие;
- Елементи на системния одит.

Съответствие със законовите изисквания

116. Ясно ли са дефинирани и стриктно документираны всички закони, подзаконови, нормативни и договорни изисквания за всяка информационна система ?

117. Съществуват ли процедури за гарантиране спазването на законовите ограничения по отношение на правата върху интелектуалната собственост?

118. Защитени ли са важни записи на организацията от загуба, унищожаване или подмяна?

119. Съществува ли структура, отговорна за управлението и контрола на защита на личните данни и неприкосновеността на личната информация?

120. Съществува ли процедура за предотвратяване на злоупотреба от използването на съоръжения и оборудване за обработка на информация?

121. Извършва ли се на национално ниво регулацията на криптографските контроли?

122. Съществува ли процес за събиране на доказателства, съобразен с нормативните изисквания?

Преглед на политиката за сигурност и техническото ѝ съответствие

123. Извършва ли се преглед на всички процедури, контроли, системи и др. за съответствие с политиката за сигурност ?

124. Проверят ли се редовно информационните системи за съответствие с имплементираните стандарти за сигурност?

Елементи на системния одит

125. Изискванията за одит и контрол на дейности, свързани с операционни системи внимателно ли са планирани и съвпадат ли с изискванията за минимизиране на риска от прекъсване на бизнес процесите?

126. Защитен ли е достъпът до системни инструменти за одит (софтуер или файлове с данни)?

4. ЗАКЛЮЧЕНИЕ

Одитът на информационните системи, свързани с Интернет, оценява организационната и технологична архитектура и процеси, за да осигури, че информационните активи са защитени, надеждни, достъпни и съвместими с процедурите и политиката на организацията, както и с приложимите закони и регулации. Целта на одита е да намали рисковете за информационната сигурност. Предложеният въпросник е базиран на съществуващите международни добри практики и стандарти. Предстои въпросникът да се апробира и валидира, както и да се допълни чрез практическото му приложение.

ЛИТЕРАТУРА

1. Murphi, C., Information Systems Audit Report, Western Australian Auditor General's Report, Report 11, June 2013
2. Popescu G., V. Popescu, C. Popescu, Information Systems Security Audit, Manager Finance – Accountancy, No. 6, 2007
3. Rahman A, A.Al-Nemrat, D.S. Preston, Sustainability in information systems auditing, European Scientific Journal, September 2014 /SPECIAL/ edition Vol.3

ОБЛАЧНА СРЕДА НА КОМУНИКАЦИОННО-ИНФОРМАЦИОННА СТРУКТУРА ЗА МРЕЖОВО-ЦЕНТРИЧНИ ОПЕРАЦИИ

Александър А. Колев¹, Стефан Р. Маринов², Иван П. Иванов³

¹ Р. България, София 1592, бул. "Цв. Лазаров" № 2,
Институт по отбрана „Професор Цветан Лазаров”
Тел. +359 0221834, E-mail: a.kolev@di.mod.bg

² Р. България, София 1606, бул. "Тотлебен" № 34,
Министерство на отбраната

Тел. +359 022415, E-mail: stefik76@yahoo.com

³ Р. България, София 1592, бул. "Цв. Лазаров" № 2,
Институт по отбрана „Професор Цветан Лазаров”
Тел. +359 0221822, E-mail: i.p.ivanov@di.mod.bg

COMMUNICATION AND INFORMATION STRUCTURES IN CLOUD ENVIRONMENT FOR NETWORK-CENTRIC OPERATIONS

Alexander A. Kolev¹, Stefan R. Marinov², Ivan P. Ivanov³

ABSTRACT: With regard to the requirements of multiple data links cooperative combat in network-centric battle field, the article analyzes the problems and the challenges faced in network-centric warfare. The focus is on the idea that cloud computing services shall be set as basis of the networking data link system in this kind of battle field. A new (battlefield-oriented, demand-based, real-time serviced) networking data link system is introduced - the Joint Data Link system built on cloud computing. It is proved that the use of cloud technology in Joined Data Links can improve the system service level markedly. An approach for geographical localization of network hosts is appropriated.

KEY WORDS: network-centric warfare, cloud computing, joint data link system, geolocation.

ВЪВЕДЕНИЕ

В мрежово-центричната война тактическите линии за обмен на данни, като например *Link-4A*, *Link-10*, *Link-11*, *Link-16* и *Link-22* (средства за разпространяване на информация, обработена от радары, сонари, системи за държавно опознаване (свой-чужд), информацията, необходима за електронна борба, за докладване, получаване на команди и за визуално наблюдение) вече не могат да покрият изискванията за висококачествено мрежово предаване на данни в реално време и споделяне между множество възли[1]. Построяването на цялостни мрежови връзки за обмен на данни е с цел прилагане на многостранно военно сътрудничество и осигуряване на крайните потребители с пълна информация от бойното поле в реално време. Чрез цялостните мрежови връзки се укрепва бойното сътрудничество и синтезът на информация между различни връзки, за да се осигури точна информация за бойно-

то поле в реално време, която да удовлетворява изискванията за контрол при управление на огъня и за изпълняване на кооперативната кампания с различни оръжейни системи. Тя интегрира различни връзки за данни в затворена система, в която връзките за данни могат взаимно да се свързват и да си взаимодействат едни с други, като осигуряват висококачествена информация за бойното поле в реално време за мрежовоцентрична война при поискване.

Основната идея да се изгради обединена линия за предаване на данни, използваща облачен компютинг, е да се изработи прозрачна и отворена мрежова архитектура за собствените и приятелски сили. В тази архитектура, от една страна, разпределената обработка на данните се използва изцяло за подобряване на бойната ефективност и жизненост на мрежата. Усъвършенстването на приложният софтуер и хардуер позволява съвместимост с оригиналните тактически линии за данни и всички други комуникационни системи. От друга страна, определянето на стандартния интерфейс гарантира, че функциите на текущото оборудване няма да бъдат засегнати с разширяване на обединена линия за предаване на данни. По този начин взаимодействието на множество линии за данни в мрежовоцентричната война се осигурява чрез жизнестойчива и надеждна мрежа за далечен пренос на информация, която може да бъде разширявана според нуждите.

Обединените линии за предаване на данни се характеризират с голяма мащабност, различност в структурата на субвръзките, висока комплексност и висока степен на дистрибутивност.

Възможностите при изграждане на обединени линии за предаване на данни, базирани на облачен компютинг са:

а) Мащабни ресурси с различни структури могат да бъдат оптимизирани и интегрирани в обединена линия за предаване на данни.

б) Инфраструктурата на обединената линия за предаване на данни може да бъде управлявана автоматично.

в) Мащабни количества данни от бойното поле могат да се съхраняват надеждно в разпределени база от данни.

г) Информацията от бойното поле от множество линии за данни може да бъде управлявана ефективно.

д) Разпределеният компютинг и анализирането на обединените линии за предаване на данни може да се направи с висока скорост.

е) Възможността за разширяване и жизнеността на обединените линии за предаване на данни може да бъде подобрена.

АРХИТЕКТУРА НА ОБЕДИНЕНИТЕ ЛИНИИ ЗА ПРЕДАВАНЕ НА ДАННИ, БАЗИРАНИ НА ОБЛАЧЕН КОМПЮТИНГ

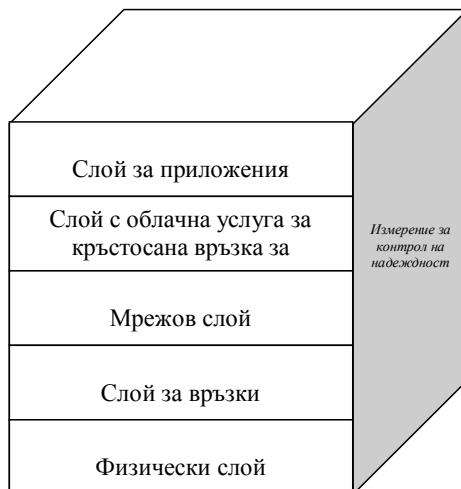
Обединените линии за предаване на данни са ядрото на комуникационната система в една мрежовоцентрична операция. Имайки предвид текущите характеристики на тактическите линии за данни и използваните технологии, правейки връзка с ТСР/IP модел, допълнително са добавени мрежов слой, слой с облачна услуга за кръстосана връзка за взаимодействие и измерение за контрол на надеждността върху трислойната архитектура за връзка на данните. Новата архитектура е изпълнена като мрежов модел, като слой с облачна услуга за кръстосана връзка за взаимодействие осигурява единни технологични стандарти. Това прави достъпни мре-

жови изчислителни функции, прави приложенията за бойното поле и услуги интелигентни.

Показаният на Фиг. 1 дизайн е архитектура на 5 нива, представляващи физически слой, слой за връзки, мрежов слой, слой с облачна услуга за кръстосана връзка за взаимодействие и слой с приложения[1].

1) Слой с приложения:

Този слой включва специфична колекция от приложения, които са



Фиг. 1: Архитектура на обединени линии за предаване на данни, базирани на облачен компютинг

необходими за изпълнение на някои специфични бойни задачи, като например приложения за въздушна отбрана, приложения за противоракетна отбрана, приложения за прецизно поразяване на големи разстояния и други тактически и стратегически бойни приложения. Този слой също така включва някои общи и специфични приложения, използващи тактически данни за конкретни мисии, като например мониторинг, управление на задачите на мисията, взаимодействие на оръжията, криптирано аудио и т.н.

2) Слой с облачна услуга за кръстосана връзка за взаимодействие

В сравнение с традиционната тактическа линия за данни, налице е нова услуга "Облачен компютинг", така че мрежата на обединените линии за предаване на данни сега има изчислителна мощ и възможности за споделяне на информация. В този слой, идеята за облачния компютинг служи за организиране и използване на физическата инфраструктура, прилагане на контрол и управление на виртуални ресурси. Състои се основно от капсулиране на виртуални бойни ресурси в облачни услуги и публикуването им, избиране на режим на разполагане на всеки от различните видове облачни услуги и осъществяване на интелектуално и ефективно управление на облачните услуги, динамично развърщане, управление на отказоустойчивост и др. Изброено на

последно място, но не и по важност е свойството за предоставяне на услугите в момент на необходимост за потребителите на бойното поле.

3) Мрежов слой

Според характеристиките на свързаността чрез маршрутизация на трафика на данни, може да се гарантира, че всяка част от информацията от бойното поле пристига в точното място и представя еднозначно и прозрачно реалната обстановка на бойното поле. Мрежовият слой трябва да отработва функции на пренос на данни, маршрутизация, контрол на грешките, контрол на претоварването, мрежово свързване и поддръжка. Той определя дали обединените линии за предаване на данни могат да бъдат дълбоко интегрирани в мрежовоцентрична война. Мрежовата свързаност, основана на протокола TCP/IP е особено важна за ефективността и общия характер на системата като цяло.

4) Слой за връзки

Осигурява пренос на данни от точка до точка с използване на TCP/IP протокол и установява линии за предаване на данни между комуникационните структури на базата на услугата за предаване на бит, предоставена от физическия слой. Този слой също така осъществява контрол за грешки и контрол за трафика, служи за диагностика и предотвратяване на потенциални прекъсвания във физическите връзки.

5) Физически слой

Този слой осигурява физическата връзка за слоя за връзки с физически носител.

6) Измерение за контрол на надеждността

В усложнена среда на бойно поле, когато обединените линии за предаване на данни, базирани на облачен компютинг, едностранно и прозрачно осигуряват приятелски потребители с индивидуализирани услуги, не може да има сигурност за надеждността на заявената услуга. Ето защо е необходимо да бъде добавен слой за контрол на надеждността в облачната архитектура. По-конкретно, контролът на надеждността трябва да включва група от атрибути: от гледна точка на потребителите, следва да се гарантира сигурността на услугите и жизнеността; от гледна точка на дизайна, трябва да се обезпечи управляемостта на системата.

Анализът на дискутираната облачна архитектура на обединените линии за предаване на данни показва, че командният състав на своите и приятелски сили разполага с мощен и надежден инструмент за предоставяне на точна информация за бойното поле в реално време, разширени възможности за контрол при управление на огъня и за водене на съвместни операции с различни оръжейни системи.

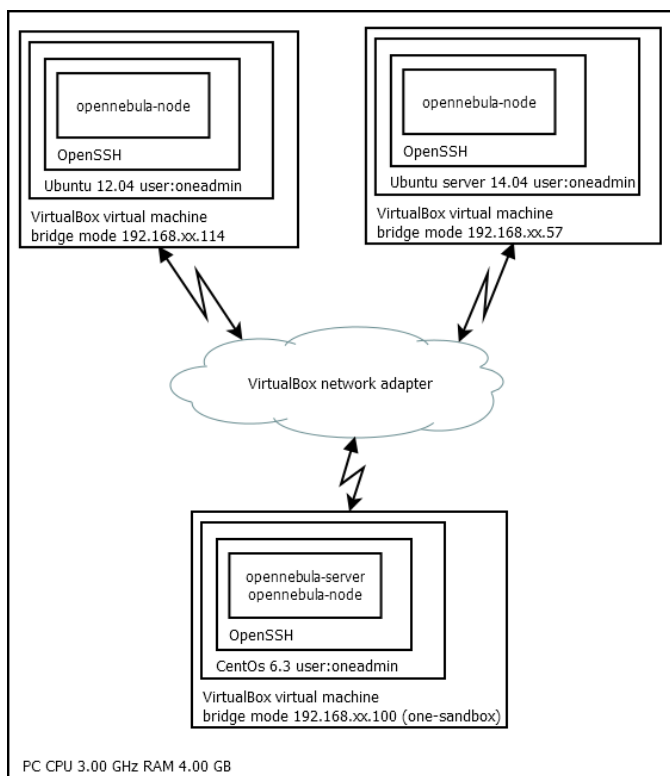
НЕОБХОДИМОСТ ОТ ГЕОГРАФСКА СВЪРЗАНОСТ В ОБЛАЧНАТА ИНФРАСТРУКТУРА

В общия случай крайният потребител на облачни услуги не се интересува от топологията и географската локализация на физически единици от инфраструктурата. Едно специфично приложение в сферата на логистиката за техническа поддръжка и диагностика на бойни летателни апарати при военно-въздушни действия е изграждането и поддръжката на високомобилни цифрови линии за данни. Съществуващата задача за осигуряване на устойчива цифрова радиовръзка борд-земя в

широк географски периметър е оперативно решаема при наличие на подходящ инструментариум за бързо инсталиране на специфични услуги на географски определени физически хостове. В тази връзка, авторите си поставят за цел изграждане на експериментална среда за апробиране на софтуерен подход, създаване или модифициране на система за управление на облачна архитектура за инсталиране на услуги на географски определени хостове.

Разгледани са системи за управление на облачна архитектура с отворен код. За основа на експерименталния процес е възприета системата с отворен код *OpenNebula v. 4.14.2* [2], като е ползвана преинсталирана версия тип *sandbox*, предоставяна на сайта на разработчиците.

На фиг. 2 е представена архитектура на изградената експериментална среда.



Фиг. 2. Архитектура на експериментална среда OpenNebula Sandbox

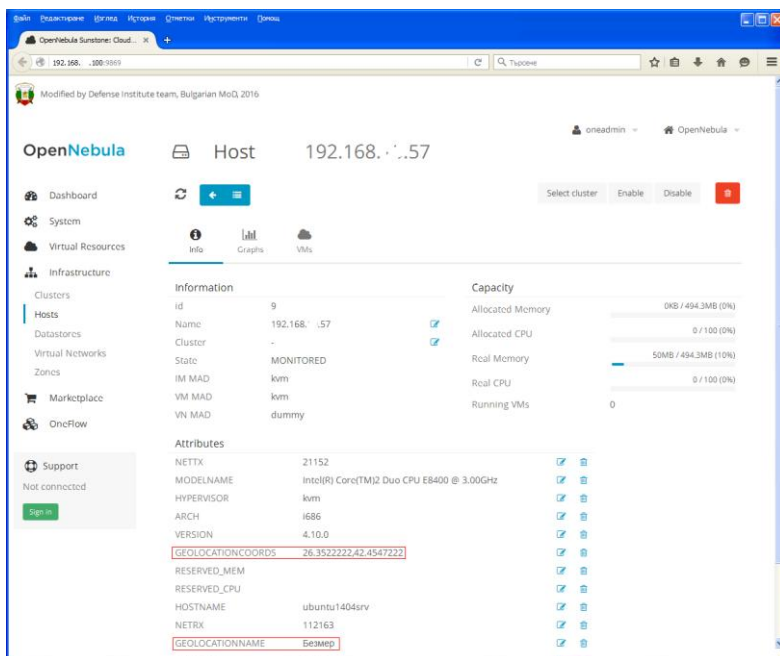
Експерименталната среда е изградена и конфигурирана върху един персонален компютър под управление на операционна система *Windows XP*. Като система за виртуализация е използвана виртуализационна платформа *Oracle VirtualBox v. 4.2* [3].

Тестовата система, предоставена от разработчиците на *OpenNebula* е виртуалната машина *one-sandbox*. На нея са инсталирани и конфигурирани интерфейсите за управление на облачна среда от команден ред *opennebula-server* и *opennebula-node* и графичният web-базиран интерфейс *Sunstone*. На разположение за експериментиране е конфигуриран един хост с възможност за развързване на един шаблон за виртуална машина с ограничена функционалност *ttylinux*.

В отговор на необходимостта за експериментиране с няколко хоста са създадени и стартирани виртуалните машини *Ubuntu 12.04* и *Ubuntu server 14.04*. Мрежовата среда на *VirtualBox* за всички машини, участващи в експеримента е конфигурирана в режим *bridge mode*. За придобиване на функционалност в облачна среда, на новодобавените хостове са извършени следните настройки:

- инсталирана е поддръжка за криптиран мрежов протокол *OpenSSH*;
- дефиниран е потребител *oneadmin* с права за *SSH* достъп;
- осигурена е способност за *passwordless SSH* конекция към машината *one-sandbox*. За целта на машината *one-sandbox* за всеки хост са генерирани частен и публичен криптографски ключове, публичният ключ е предоставен на съответния хост;
- инсталиран е софтуерният пакет *opennebula-node*.

Стартирането на графичния web-базиран административен интерфейс *Sunstone* (виж фиг. 3) показва функционална адекватност на изградената тестова облачна среда.



Фиг. 3. WEB-базиран графичен интерфейс *OpenNebula Sunstone*

В случая, когато хостовете от облачната инфраструктура са физически машини в по-горе описаната обединена линия за предаване на данни е в сила въпросът за въвеждане на информация относно тяхното гео-локализиране. Към времето на настоящето научно изследване публична документация на информационната структура на продукта *Sunstone* по мнение на авторите не е достъпна. Лицензионната политика разработчиците на продукта *Apache License, Version 2.0* [4] позволява трети страни да извършват изменения в кода и това обстоятелство е използвано от авторите за доизграждане на подсистема за географско привързване.

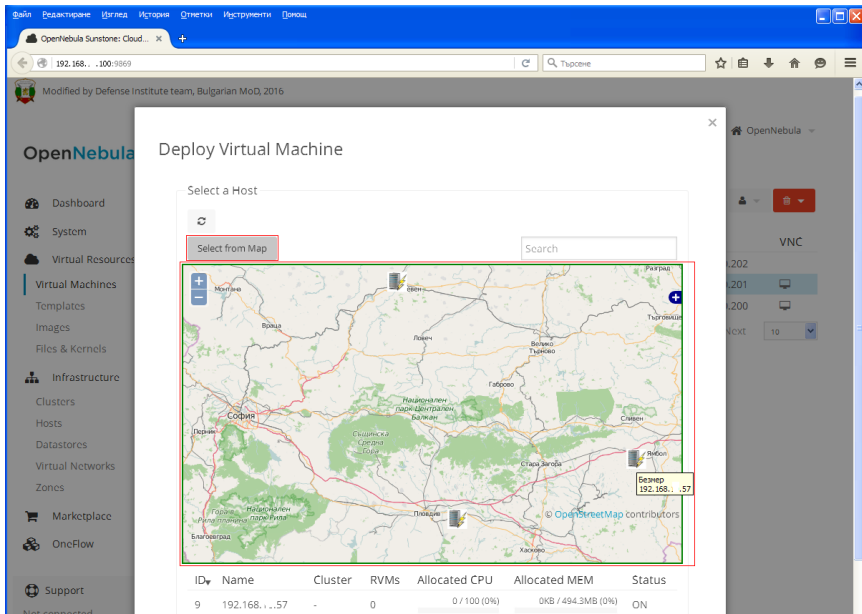
Извършени са модификации във файловете:

/usr/lib/one/sunstone/views/index.erb
 /usr/lib/one/sunstone/public/js/sunstone.js
 /usr/lib/one/sunstone/public/js/plugins/vms-tab.js
 /usr/lib/one/sunstone/public/js/plugins/hosts-tab.js

Добавени са файловете:

/usr/lib/one/sunstone/public/images/logos/logo-io.png
 /usr/lib/one/sunstone/public/js/vm-host-deploy.js
 /usr/lib/one/sunstone/public/js/OpenLayers-2.13.1/*.*
 /usr/lib/one/sunstone/public/js/image/ahost.jpg

В резултат от извършената работа по изменение на софтуерния код на продукта *OpenNebula Sunstone*, администраторът на облачната инфраструктура получава способността да развърща шаблони за виртуални машини на точно определени хостове с посочване на електронна географска карта. Екран от работещата система е представен на Фиг. 4.



Фиг. 4. Графичен интерфейс с електронна географска карта

В екрана *Deploy Virtual Machine* е добавен бутон *Select from Map*. С кликването на този бутон администратора извежда електронна географска карта с визуализирани позиции на хостовете от облачната инфраструктура. Задръжането на курсора на мишката върху съответната пиктограма показва екранен хинт с географското и мрежово наименование на въпросния хост. Кликването на пиктограмата селектира хоста, на който да се ръзвърне виртуалната машина.

ЗАКЛЮЧЕНИЕ

Въпреки че тактическите връзки за данни играят много важна роля в съвременната война и техните функции са много по-добри от тези на обикновените тактически комуникационни системи, те имат свойствени ограничения. Ограничения като ориентираност към специфична платформа и липса на универсалност значително ограничават възможността за взаимодействие между връзките за данни на бойното поле. Облачният компютинг е иновация в информационното поле. Така че дискутираната в материала архитектура за обединени линии за предаване на данни, базирани на облачен компютинг, заедно с предложената от авторите модификация за географска свързаност на физически компоненти позволява тактическите връзки за данни да се развият до интелигентна мрежова система за бойното поле. Комбинацията преобразува оригиналните комуникационни канали в "интелигентни канали". По този начин се постига взаимодействие между няколко връзки за данни, осъществява се качествено информационно обслужване, отговаря се на изискването за предаване на "правилната информация" към "правилния приемник" в "правилния формат" в "точното време". По-добре развитата способност за получаване и обработка информация се превръща в способност за вземане на научнообосновано решение и научнообосновано водене на военни действия в максимална степен.

Литература:

1. Yang Juan. Joint Data Link Based on Cloud Computing, Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013), China, 2013;
2. The Simplest Cloud Deployment and Management Experience, <http://opennebula.org/>, accessed march 2016;
3. VirtualBox, <https://www.virtualbox.org/>, accessed march 2016;
4. <https://github.com/burgosz/opennebula-sunstone-shib/blob/master/ruby/opennebula.rb>, accessed march 2016;

АРХИТЕКТУРА НА ОБЛАЧНА МРЕЖА ЗА РАДИОДОСТЪП ЗА НУЖДИТЕ НА СИГУРНОСТТА И ОТБРАНАТА

Иван П. Иванов

Р България, София 1592, бул. "Цв. Лазаров" № 2,
Институт по отбрана „Професор Цветан Лазаров”
Тел. +359 2 92 21822, E-mail: i.p.ivanov@di.mod.bg

ARCHITECTURE OF CLOUD RADIO ACCESS NETWORK FOR SECURITY AND DEFENCE

Ivan P. Ivanov

ABSTRACT: *Radio Access Networks are the foundation of mobile communication systems. Demand for high-speed services and capacity require implementation of new approaches and technologies. The proposed architecture is based on the paradigm of cloud computing and software-defined radio and introduces new functionality for multiprotocol support. Summarized are main advantages and disadvantages of cloud radio access network for security and defense.*

KEY WORDS: *cloud radio access network, software-defined radio, network architecture.*

Въведение

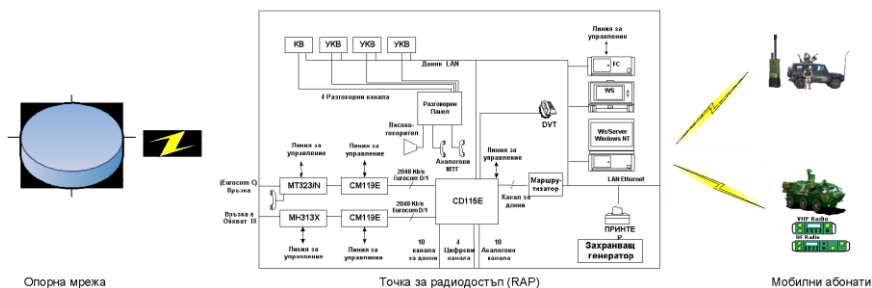
Мобилните радиокомуникации са в основата на всяка съвременна военна комуникационно-информационна система (КИС), осигурявайки на командирите обмен и достъп до информационни ресурси навсякъде и по всяко време. Запазва се тенденцията на нарастване на потребностите от високоскоростен обмен на данни, което води до усложняване на базовите станции на клетъчна система и точките за достъп до радиомрежите за бойно управление. Гражданските технологии активно навлизат във военните КИС и се очаква в бъдеще да бъдат в основата на конкретни реализации на подсистемата за мобилен радиодостъп. Бумът в разпространението на смартфоните, използването на социалните мрежи, тенденцията по навлизане на концепцията „Интернет на нещата“ (Internet of things) и др. поставя значителни предизвикателства пред следваща генерация безжични комуникационни мрежи и системи. Предвижда се скокообразна увеличение на потребителите на мобилни услуги и потребност от по-високи скорости, в условията на ограничен честотен ресурс. В същото време запазването на тенденцията за увеличаване на компютърната мощ по закона на Мур, развитието на технологии като облачни изчисления (cloud computing), софтуерно-дефинирани мрежи, виртуализация на мрежови функции (Network Function Virtualization - NFV), масивни MIMO (multiple input multiple output), софтуерно-дефинирани радиостанции и др. предлага решения за оптимизиране на ресурсите и разширение на възможностите на бъдещите безжични мрежи. В последните години парадигмата за облачна мрежа за радиодостъп (Cloud Radio Access Network - CRAN) поражда значителен изследователски интерес като потенциално решение за оптимизиране на изчислителните и радиочестот-

ни ресурси, повишаване на пропускателната способност, увеличаване на брой на обслужваните потребители и др. [1][2]. В спецификация GS NFV 001 v.1.1.1 (2013-10) на форума на Европейския стандартизационен институт по телекомуникации (ETSI) е разработен вариант за реализиране на парадигмата чрез използване на NFV[3]. Предложените концепции и изследвания разглеждат възможността за използване на облачните изчисления в мрежите за радиодостъп в тясната област на едно конкретно приложение или технология. Интерес представлява обединяването им в единна архитектура за нуждите на военни комуникационно-информационни системи.

Мрежи за радиодостъп в КИС на БА. Текущо състояние и проблеми

Мрежата за радиодостъп е подсистема на мобилната комуникационна мрежа и осигурява най-общо свързаността на мобилните устройства до опорната мрежа, преноса на услугите и контрола на достъпа. Типични структурни елементи за реализиране на технологията са базов приемо/предавател и контролер на мрежата за радиодостъп. Характерни примери за мрежи за радиодостъп в КИС на БА са подсистема CNRA на Полевата интегрирана комуникационно-информационна система (ПИКИС) на 61 мбр и подсистема RAN на Автоматизираната система за свързаност с подвижни обекти (АМСПО) на БА по стандарт “Тетра”.

Системата CNRA позволява на мобилните абонати да комуникират с всички абонати (стационарни и мобилни) на ПИКИС и други мрежи, с които ПИКИС е свързана. На фиг. 1. е показана архитектурата на мрежата за радиодостъп в ПИКИС на 61 мбр [4]. Основни елементи са мобилна абонатна станция, базирана на едно-канална радиостанция и точка за радиодостъп (RAP) или мобилен команден пункт (MCP).



Фиг. 1. Мрежа за радиодостъп на система ПИКИС 61 мбр.

На базата на едноканалните радиостанции (мобилни и от състава на RAP) и мрежовото оборудване от опорна мрежа се изгражда т.нар. “Тактически Интернет” - рутерна TCP/IP мрежа, позволяваща на абонатите на ПИКИС да обменят съобщения и осигуряваща достъп до информационната система за командване и управление. Архитектурата на тази система води до струпването на над 60 едноканални радиостанции на пункта за управление на механизирания бригада.

Автоматизираната система за свързаност с подвижни обекти (АМСПО) на БА е въведена в експлоатация през 2003 г. и е многократно развивана през годините до

днес. Системата е базирана на стандарта за професионални мобилни мрежи TETRA на ETSI. Архитектурата на системата Tetra-Dimetra е показана на Фигура 2 [5].



Фиг. 2. Архитектура на Автоматизирана мрежа за свързка с подвижни обекти на БА по стандарт TETRA.

Мрежата за радиодостъп на системата включва мрежовата част на мобилните абонатски станции (МАС), базовите станции (БС) и радиоинтерфейса МАС-БС.

Основните капиталови разходи в мрежата за радиодостъп се пада на базовата станция (точката за достъп). Типично, този компонент на системата е монолитен блок, специално разработен за конкретна технология за мобилна мрежа, изграден със специализирани интегрални схеми, без възможност за хардуерни и софтуерни промени. Базовата станция реализира в себе си и трите слоя - от физическия до мрежовия на еталонния модел на OSI. Промяната в софтуера на Центъра за управление и комутация (ЦУК) или обновяването на стандарта за мобилна мрежова технология налага цялостна подмяна на базовата станция. Много често на едно и също физическо място се разполагат базови станции на различни ведомствени мрежи (например МО и МВР) без възможност за споделяне на ресурси. В традиционната архитектура на мрежите за радиодостъп, всяка БС комуникира по самостоятелен интерфейс с ЦУК. Това намалява възможностите за коопериране, разпределение на ресурсите и натоварването между БС, в зависимост от разпределението на потребителите. Всяка базова станция е проектирана и реализира конкретен стандарт за радиодостъп. В условията на многообразие на използваните технологии за радиодостъп в КИС на БА, на комуникационния възел на пункта за управление се получава струпване на технически средства, което води до намаляване на скритостта, както и до увеличаване на консумираната енергия.

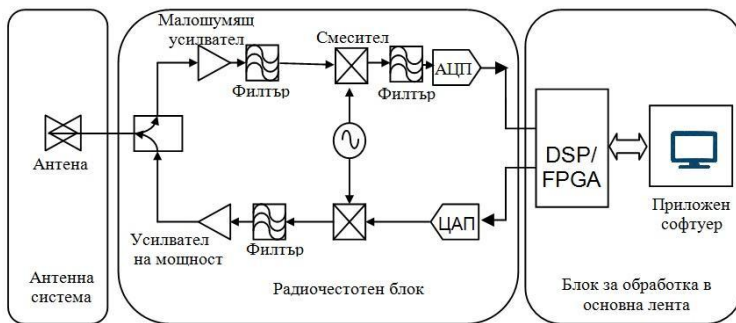
Облачна мрежа за радиодостъп за нуждите на сигурността и отбраната

Решение за преодоляване на недостатъците на текущите системи предлага парадигмата за използване на облачните технологии в мрежите за радиодостъп. Предлагащата облачна мрежа за радиодостъп за нуждите на сигурността и отбрана-

та се базира на технологиите - софтуерно-дефинирана радиостанция, пренос на радиочестотни сигнали по оптика и облачни изчисления и включва следните основни структурни компоненти:

- виртуализирана софтуерно-дефинирана базова станция;
- виртуализиран споделен блок за обработка в основна лента;
- виртуализиран център за управление и комутация.

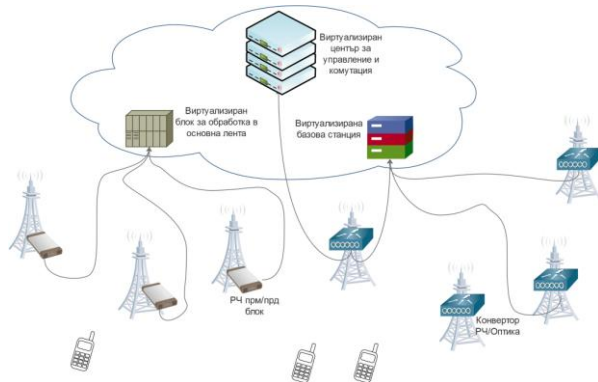
Софтуерно-дефинираната радиостанция (СДР) е съвременна технология за изграждане на радиочестотни приемо-предаватели [4]. Една от основните ѝ характеристики е, че обработката в основна лента се извършва от цифров сигнален процесор и/или персонален компютър. Блокова схема на СДР е показана на фиг.3.



Фиг. 3. Блокова схема на софтуерно-дефинирана радиостанция.

Архитектурата на СДР се състои от три основни блока – антенна система, радиочестотен блок и блок за обработка в основна лента. При наличие на развита оптична инфраструктура, тези компоненти могат да се намират на значително разстояние помежду си.

Архитектурата на облачна мрежа за радиодостъп за нуждите на сигурността и отбраната е показана на фиг. 4.



Фиг. 4. Архитектура на облачна мрежа за радиодостъп.

Основна характеристика в предложената архитектура е разполагането на обработката в основна лента в облака, на виртуализирана платформа. Виртуализираният блок за обработка на сигнала в основна лента (ВБОУЛ) извършва филтриране, честотно преобразуване, демодулация и др. Блокът е общ за клъстер от базови станции. Физически ВБОУЛ е единен блок, а виртуализацията гарантира заделянето на подходящи ресурси за всяка базова станция. Процесът по заделяне на ресурси може да е динамичен, като при липса на потребители за определена БС, ресурси не се заделят. Виртуализираният блок за обработка на сигнала в основна лента реализира различни мрежови протоколи – GSM, LTE, WiMAX, WiFi, TETRA и др., които се зареждат като приложения от ЦУК, в зависимост от конкретния абонат. В зависимост от мястото на разполагането на РЧ блок има два типа базови станции – БС с прм/прд РЧ блок и БС само с усилвател на мощност и конвертор РЧ/оптика. Първият тип осигурява оптичен интерфейс по който се обменят реалната и имажинерната част (IQ) на дискретите с ВБОУЛ. Вторият тип ползва технологията “RF over optics”, при която приетият РЧ сигнал се преобразува в оптичен, пренася се през инфраструктурата и се преобразува в РЧ сигнал в облака. При този подход цялата обработка на сигнала се извършва в блока „виртуализираната базова станция”, т.е. базовата станция се изнася в облака.

Предложената архитектура предлага следните основни предимства:

- Опростява се радиочестотният сайт (точката за достъп) и се намалява неговият физически размер.
- Базовата станция става индиферентна към протокола на мобилната мрежа, който пренася, което от своя страна предлага решения за съвместимост между различни мрежи и протоколи.
- Намалява се интерференцията между клетките, а от там се повишава капацитета на мрежата.
- Увеличава се еластичността на мрежата - ресурсите се централизират и могат да се преразпределят в зависимост от натоварването.
- Създават се подходящи условия за коопериране в канала БС-МС.
- Повишава се сигурността на информацията - криптирането се извършва в облака.
- Опростява се криптомрежата - при традиционните модели ключът се намира в базовата станция. Сега ключът е в облака (центъра за данни). Избягва се необходимостта при обновяване на системата да се обходи физически цялата система за промяна на ключовете. За мрежи с национално покритие това е трудно, а понякога невъзможно за определени точки за радиодостъп, в определени годишни сезони.
- Централизацията намалява цената на притежания на мрежата (ОРЕХ).
- Виртуализацията позволява типичната (позната) базова станция да се изгражда на базата на разпространени COTS сървъри.

Някои от предизвикателствата и проблемите в предложената архитектура са свързани с необходимостта от наличие на развита оптична инфраструктура. В същото време оптичните технологии, особено базираните на Ethernet, непрекъснато поевтиняват, което предлага нови решения. Друг проблем е свързан с увеличаването на време-закъснението, породено от необходимостта сигналът да бъде пренесен до разположените в облака блокове за обработка. Решението е в зависимост от конкретната технология и изискванията към този параметър. Възможен подход е обе-

диняването на група от базови станции в клъстер и разполагането на ВБОУЛ в облака, при изпълняване на изискванията за максимално отстояние от БС.

Заклучение

Парадигмата за облачни изчисления предлага решения на актуални проблеми на съвременните мрежи за радиодостъп. Предложената архитектура се базира на изнасянето на обработката на сигнала в облака, като е предложено и реализирането на множество от протоколи и виртуализация им. Направление за по-нататъшни изследвания е възможността за прилагане на такива протоколи и технологии като коопериране на БС в канала БС-МС, мрежово кодиране, противодействие на преднамерени смущения и др.

Източници:

1. China Mobile Research Institute. C-RAN International Workshop "the 1st C-RAN International Workshop"<http://labs.chinamobile.com/focus/C-RAN>
2. D. Pompili, A. Hajisami, and H. Viswanathan, Dynamic provisioning and allocation in Cloud Radio Access Networks (C-RANs). Ad Hoc Networks, vol. 30, 2015.
3. ETSI GS NFV 001 V1.1.1 (2013-10). Network Functions Virtualisation (NFV); Use Cases.
4. Иванов И. “Софтуерна” радиостанция – перспектива за радиокомуникационната подсистема на С4ISR системи и автоматизирани системи за управление на оръжията за тактическото звено. Международна научна конференция – Изследвания и технологии за нуждите на отбраната “Модернизация на въоръжените сили – крайъгълен камък по пътя към НАТО” в рамките на 5-та международна изложба на военна техника “Хемус 2002”.
5. Диков Д., И. Иванов. Военна мобилна мрежа по стандарт TETRA. Състояние и перспективи за развитие. Шумен 2010.

ПРИЛОЖЕНИЕ НА ЛИНЕЙНОТО ОПТИМИРАНЕ В УПРАВЛЕНИЕТО НА СИСТЕМИТЕ ЗА ИНФОРМАЦИОННА СИГУРНОСТ.

Илиян Н. Лилев, Иван Й. Георгиев

*Адрес за кореспонденция: гр. Велико Търново
Национален военен университет „Васил Левски“ бул. „България“ №76
служебен тел.62072 GSM 0884 54 15 85, e-mail: inl@abv.bg*

*Адрес за кореспонденция: гр. Велико Търново
Национален военен университет „Васил Левски“ бул. „България“ №76
служебен тел.62156 GSM 0884 13 48 19, e-mail: ivan_georgiev688@abv.bg*

APPLICATION OF LINEAR OPTIMIZATION IN SYSTEMS FOR INFORMATIONAL SECURITY.

Ilian N. Lilov, Ivan Y. Georgiev

ABSTRACT: *An application of linear optimization for solving assignment tasks in area of informational security is examined in this article. A Microsoft Excel –Solver method for solving of mathematical models is presented with following analysis.*

KEY WORDS: *linear optimization, informational security.*

Развитието на човешката цивилизация е съпроводено от непрекъснатите усилията на хората да взаимодействат с природата и помежду си като по този начин се създават условия за по-добър живот, сигурност и благоденствие. Крайните резултати от тези взаимодействия могат да бъдат повече или по-малко благоприятни. Стремелът на индивидите е да действат по такъв начин, че да избегнат неблагоприятните и да реализират благоприятни резултати.

Насоката на правилните действия се подпомага от опита, интуицията, чувствата и знанията на хората за развитието на природата, обществото и мисълта. Важна предпоставка за постигане на благоприятният изход е да се разгледа, анализира и осмисли процеса на вземане на решение, който е основния предмет на дисциплината изследване на операциите. Нейното начало се поставя с раздела линейно оптимизиране.

Едно от приложенията на линейното оптимизиране е при решаване на т.н. разпределителни задачи. Разпространено е становището, че тези математически модели се прилагат основно в сферата на логистиката за оптимално управление на транспортни потоци.

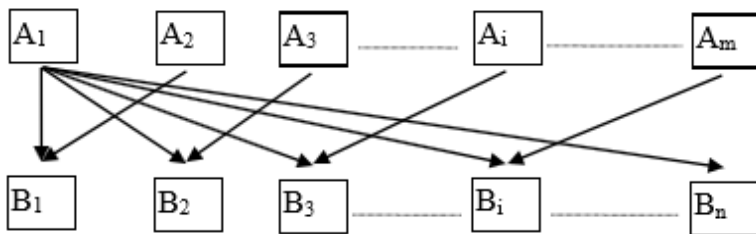
Целта на настоящия доклад е да покаже, че гореспоменатите модели могат да бъдат приложени и за оптимално управление на информационни потоци.

Често в практиката се налага ресурси, намиращи се в едно състояние, количество и място, да бъдат разпределени в други състояния, количества или на друго място. Когато тази дейност се извършва по предварително зададен критерий за

оптималност това са т.нар. разпределителни оптимизационни задачи. Особеното при разпределителните задачи е, че обобщените координати се задават с матрица на неизвестните.

Математическият модел на тези задачи както всички от този клас включва целева функция, ограничителни условия, условия за неотрицателност и условия за целочисленост, когато се налага.

Формулира се задачата по следния начин. Дадени са m отправни пункта (доставчици на информация) $A_1, A_2, A_i, \dots, A_m$ и n приемателни пункта (потребители) $B_1, B_2, B_3, \dots, B_j \dots B_n$.



Фиг. 1. Примерна схема на информационния поток.

Във всеки отправен пункт има наличност от еднороден продукт в количества съответно $a_1, a_2, \dots, a_i \dots a_m$. Този продукт следва да бъде доставен в пунктовете за потребление в количества съответно $b_1, b_2, \dots, b_j \dots b_n$. За доставянето **на единица продукт** от i -тия отправен пункт до j -тия приемателен пункт се изразходват определени ресурси, които се оценяват на c_{ij} .

Матрицата на ресурсите е:

$$(1) \quad C = \|C_{ij}\|_{m,n} = \begin{vmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mn} \end{vmatrix}$$

Целта на разпределителната задача е да се намери оптимален план на доставка на определените количества от необходимият продукт, който следва да бъде изпратен от всеки отправен пункт до всеки пункт за потребление, така че степента на защита на информацията да бъде максимална.

План на разпределителната задача е матрицата

$$(2) \quad \|x_{ij}\|_{m,n} = \begin{vmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{vmatrix},$$

където x_{ij} представлява количеството продукт, което трябва да бъде доставено от i -тия отправен пункт в j -тия приемателен пункт. Тя се нарича матрица на достав-

ката или още е матрица на неизвестните, тъй като именно x_{ij} се търси при решението на задачата.

Двете матрици се поместват в т.нар. разпределителна таблица [1, 2].

$A_i \backslash B_j$	B_1	B_2	B_3	...	B_j	...	B_n	a_i
A_1	x_{11}	c_{12}	x_{13}	...	x_{1j}	...	x_{1n}	a_1
A_2	x_{21}	c_{22}	x_{23}	...	x_{2j}	...	x_{2n}	a_2
...	...	...	...	...	...	...	...	...
A_i	x_{i1}	c_{i2}	x_{i3}	...	x_{ij}	...	x_{in}	a_i
A_m	x_{m1}	c_{m2}	x_{m3}	...	x_{mj}	...	x_{mn}	a_m
b_j	b_1	b_2	b_3	...	b_j	...	b_n	$\sum a_i$ $\sum b_j$

На базата на тази теоретична обосновка е възможно с помощта на **Microsoft Excel – Solver** да се решават задачи от подобен тип. Разработен е примерен вариант на задача за максимална защита на класифицирана информация.

Пример: Ежедневният обмен на класифицирана информация между три областни и 4 районни кризисни центъра е **9800MB**. Наличната информация в областните центрове, необходимата такава за районните центрове и количественото изражение на степента на сигурност за пренасяне на информация по всеки канал са дадени в таблицата. Координаторът по защита на класифицираната информация трябва да вземе решение кои канали да използва и как да разпредели обмена на информация, така че да осигури максималната ѝ защита.

Таблица 1

Областни центрове \ Районни центрове	1 ^{ви} районен център	2 ^{ви} районен център	3 ^{ви} районен център	4 ^{ви} районен център	Налична информация
1 ^{ва} областен център	0,8	0,5	0,4	0,6	3000MB
2 ^{ва} областен център	0,2	0,1	0,9	0,3	5000 MB
3 ^{та} областен център	1	0,5	0,8	0,4	1800 MB
Необходима Информация	2200 MB	3100 MB	2000 MB	2500 MB	9800 MB

Решение:

Матрицата на разпределението на сигурността на информацията на каналите е:

$$(3) \quad c_{ij} = \begin{vmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \end{vmatrix} [3, 4, 5]$$

Планът на разпределение на информацията е матрицата на неизвестните:

$$(4) \quad x_{ij} = \begin{vmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{34} \end{vmatrix} [3, 4, 5]$$

Дефинира се целевата функция на задачата съобразена със представения план в таблица 1.

$$(5) \quad Z = 0,8.x_{11} + 0,5.x_{12} + 0,4.x_{13} + 0,6.x_{14} + 0,2.x_{21} + 0,1.x_{22} + 0,9.x_{23} + 0,3.x_{24} + 1.x_{31} + 0,5.x_{32} + 0,8.x_{33} + 0,4.x_{34} \rightarrow \max$$

Задават се ограничителните условия на задачата.

Неизвестните величини x_{ij} трябва да удовлетворяват следните условия:

Цялото количество информация от областните центрове a_1 , a_2 и a_3 , трябва да бъде предадено с необходимата сигурност.

$$(6) \quad \begin{aligned} x_{11} + x_{12} + x_{13} + x_{14} &= 3000 \\ x_{21} + x_{22} + x_{23} + x_{24} &= 5000 \\ x_{31} + x_{32} + x_{33} + x_{34} &= 1800 \end{aligned}$$

Във всеки районен център трябва да бъде доставена заявеното количество информация.

$$(7) \quad \begin{aligned} x_{11} + x_{21} + x_{31} &= 2200 \\ x_{12} + x_{22} + x_{32} &= 3100 \\ x_{13} + x_{23} + x_{33} &= 2000 \\ x_{14} + x_{24} + x_{34} &= 2500 \end{aligned}$$

Задава се условие за неотрицателност $x_{1-4} \geq 0$.

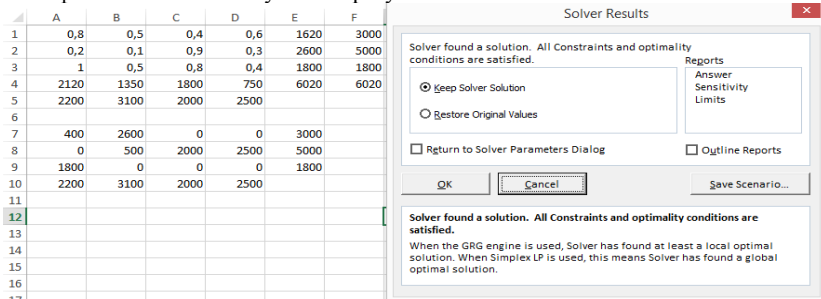
За решаване на математическата задача информацията се въвежда в основната таблица на *Microsoft Excel*. Задават се коефициентите на целевата функция, ограничителните условия и неизвестните (фиг. 1) [3].

S22							
	A	B	C	D	E	F	G
1	0,8	0,5	0,4	0,6		3000	
2	0,2	0,1	0,9	0,3		5000	
3	1	0,5	0,8	0,4		1800	
4							
5	2200	3100	2000	2500			
6							
7	1	1	1	1			
8	1	1	1	1			
9	1	1	1	1			
10							

Фиг. 1

Задава се формулата на целевата функция (фиг. 2).

На фиг. 5 е показан полученият резултат:



Фиг. 5

Решение на задачата:

Районни центрове		2	3	4	5	6	7	8
Областни центрове	1-и районен център	0,8	0,5	0,4	0,6	Налична информация в ОЦ, [МВ]	информация изпратена от ОЦ, [МВ]	Коефициент на успеваемост на ОЦ, %
	2-ри областен център	400	2600	0	0	3000	1620	54
	3-ти областен център	0	500	2000	2500	5000	2600	52
	4-ти областен център	1800	0	0	0	1800	1800	100
5	Необходима информация в РЦ, [МВ]	2200	3100	2000	2500	9800	Общо изпратена информация	
6	информация получена в РЦ, [МВ]	2120	1350	1800	750		6020	Целева функция (общо количество получена информация)
7	Коефициент на успеваемост на РЦ, %	96,36	43,55	90	30		Коефициент на успеваемост на информационната система	61,43

Таблица 2

Коефициентът на успеваемост (сигурност) на предадената/получената информация се определя след окончателното ѝ разпределение в таблица 2.

Действително изпратената информация от областните центрове е представена в колона 7, а коефициента на успеваемост в колона 8 на таблица 2.

Действително получената информация от районните центрове е представена в ред 6, а коефициента на успеваемост в ред 7 на таблица 2.

С формула (8) е показано как се изчислява коефициента на успеваемост на областните центрове.

$$(8) \quad K_{i_{oc}} = \frac{100 \cdot (c_{i1} \cdot x_{i1} + c_{i2} \cdot x_{i2} + c_{i3} \cdot x_{i3} + c_{i4} \cdot x_{i4})}{a_i} = \frac{54}{52} \cdot \frac{52}{100}, \%$$

а с (9) – на районните центрове:

$$(9) \quad K_{j_{pu}} = \frac{100 \cdot (c_{1j} \cdot x_{1j} + c_{2j} \cdot x_{2j} + c_{3j} \cdot x_{3j})}{b_j} = \begin{bmatrix} 96,36 \\ 43,55 \\ 90 \\ 30 \end{bmatrix}, \%$$

Изводи:

1. От наличната **9800Mb** информация, която се разпределя ежедневно, максимално възможната степен на защитеност, която може да се постигне при дадените обстоятелства е **61,43% или 6020Mb**.

2. Ако се направи класификация по районни и областни кризисни центрове, анализът показва, че от районните центрове най-защитен за получаване на информация се оказва първият (**96,36%**), а най-слабо е последният (**30%**). Най-удачен за изпращане на информация се оказва третият областен център (**100%**), а най-незащитен е вторият (**52%**).

Литература:

1. Изследване на операциите, ДВИ, София, 1975.
2. Василев Н., Цанов Л. и др., Приложна математика, ВИ, София, 1985.
3. Лилев И., Количествени методи в логистиката, НВУ „Васил Левски”, В. Търново, 2013.
4. Taha H. Operations research an introduction. Education, Ins, 2003.
5. Winston W. L. Operations research. Applications and algorithms, Duxbury press, 2003.

МОДЕЛИ ЗА КОНТРОЛ НА ДОСТЪПА ДО ИНФОРМАЦИЯ

Димитър Т. Дойчинов

*Национален Военен Университет "В. Левски",
Факултет „Артилерия, ПВО и КИС“, ул. „Карел Шкорпил“ 1, Шумен,
e-mail: d.doychinov@nvu.bg*

INFORMATION ACCESS CONTROL MODELS

Dimitar T. Doychinov

ABSTRACT: The purpose of this paper is make a review of information access control models. Advantages and disadvantages of some models are shown.

KEY WORDS: information security, access control, models.

Моделите за сигурност определят основата за създаване на политика за сигурност. Създадени са много модели, за да се обхванат различните съображения за сигурност. Целта на всички модели на сигурност е да се определят разрешените и неразрешени състояния на една система и да ограничат преминаването ѝ в неразрешено състояние. Моделите за сигурност се разработват на базата на типа на системата за която ще се използват. Някои модели се използват, за да се гарантира сигурността на операционните системи, докато други се използват за специфично приложение, например база от данни.

В етапа на моделиране се използват обобщени модели със следното предназначение:

- проектиране и реализация на архитектура на политика за сигурност;
- проверка на качествата на конкретна архитектура за реализация на желана политика за сигурност.

В литературата се срещат три основни класа модели на политика за сигурност: дискреционни, задължителни и ролеви [7, 8, 9].

Основа на дискреционна (избирателна) политика за сигурност е дискреционно-то управление на достъпа (discretionary access control - DAC), който се характеризира със следните свойства:

- всички субекти и обекти трябва да бъдат идентифицирани;
- права на достъп на субекта към обектите на системата са базирани на някакви външни за системата правилата.

Правила при дискреционното управление на достъпа често се задават с матрицата за достъп. В такава матрица редове съответстват на субектите, колоните на обектите, елементите на матрицата описват правата за достъп до съответната двойка на "субект - обект".

Един от най-известните дискреционни модели е моделът Harrison-Russo-Ullman, наричан още „матричен модел“. Този тип на контрол на достъпа е най-често използвания в операционни системи, поради относителната лекота на прила-

гане. В този случай правилата за контрол на достъпа често са описват чрез на списъци на контрол на достъпа (Access Control List – ACL). Списъка е свързан със защитаваните обект и съхранява списък на субектите и техните разрешения за даден обект.

Основа за мандатната политика за сигурност (mandatory access control – MAC) е мандатното управление на достъпа, което означава, че:

- всички субекти и обекти трябва да бъдат идентифицирани;
- зададен е линеен набор от степени на класификация на поверителност;
- на всеки обект е присвоена степен на поверителност, определяща ценността на информацията, съдържаща се него – степен на секретност;
- на всеки субект е присвоено ниво на поверителност, определящо степента на доверие към него – неговото ниво на достъп ;
- решението да се позволи достъп до обекта на субекта е взето въз основа на вида на достъп и сравняване на степените на субекта и обекта.

Контрол на достъпа на базата на роли, оперира с термините "роля", "потребител", "операция". Информация се разглежда като принадлежаща на организацията, а не на създателя ѝ. Решенията за позволяване или отказване на достъп се вземат въз основа на информацията за функцията (ролята), които потребителят изпълнява в организацията. Роля може да се разбира като съвкупност от действия, които са разрешени на потребителите за изпълнението на техните задължения. Администраторът описва ролите и упълномощава потребителите да изпълняват дадена роля. Ролевите модели съдържат признаци на мандатните и на избирателните модели.

За проектиране и реализация на архитектура на политика за сигурност в теорията са популярни следните модели за управление на сигурността на няколко нива [7]:

- модел на Bell-La Padula за гарантиране на конфиденциалност на информацията;
- модел на Biba за контрол на достъпа;
- решетъчен модел на достъпа (Lattice Model of Access Security).

За проверка на теоретичните ограничения на конкретна архитектура на система управление на сигурността се използват следните модели:

- модел на Graham-Denning;
- модел на Jones (take-grant).

1. Решетъчен модел на достъпа (Lattice Model of Access Security)

В този модел понятието *решетка* представлява математическа структура от елементи и релациите между тях, представени от релационен оператор, означен с нотацията $\leq$. Отношението (релацията) е транзитивно и асиметрично. По смисъла на това отношение най-големият елемент от решетката представлява най-високото ниво на класификация и доминира над всички останали. Съответно най-малкият елемент е най-ниското ниво на класификация и е доминиран от всички останали елементи.

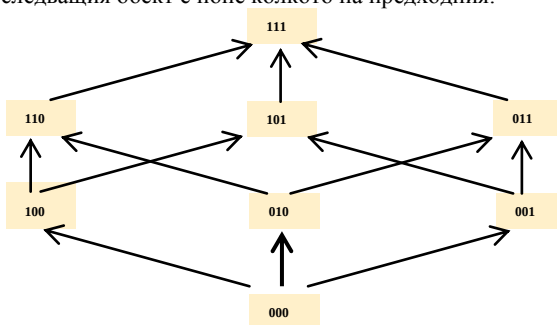
В моделна релацията се нарича частично подредена, когато тя е едновременно транзитивна и асиметрична. Това означава, че за всеки три елемента **a**, **b** и **c** са валидни следните две правила:

транзитивност: Ако $a \leq b$ и $b \leq c$, тогава $a \leq c$,

асиметричност: Ако $a \leq b$ и $b \leq a$, тогава $a = b$.

В решетката не е задължително всяка двойка елементи да бъдат сравними, т.е. допускат се елементи a и b , за които твърденията $a \leq b$ и $b \geq a$ са неистина. Същевременно всяка двойка елементи притежава горна граница – елемент u , такъв, че са изпълнени условията $a \leq u$ и $b \leq u$, както и долна граница – елемент l , доминиран от a и b , такъв, че са изпълнени условията $l \leq a$ и $l \leq b$.

На фигура 1 е изобразява решетъчен модел, представящ вариациите 2^n при $n = 3$ права за достъп, представени като битови вектори. Този модел се използва при системи в които обмена на информацията е възможен само ако нивото на класификация на следващия обект е поне колкото на предходния.



Фигура 1. Решетка на правата за достъп при $n = 3$

2. Модел на Bell-La Padula за гарантиране на конфиденциалност на информацията

Моделът Bell и La Padula [2] е формално описание на разрешените маршрути на движение на информационния поток в една сигурна система. Целта на модела е да се идентифицират допустимите комуникации, когато поддържането на определено ниво на конфиденциалност е първостепенно значение. Този модел се ползва за определяне на изискванията за сигурност на системи за обработка на информация с различни нива на класификация.

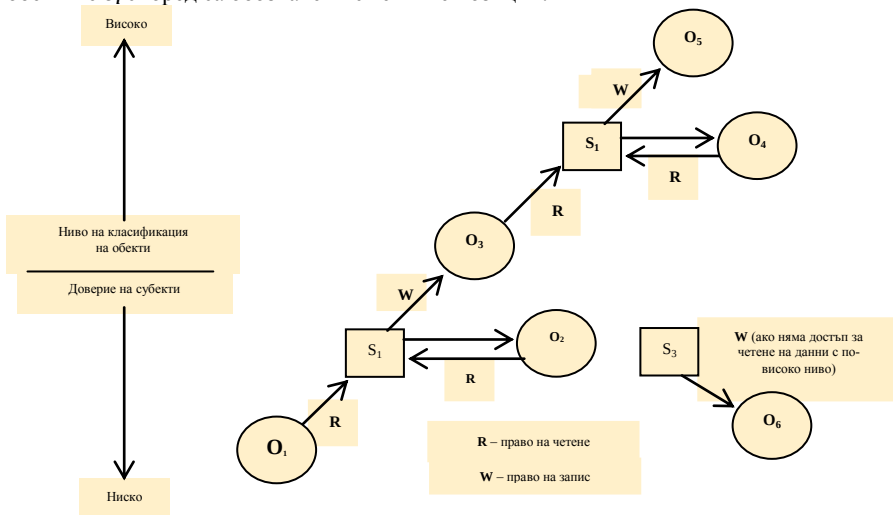
В този модел системата за сигурност се състои множества от субекти $S\{s_1, s_2, \dots, s_i\}$ и обекти $O\{o_1, o_2, \dots, o_j\}$. Всеки субект s_i и всеки обект o_j притежава определен клас на сигурност $C_i(s_i)$ и респективно $C_j(o_j)$, обозначаващи правата на достъп и нивото на класификация. Класовете на сигурността са структурирани йерархично.

При този модел потокът на информация по отношение на сигурността се дефинира чрез следните свойства.

Първо свойство (Simple Security Property) – субект s_i притежава достъп за четене на информация от обекта o_j само, ако е изпълнено условието $C_j(o_j) \leq C_i(s_i)$. С други думи нивото на достъп на получаващия информация следва да бъде поне от същото ниво на класификация на информацията (**no read-up**).

Второ свойство (Star Property) – субект s_i , който има достъп за четене до обекта o_j може да има достъп за писане до обекта p_k само, ако е изпълнено условието $C_j(o_j) \leq C_k(p_k)$. Това означава, че даден субект има право на запис в конкретен информационен обект, само ако обектът е ниво на класификация по-високо, отколкото е ниво на достъп на субекта (**no write-down**). По този начин се предотвратява осъществяването на запис в обект с ниско ниво на класификация от субект, който притежава достъп от високо ниво.

Въздействията на свойствата върху информационните потоци са показани на фигура 2, където нивата на достъп на субектите s_i и нивата на класификация на обектите o_i според са обозначени с техните позиции.



Фиг. 2. Схема на информационните потоци в съответствие с модела на Bell-La Padula.

3. Модел на Biba за контрол на достъпа

Моделът на Bell-La Padula се прилага само за поверителност на информацията: моделът идентифицира възможностите, които биха могли да доведат до компрометиране на информацията. Освен поверителността, цялостността на данните също е важна. “Цялостност” означава, че данните са защитени в достатъчна степен срещу неправомерен достъп и изменение. В [3] Biba предлага модел за предотвратяване на неподходяща промяна на данни.

Подобно на модела на Bell-La Padula, моделът на Biba използва обекти и субекти, но те са групирани в нива на цялостност, вместо нива на класификация.

С цел запазване на целостта, обектите могат да създават съдържание на или под тяхното собствено ниво на цялостност и да четат съдържанието на своето собствено ниво на цялостност или по-високо. Това предотвратява повреждане на данните и по този начин се запазва цялостността им.

Моделът на Biba има две свойства за сигурност:

- субект с дадено ниво на цялостност, не трябва да се чете обект с по-ниско ниво на цялостност (**no read-down**);
- субект с дадено ниво на цялостност, не трябва да пише в кой да е обект с по-високо ниво на цялостност (**no write-up**).

Моделът на Biba разглежда въпросът за цялостността, който моделът на Bell-La Padula игнорира, обаче игнорира поверителността.

4. Модел на Graham-Denning

В [4] Graham and Denning представят концепцията за формална система от права за защита. Модел оперира с множество от субекти S , множество от обекти O , с множество от права R и матрица за контрол на достъпа A . Матрицата съдържа един ред за всеки субект и една колона за всеки субект и всеки обект. Правата на всеки субект към друг субект или обект са показани чрез съдържанието на елементите на матрицата.

Моделът има осем примитиви на правилата за защита, показани в таблица 2.1. Тези права са формулирани като команди, които могат да бъдат издадени от субектите, с ефекти върху други субекти или обекти. Матрицата за контрол на достъпа е $A[s,o]$, където s е субект, а o е обект. Субектът, изпълняващ всяка команда е обозначен с x , прехвърляемо право с r^* и непрехвърляемо право с r .

Команда	Предварително условие	Ефект
Създаване на обект o		Добавяне на колона за o в A ; поставя собственик в $A[x,o]$
Създаване на субект s		Добавяне на ред за s в A ; поставя контрол в $A[x,s]$
Изтриване на обект o	Собственик в $A[x,o]$	Изтриване на колона
Изтриване на субект s	Контрол в $A[x,s]$	Изтриване на ред s
Право за четене на s над o	Контрол в $A[x,s]$ или собственик в $A[x,o]$	Копиране на $A[s,o]$ в x
Право за изтриване r на s над o	Контрол в $A[x,s]$ или собственик в $A[x,o]$	Премахване на r от $A[s,o]$
Предоставяне на право r на s над o	Собственик в $A[x,o]$	Добавяне r в $A[s,o]$
Прехвърляне на право r или r^* на s над o	r^* в $A[x,o]$	Добавяне r или r^* в $A[s,o]$

Таблица 1. Примитиви на правилата за защита

5. Модел на Harrison-Ruzzo-Ullman (HRU)

Harrison-Ruzzo-Ullman модела (наричан още матричен модел) се използва за анализ на системата за защита, реализиращ дискреционна политика на сигурност. Системата е представена от краен автомат, функциониращ в съответствие с определени правила на преход.

При използване матричен модел на достъп трябва да бъдат определени множества от субекти S , обекти O и разрешения R . Като субекти на системата се разглеждат изпълняващите се програми като се допуска, че $S \subseteq O$. Условието за достъп на субекта $s \in S$ към обекта $o \in O$ определя от матрицата на достъпа. Да предположим, множеството от права на достъп е право на четене (r), писане (w), изпълнение (e). Забраната ще съответства на празен набор от права на достъп ($\emptyset$). Тогава матрицата за достъп може бъде следната:

	O_1	O_2	O_3	O_4
S_1	rwe	$\emptyset$	rw	rw
S_2	e	rwe	r	$\emptyset$

Тук се предполага, че обектите O_1, O_2 са изпълними файлове, които, след като стартирането станат субекти S_1 и S_2 .

При описването на системи с голям брой обекти и субекти, размера на матрицата на достъпа силно нараства. За да се намали, еднаквите по права субекти и свързаните с тях обекти, могат да бъдат организирани в групи и да се дава разрешение за група субекти върху група обекти.

Функционирането на системата се разглежда по отношение на промени в достъпа на матрица. Моделът идентифицира шест примитивни операции: създаване на субект, създаване на обект, унищожаване на субект, унищожаване на обект, даване на право, отнемане на право;

Началното състояние на системата се описва с помощта на множествата от права на достъп R , субекти S , обекти O ($S \subseteq O$, мощността на тези комплекти $|S| = i$, $|O| = j$, $i \leq j$), матрицата на достъпа M_{ij} (елемент на матрицата, съответстващ на субекта s и обекта o , означен с $M[s,o]$ и е подмножество на множеството на права за достъп). Крайното състояние (след операцията) е S', O', M', R (множеството от права на достъп не се променя).

От примитивните оператори могат да се изграждат команди. Командата се състои от две части: условията, при които тя се извършва, и последователност операторите.

Общ вид на командите:

```
command name( $o_1, o_2, \dots, o_k$ )
    if  $r_1 \in M[x_{s1}, x_{o1}]$  and ... and  $r_m \in M[x_{sm}, x_{om}]$  then
        op1;
        ...
        opn;
    end,
```

където $r_1, r_2, \dots, r_m \in R$ – права на достъп, $op_1, \dots, op_n$ – последователност от примитивни оператори. При изпълнение на командите системата преминава от състояние Q в ново състояние Q' , при това, ако само едно от условията на командите не бъде изпълнено, $Q = Q'$.

Една система се нарича монооперационна, ако всяка команда съдържа само един примитивен оператор.

Два резултата, получени от Harrison, Ruzzo и Ullman са от особена важност за проектантите на системи за защита:

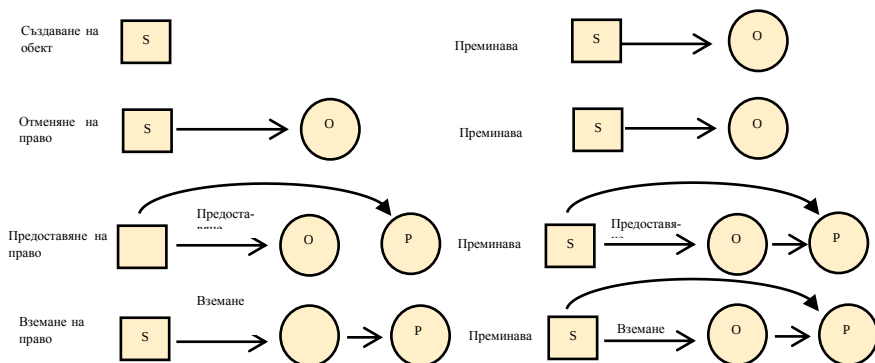
- в моделирана система, в която всички команди са ограничени до една операция, е възможно да се реши дали даден субект може да получи конкретно право на обект;
- ако командите не са ограничени до една операция, то не винаги е решимо дали една система за защита може да наложи дадено право. Следователно, не може да се определи като цяло дали даден субект може да получи конкретно право на един обект.

По този начин, от една страна, на общия модел на Harrison-Ruzzo-Ullman може да изрази голямо разнообразие от дискреционни политики за достъп, но не съществува алгоритъм за проверка на тяхната сигурност. От друга страна, може да се предпочете монооперационна система, за които съществува алгоритъм за проверка за сигурност, но този клас системи е прекалено тесен. Например, монооперационна система не може да изрази политика даваща права на субекти върху създаваните от тях обекти, тъй като не съществува една единствена операция, която да създаде един обект и едновременно с това да го маркира като собственост на създателя му.

6. Модел на Jones (take-grant)

Моделът има четири основни операции: създаване, отменяне, вземане и предоставяне. Създаването и отменянето са подобни на модела на Graham-Denning; вземане и предоставяне са нови видове операции [6].

Нека S е множество от субекти, O е множество от обекти и R е множество от права. Всеки субект или обект е обозначен с един възел на графика; правата на даден субект над даден обект са надписана насочена стрелка от субекта към обекта. Нека s е обект, изпълняващ всяка една от операциите. Ефектите на тези операции са показани на фигура 3. Четирите операции са –създаване на обект – **create(o,r)**, отнемане на право – **revoke(o,r)**, предоставяне на право – **grant(o,p,r;** и вземане на право – **take(o,p,r)**.



Фиг. 3. Създаване на обект, отменяне, предоставяне и вземане на право

7. Модел за контрол на достъпа с използване на роли

В концепцията на модела за контрол на достъпа с използване на роли понятието "обект" се заменя с понятията "потребител" и "роля". Потребител – човек, работещ със системата и да изпълняващ определени задължения. Роля – активно действащ в системата абстрактен субект със съответен набор от необходими разрешения за извършване на определени дейности. Такова разделение добре отразява особеностите на дейността на различните организации. На един потребител може оторизиран от администратора да изпълнява една или няколко роли, както и една роля може да бъде съпоставена на един или повече потребители.

Разрешенията за извършване на определени операции са свързани със специфични роли. На потребителите на системата са назначени конкретни роли и чрез тях те придобиват разрешения за извършване на определени операции в системата. Тъй като на потребителите не се присвояват пряко разрешения, а ги придобиват чрез тяхната роля, управлението на индивидуалните права на потребителя се извършва чрез задаването на подходящи роли в профила на потребителя.

Дефинирани са три основни правила:

Назначаване на роля: субекта може да извърши действие само ако има назначена роля.

Оторизация на роля: активната роля на субекта трябва да бъде оторизирана за конкретния субект. Това означава, че субектите могат да приемат само роли, за които са оторизирани.

Оторизация на действия: субектът може да изпълни действие само ако действието е оторизирано за активната му роля.

Контрол на достъпа се извършва на два етапа:

- за всяка роля се определя набор от пълномощия (разрешения за различни обекти в системата);

- на всеки потребител се съпоставя списък с достъпните му роли.

При ролевия модел на контрол на достъпа се използват следните множества $[L_{22}]$:

U – множеството на потребители;

R – множеството от роли;

P – множеството от правомощия (разрешения) за достъп до обектите на системата;

S – множеството от потребителски сесии със системата.

Дефинирани са следните множества:

$PA \subseteq P \times R$ – определя множеството от правомощия за установената роля;

$UA \subseteq U \times R$ – задава съответствието между потребители и достъпните им роли.

Да разгледаме процеса на определяне на правата за достъп на потребителя, отквиващ сесия със системата (в една сесия работи само един потребител). Правила за контрол за достъп се определят с помощта на следните функции:

user: $S \rightarrow U$ – за всяка сесия $s \in S$ тази функция определя потребителя, който изпълнява тази потребителска сесия:

$user(s) = u \mid u \in U$

roles – за всяка сесия $s \in S$ тази функция определя подмножество от роли, които могат да бъдат достъпни едновременно за потребителя по време на сесията:

$roles(s) = \{ri \mid (user(s), ri) \in UA\}$;

permissions: $S \rightarrow P$ – за всяка сесия $s \in S$ тази функция определя набора от достъпните правомощия, които се определят по пътя на обединяването на правомощията на всички роли, участващи в тази сесия:

$permissions(s) = \bigcup_{r \in roles(s)} \{p_i \mid (p_i, r) \in PA\}$

За критерий за безопасността на модела се използва следното правило: системата се счита за безопасна, ако всеки потребител на системата, работещ в сесията $s \in S$, може да извършва действия, изискващи правомощия $p \in P$ само ако $p \in permissions(s)$.

Съществуват няколко вида ролеви модели на контрол на достъпа, различаващи се по функциите **user**, **roles** и **permissions**, и ограниченията, наложени на множествата PA и UA .

Например, може да се установи йерархична организация на ролите, в която всяка роля наследява разрешения на всички ѝ подчинени роли.

Могат да бъдат определени взаимно изключващи се роли – това са роли, които не могат да бъдат назначени едновременно на един потребител. Също така може да наложи ограничения върху едновременното използване на ролите в една сесия, количествени ограничения при възлагането на роли и пълномощия.

Заключение

При използване на моделите за сигурност възникват следните редица проблеми:

1. При моделите за сигурност съществуват теоретични ограничения. Не винаги може да се докаже, че даден модел изпълнява определени условия за сигурност.
2. модели за сигурност, основани на строги математически свойства могат да доведат до системи, които са напълно неизползваеми.
3. Изграждане на системи от строги математически модели за сигурност е изключително времеемко и скъпо. Повечето реални системи не се основават на формални модели.
4. Моделите за сигурност и формалните методи не установяват сигурност.

Дори когато един модел за сигурност доказва, че системата е сигурна, тя може да бъде уязвима. Човешкият елемент и социалното инженерство позволяват дори най-сигурните системи да бъдат компрометирани. Също така, механизми за сигурност, които е даден момент са смятани за сигурни, в бъдеще може да бъде установено, че са несигурни. Без значение е дали дадена система е доказано сигурна по модел, тя е винаги в опасност.

Разгледаните модели са разработени за справяне с различни проблеми със сигурността. Няма модел, подходящ за всяка ситуация, поради това са разработени редица различни модели. Дори един модел може да не е достатъчен, за да се поддържа един от аспектите на сигурността като конфиденциалността или целостта. Доказателство за това е моделът Biba, създаващ редица различни политики, които да се използват в зависимост от нуждите на системата. Някои политики са по-ограничителни от други, което води до един модел, който е лесен за използване, но по-малко сигурен. Моделът на Take-Grant от друга страна поддържа оторизирането на привилегии, които моделът Biba изключва. В повечето случаи ще са необходими повече от един модел, за да осигури изискваната сигурност.

Компютърна сигурност винаги ще бъде частично реакционен процес. Без знание активни мерки за сигурност са планирани и се използват, проблеми ще възникнат. Въпреки че звучи добре да се използва модел за сигурност, винаги ще има пробиви в сигурността. Дори модели, които са се смятали за сигурни, са по-късно било установено, че са уязвими за атаки. Моделът HRU е един такъв модел, който по-късно бе установено, че има слаби места, защото "теоретично не е решимо дали един модел с матрица на достъп е сигурен"[5].

Литература:

1. Backfield, J. , Network Security Model [онлайн], [прегледано на 06.03.2016] достъпно от: <https://www.sans.org/reading-room/whitepapers/modeling/network-security-model-32843>
2. Bell, David Elliott and LaPadula, Leonard J. (1976). "Secure Computer System: Unified Exposition and Multics Interpretation". MITRE Corporation.
3. Biba, K. J. "Integrity Considerations for Secure Computer Systems", MTR-3153, The Mitre Corporation, June 1975
4. Graham G., Denning P., Protection - principles and practice, AFIPS '72, spring joint computer conference, p. 417-429
5. Denning, D. "The Limits of Formal Security Models". National Computer Systems Security Award Acceptance Speech. October 18, 1999.

6. Jones, A. Protection Mechanism Models: Their Usefulness. in DeMillo. Foundations of Secure Computation
7. National Security Institute - 5200.28-STD Trusted Computer System Evaluation Criteria, 1985
8. Pfleeger, C. P., Security in Computing, Fourth Edition, Prentice Hall, 2006
9. Smyth N. Security+ Essentials, Payload Media, 2012

ВЪЗМОЖНОСТИ ЗА КОМПЮТЪРНА СТЕГАНОГРАФИЯ В ОБЛАЧНИТЕ ТЕХНОЛОГИИ

Веселка Т. Стоянова

НВУ „В. Левски”, Факултет „А. ПВО и КИС”

POSSIBILITIES FOR COMPUTER STEGANOGRAPHY IN CLOUD COMPUTING

Veselka T. Stoyanova

ABSTRACT: *The use of cloud computing has increased rapidly in many organizations. Security is considered to be the most critical aspects in a cloud computing environment due to the sensitive information stored in the cloud for users. The goal of cloud security is mainly focused on the issues related to the data security and privacy aspects in cloud computing. This project aspires to provide secured data sharing in cloud storage with the help of steganography concepts in addition with the sharing of aggregate keys between data owners and data users.*

KEY WORDS: *cloud computing, computer steganography, protect information, data sharing*

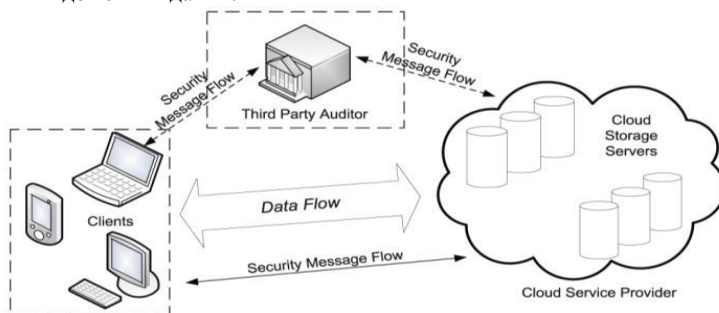
Увод

Развитието на модерните технологии води до бум в ежедневието ни и много устройства, които преди години са описани само в научно-фантастичните романи, сега са част от него. Доказано широкото разпространение на мобилните телефони, мобилните компютри и повсеместният компютинг дават възможност за лесно предаване на конфиденциални съобщения и разпространението на информация, която има личен или делови характер и не би трябвало да се разпространява в явен вид. Така възниква въпросът достатъчно защитени ли сме в интернет пространството. Кибератаките толкова са се усъвършенствали и нанасят множество щети, че се търсят всякакви възможности за решаване на проблема. Един от начините за борбата с киберпрестъпността и осигуряване предаването на тайни, конфиденциални съобщения е компютърната стеганография.

Естествена възможност за реализиране на компютърната стеганография вече се явяват облачните технологии. Облачната технология е модел, който прави възможен мрежовия достъп до споделени ресурси като интернет мрежи, сървъри, хранилища за масиви от данни и софтуерни приложения с минимално участие или управление от доставчика на услугата [3].

Нов и модерен начин за споделяне на информация е използването на облачните технологии. Именно там се открива възможност за споделянето на стегофайлове, които да бъдат достигнати без проблем от адресата и да бъде извлечена конфиденциалната информация от тях. Облачните технологии или изчисленията в облак са модел за предоставяне на информационни технологии под формата на услуга, а не като продукт [2]. Според редица организации Cloud Security Alliance (CSA), Cloud Computing Information Assurance Framework (ENISA), Information Security Forum (ISF) и др. част от основните заплахи за информационната сигурност на потребителите в облачна среда са свързани с: оторизирането на потребителя, шифриране на данните, физическата безопасност при работата на оборудването, „вреден“ трафик и др. [1].

На фиг. 1 е представено, как бива споделен файл в облака, като в него има скрито конфиденциално съобщение. Достатъчно условие за подсигуряване на защитата от извличане на конфиденциалната информация от неоторизирани за съответната комуникация наблюдатели е тя да бъде защитена с парола, която бива предавана по друг независим канал. Това разбира се не е достатъчно условие за предпазване от унищожаване на стегофайла и по този начин предпазване от загуба на данни. При такъв тип комуникация изцяло се разчита на факта, че има незабележимост на предаваните данни при визуален контрол, което е едно от предимствата пред криптографията, където факта за наличие на конфиденциална информация е явен. Счита се, че каналите за връзка и данните поместени в облака е по-добре да се шифрират. При обмен на данни по мрежата обикновено няма проблеми, тъй като доставчиците в повечето случаи предоставят достъп до данните по защитен протокол HTTPS. Проблеми възникват при контрол на данните в облака, което се дължи на използването на шифриране за всички акаунти с един ключ и страничният наблюдател успявайки да получи достъп до ключа, би могъл да получи достъп и до всички данни.



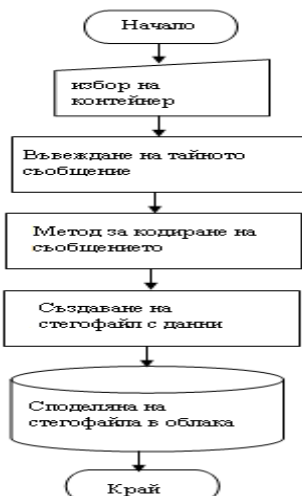
Фиг. 1. Споделяне на стегофайл през облака

Други възможности за предаване на тайни съобщения през Интернет са:

- Използване на социалните мрежи;

- Използване на електронна поща;
- Използване на Skype;
- Използване на Google Suggest;
- Използване на Wi-Fi безжични мрежи;
- Използване на BitTorrent като начин за споделяне.

Алгоритъмът за създаване и споделяне на стегофайла в облачно пространство е представено на фиг.2.

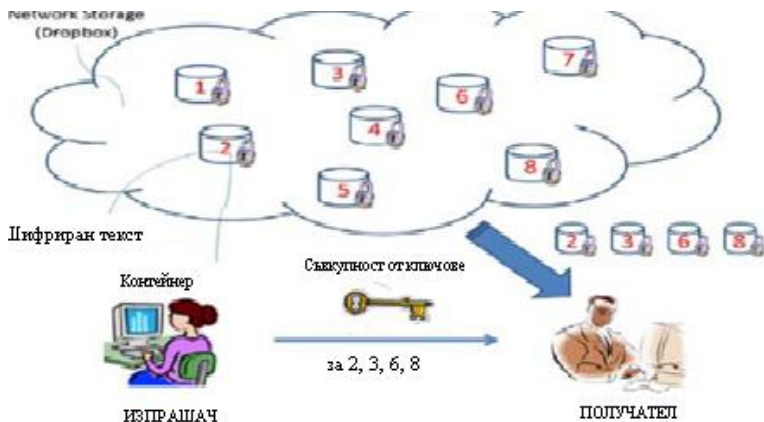


Фиг. 2. Блок-схема за вграждане на конфиденциална информация и споделянето ѝ в облачното пространство

Първоначално е необходимо да се избере контейнерът (прикриващият обект) в когото ще биват вградени конфиденциалните данни, след което трябва да се добавят самите данни. От особено значение е изборът на стеганографски метод за гарантиране на незабележимостта на вградените данни. Така полученият стегофайл вече може да бъде споделен в изчислителния облак и от там да бъде извлечен от адресата. Контейнерите, които се използват от мобилните стеганографски приложения за скриване на информацията, в по-голямата си част биват изображения, но съществуват и голям брой приложения, които използват звукови и видео файлове. Много от стеганографските приложения са платени и би могло да се използват след заплащането на съответният лиценз. Съществуват също така и безплатни приложения, като пример за такива са: „Hide it in“, „Acoustic Picture Transmitter Pro“, „Stegais“, „DaVinci Secret Image“ и други. Така изброените апове могат да бъдат сваляни от Google Play магазин. Информацията, която може да бъде предавана, може да е както текстово съобщение, така и снимка или пък дори и запис на гласово съобщение.

За да бъде успешно предаването на скрита информация задължително условие е потребителите, които я обменят да ползват едно и също приложение на мобилните си устройства, тъй като кодирането на информацията за всяко от тях, се реализира по свой собствен метод. Повечето стеганографски мобилни приложения предлагат лесен за употреба интерфейс и интуитивен подход за работа.

Особено важен е въпросът със споделянето на стегофайловете и предаването на ключовете, които гарантират, че информацията ще бъде извлечена само от получателя или притежателя на такъв ключ. На фигура 3 е предложена схема на стеганографската комуникация реализирана между изпращача и получателя на стегофайла и вграденото в него конфиденциално съобщение. От нея се вижда, че изпращача споделя съвкупност от стегофайлове и автоматично се генерират ключове, които биват изпратени по друг канал, които е различен от облачното пространство, в което са споделени стегофайловете.



Фиг. 3. Схема на предаване на конфиденциалното съобщение и съвкупността от ключове

Важно е да се отбележи, че много от синтезираните стегофайлове е възможно да не носят конфиденциална (полезна) информация и само малка част от тях да са носители. Това се прави с цел за заблуждаване на стеганализатора, както е видно и от фиг. 3 това са стегофайлове с номера 2,3,6,8, всички останали са споделени за да може да се реализира съвкупност от споделени в облачната технология файлове. Естеството на споделените стегофайлове трябва да е еднотипно и да не буди подозрение.

Облачните технологии откриват нови хоризонти за развитието на компютърната стеганография. Те позволяват една бърза, лесна, интуитивна употреба на приложения и споделянето на създадените стегофайлове. Възможностите за свободно споделяне и запазването на цялостната структура на стегофайловете позволява в реално време без обработка те да бъдат споделяни.

Заклучение

Бързо променящ се технологии от ежедневието ни и облачните технологии не са отговорът на всичките ни въпроси свързани със стеганографията, но са сред основните фактори за постигане на развитие в скритата комуникация, която тя предлага. Облачните услуги са лесно достъпни и за ползването им не се изискват допълнителни познания, услугите, които предоставят осигуряват среда за намиране на творчество не ограничавано от хардуерни, софтуерни или мрежови изисквания.

Сравнително нова като технология, стеганографията в облачните технологии се очаква да реализира стремежа за развитие и усъвършенстване.

Използвана литература:

1. Халачев П., Проблеми на сигурността при облачните услуги, E-Journal Mathematical Modeling and Computer Simulation Volume II, Number 6, Year 2014 (прегледано на 09.05.2016г.).
2. Plummer, D., et al. Cloud Computing: Defining and Describing an Emerging Phenomenon. Gartner Inc. 2008. p. 1–9.
3. <http://patetomahalnishka.weebly.com/1055108810771076108010841089109010741072.html> (прегледано на 09.05.2016г.).

СТУДЕНТСКО-ДОКТОРАНТСКА СЕКЦИЯ

ОБРАБОТКА НА АКУСТИЧНИЯ СИГНАЛ ПРИ ЛОКАЛИЗАЦИЯ НА ЗВУКОВИ ИЗТОЧНИЦИ

Филип Цв. Филипов

e-mail: filipov_filip@abv.bg, GSM: +359887633956

ACOUSTIC SIGNAL PROCESSING IN SOUND SOURCE LOCALIZATION

Filip Ts. Filipov

ABSTRACT: *This paper will discuss the acoustic signal processing using the Discrete Fourier Transform for preparing data for subsequent operations over them.*

KEY WORDS: *acoustics, digital signal processing, DFT*

В последните години населението на планетата живее в силно урбанизирани територии от градски тип. Военните действия вече не са на бойното поле и фронтната линия, а се водят в градските зони. Също така се забелязва нарастване на броя терористични актове в отдалечени от местоположението на военните действия силно урбанизирани зони. Затова в последните години можем вече да говорим за друг тип военни действия. Действия, при които нямаме реален противник, а противникът е до самите нас, анонимен и неразличим. В началото на 21 век се появи един нов термин – хибридна война. За първи път през 2005 г. военният автор и политолог Frank G. Hoffman използва термина хибридна война. Според неговата дефиниция за хибридна война, това е война, която комбинира участието на конвенционална и нерегулярна войска, с едновременни терористични и криминални акции. Според други автори, терминът хибридна война обединява бойни действия с използване на ядрено оръжие, химическо- и биологическо-оръжие, самоделни взривни устройства, информационно-психологическа война и манипулации.

При военни действия в урбанизирани територии използването на сензорни мрежи за откриване, проследяване и наблюдаване на цели може да се окаже най-доброто възможно решение. Сензорните мрежи могат да предоставят различен тип информация с цел точно и ясно локализиране на целта. Желателно е сензорната мрежа да бъде изградена предварително, като превантивна с цел отбрана, но също така трябва да има създадена възможност за бързо развързване на самостоятелна безжична сензорна мрежа, която би могла да се използва и при настъпление и при отбрана. Предварително изградената мрежа може да бъде разположена на стълбове, сгради, паметници, автобусни спирки, моторни превозни средства и други. Вече

има реализирана самостоятелна бързо развърщаема мрежа, като датчиците са разположени в облеклото и каските на войниците и съответно на автомобили оборудвани с датчици, както и на специално оборудвани за целта автомобили снабдени и със системи за анализ и решения в реално време. Възможно е решение с разпръскаеми датчици от самолет или друг носител.

При анализа и обработката на звукови сигнали често се работи, както с времените, така и със спектралните компоненти на сигналите. В този смисъл ще се разгледа един пример на спектрален анализ на звукови сигнали с помощта на достъпни технологии, [1]

Основата на спектралния анализ е ортогоналното разложение на дадена функция (сигнал) $s(t) \in \mathbb{C}^n$ за зададена в интервал от време T в ред на Фурие по тригонометричен базис. В комплексна форма за $t \in (-\frac{T}{2}, \frac{T}{2}]$ това е следния ред:

$$s(t) \sim \sum_{k=-\infty}^{\infty} c_k e^{-jk\frac{2\pi}{T}t}.$$

Ако сигналът $s(t)$ е зададен по цялата ос на времето за $t \in (-\infty, \infty)$, е периодичен, и е с крайна енергия, то спектралното представяне се реализира чрез интегралното преобразуване на Фурие (право и обратно):

$$g(\omega) = \int_{-\infty}^{\infty} s(t) e^{-j\omega t} dt,$$

$$s(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} g(\omega) e^{j\omega t} d\omega$$

Актуална е обработката чрез дискретното преобразуване на Фурие – ДПФ:

$$F_k = \sum_{n=0}^{N-1} s_n e^{-j\frac{2\pi}{N}nk} = \sum_{n=0}^{N-1} s_n W_N^{-nk}$$

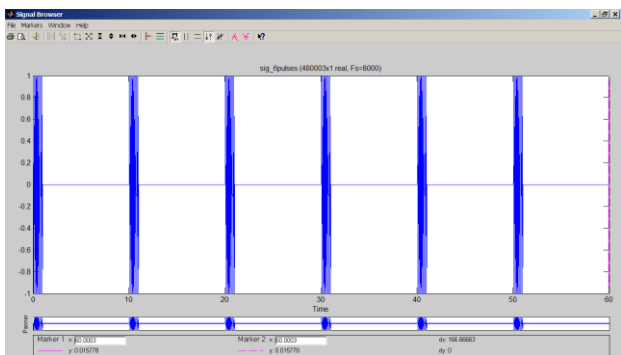
$$s_n = \frac{1}{N} \sum_{k=0}^{N-1} F_k e^{j\frac{2\pi}{N}nk} = \frac{1}{N} \sum_{k=0}^{N-1} F_k W_N^{-nk}$$

Тук индексите n за времето и k за честотата се изменят от 0 до $N-1$, а $W_N = e^{-j\frac{2\pi}{N}}$ е примитивен N -ти корен на единицата, [1,2,4,6].

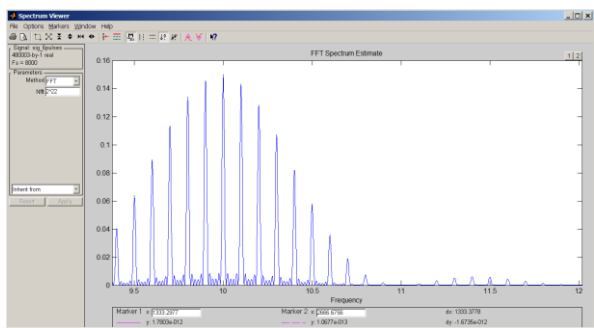
В началото ще се разгледат спектралните компоненти на серия от импулси модулирани с определена носеща честота. На фиг. 1а) и на фиг. 1б),в) са представени съответно сигнала във времевата (в случая от шест радиоимпулса) и в честотната област (т.е. пресметнато ДПФ чрез алгоритъм за бързо преобразуване на Фурие - БПФ), като на фиг. 1в) разделителната способност е повишена [3,5].

По подобен начин ще се анализира фрагмент от конкретен акустичен сигнал.

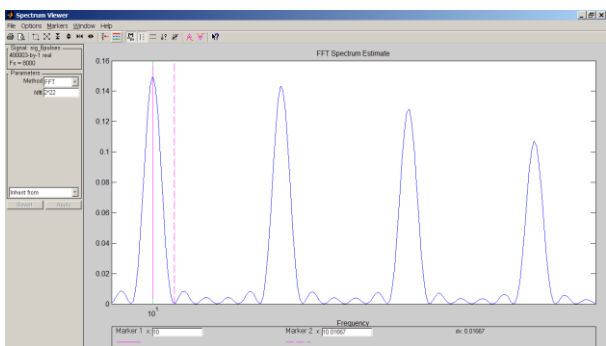
В предложената работа целта е да се анализират спектрални характеристики на регистрирани акустични сигнали, породени от артилерийска система .



Фиг. 1 а)



Фиг. 1 б)



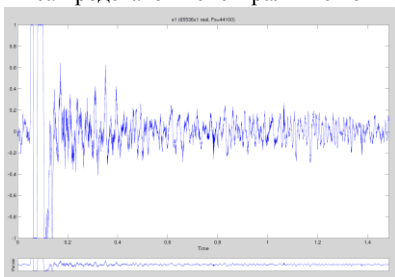
Фиг. 1 в)

Измерванията са направени през време на демонстративните стрелби на курсантите от Факултет „Артилерия, ПВО и КИС“ на Артилерийски стрелкови полигон „Марково“, 23 април 2015 г. Използван за регистриране бе вграденият микрофон на общодостъпен модел ноутбук Asus. Компютърът бе разположен на

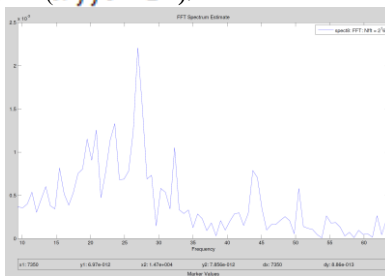
височина 50 см над повърността, на десет метра от публиката. Използваният за целта софтуер е Audacity (свободен лиценз).

От целия регистриран чрез Audacity сигнал, за анализ бе отделен фрагмент на звук от разрив, предизвикан от попадение при стрелба със 122мм самоходна гаубица 2С1. Изрязаният фрагмент е с продължителност 2 сек. Той съдържа звука присигнал от разрива, породените шумове от участващите персонал и машини и публиката и фоновия шум на местността. Честотата на дискретизация за всички примери подолу е $F_s = 44100\text{Hz}$. Ще бъдат анализирани най-силните спектрални компоненти.

На фиг. 2 е представена част от посочения сигнал, избрани са 2^{16} отчета, или във времето 1.49 сек. Пресметнато е ДПФ с прозорец на този сигнал, като на фиг. 2 са представени спектралните компоненти ($N_{fft} = 2^{16}$).



Фиг. 2. Регистриран звуков сигнал от разрив, предизвикан от попадение при стрелба със самоходна гаубица 2С1, на фона на околните шумове от участващите.

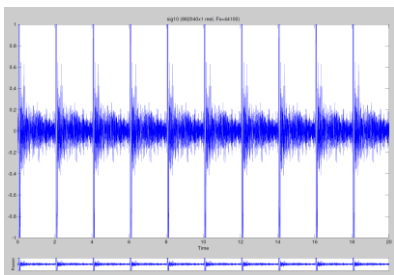


Фиг. 3. Спектрални компоненти на сигнала от фиг. 1 (DFT, $N_{fft} = 2^{16}$).

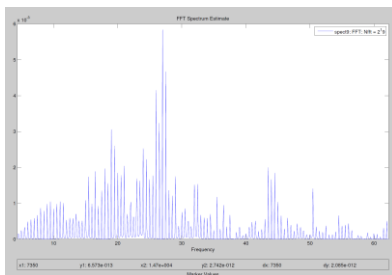
На фиг. 4 е представен повторен десет пъти фрагментът на сигнала, като отново е пресметнато ДПФ, ($N_{fft} = 2^{16}$) и е показано на фиг. 5.

На фиг. 6 е представена част от посочения сигнал, като тук с цел изолиране на шумовете по амплитуда, са приравнени на нула всички отчети, които по модул са под **0.7** от максимума. Отново е пресметнато ДПФ, $N_{fft} = 2^{16}$, фиг. 7.

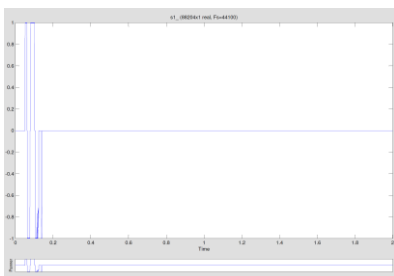
На фиг. 8 е представен повторен десет пъти фрагмента на сигнала, и с приравнени на нула всички отчети, които по модул са под **0.7** от максимума с цел изолиране на шумовете по амплитуда. Отново е пресметнато ДПФ, $N_{fft} = 2^{16}$, фиг. 9.



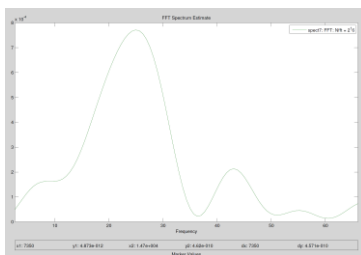
Фиг. 4. Повторен десет пъти звуковия сигнал от разрыв от фиг. 2.



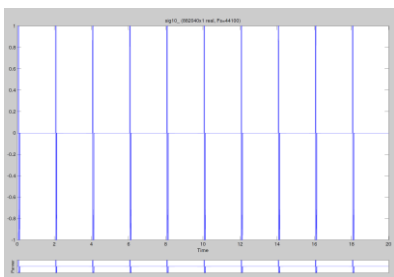
Фиг. 5. Спектрални компоненти на сигнала от фиг. 4 (DFT, $Nfft = 2^{15}$).



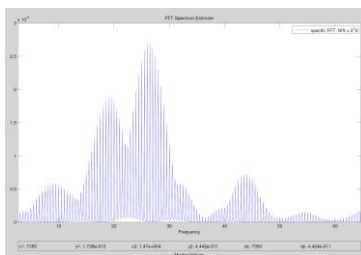
Фиг. 6. Звуковият сигнал от разрыв (без шумовите компоненти) от фиг. 2.



Фиг. 7. Спектрални компоненти на сигнала от фиг. 6 (DFT, $Nfft = 2^{15}$).



Фиг. 8. Повторен десет пъти звуковият сигнал (без шумовите компоненти) от разрыв от фиг. 2.



Фиг. 9. Спектрални компоненти на сигнала от фиг. 8 (DFT, $Nfft = 2^{15}$).

За много сигнали, нискочестотните компоненти са най-важната част. Тя дава идентичността на сигнала. Високочестотната част от друга страна придава окраска на сигнала. Човешкият глас, например звучи неповторимо благодарение на високочестотните съставки на сигнала. Ако се премахнат високочестотните съставки на сигнала, гласът звучи различно, но може да се разбере какво е казано. Но ако се премахнат в достатъчно висока степен някои от нискочестотните компоненти говорът става неразбираем.

Изводи: От разгледания пример се виждат възможностите за регистриране и обработка (Фурие анализ) на акустични сигнали с висок динамичен диапазон, които се предоставят от общодостъпни преносими компютърни системи.

Литература:

1. Michael Parker, „Digital Signal Processing 101” Everything you need to know to get started, Elsevier, 2010, pages 97-112
2. Димков Г., Ал. Алексиев, И. Симеонов, Т. Трифонов, К. Симеонов, Акустични изследвания на исторически ценни български камбани, Национална научна конференция по Акустика, София, България, 2008, 115-124 стр.
3. O. Rioul and M. Vatterli “Wavelets and Signal Processing” IEEE Signal processing magazine, pages 14-38, October 1991
4. Tihomir Trifonov, Georgi Dimkov, Rosen Dzhakov, Ivan Simeonov, Research and identification of valuable bells of the national historic and cultural heritage of Bulgaria, In Proceedings of the XXII Conference with International Participation "Noise and Vibration", Nish, Serbia, 2010, pages 103-107.
5. The Matlab Wavelet Toolbox, The Mathworks, Ink., Natick, MA, 1996
6. Т. Трифонов, И.С. Иванов Експериментално изследване на звукови отпечатъци на тактически оръжейни системи, Университетска годишна научна конференция 2014, НВУ “Васил Левски”, В. Търново, 3-4 Юли 2014г.

ПРОЕКТЪТ ЗА НАЦИОНАЛНА СТРАТЕГИЯ ЗА КИБЕР СИГУРНОСТ И ОТРАЖЕНИЕТО МУ ВЪРХУ ПОДОБРЯВАНЕ НА ЕФЕКТИВНОСТТА НА УПРАВЛЕНИЕТО НА ИНЦИДЕНТИ В ИНФОРМАЦИОННАТА СИГУРНОСТ

Владимир П. Крумов

vladimirkr_vd@abv.bg

THE DRAFT NATIONAL STRATEGY FOR CYBER SECURITY AND ITS IMPACT ON IMPROVING THE EFFICIENCY OF THE MANAGEMENT OF INFORMATION SECURITY INCIDENTS

Vladimir P. Krumov

ABSTRACT: In this report are discussed the objectives and measures set by the strategy to increase the efficiency and the security level of information resources. What results are described of the performance of activities in the various stages and their impact on improving efficiency.

KEY WORDS: information security, incident, incident management, efficiency

Развитието на информационното общество в Република България, от една страна, и увеличеният брой заплахи за сигурността на информацията, водещи до инциденти, от друга, поставят с особена острота въпроса за ефективното управление на инцидентите по информационна сигурност като един от възловите въпроси за осигуряване на защита на информационните ресурси на всяка една организация.

Съвременните заплахи са комплексни и динамични. Традиционните подходи като защитни стени (firewalls), системи за откриване на пробиви (IDS), анти-вирусни програми и традиционните методологии за отговор при инцидент, вече не са достатъчни, за да се справяме с постоянно нарастващите все по-чести атаки на недоброжелатели. Организацията днес се сблъскват с Комплексни устойчиви атаки (Advanced Persistent Threats (APTs)) и атаки от организирани престъпни групи. Те са добре подготвени и използват многобройни ресурси, за да проникнат и в най-добре защитените системи. Тези атаки не се извършват като изолирани опити, а те много често са част от дългогодишни кампании, насочени към ценна и чувствителна информация. От една страна, е необходимо компаниите да обогатяват своите познания за методите на заплахите, инфраструктурата и ресурсите, а от друга, да интегрират оперативна и стратегическа защита на информационните активи. Ето за това създаването на национална стратегия за киберсигурност е стъпка в правилната посока в борбата с нарастващия брой атаки свързани с информационните активи на организациите.

Стратегията е разработена от междуведомствена работна група създадена със заповед на министър – председателя на Република България. Тя набелязва цели и мерки за развитие в девет ключови области [1]:

1. Установяване и развитие на националната система за кибер сигурност и устойчивост
2. Мрежовата и информационна сигурност – фундамент на кибер устойчивостта
3. Защита и устойчивост на дигитално зависимите критични инфраструктури
4. Подобряване на взаимодействието и споделянето на информация между държава, бизнес и общество
5. Развитие и подобряване на регулаторната рамка
6. Засилване на противодействието на кибер престъпността
7. Кибер отбрана и защита на националната сигурност
8. Повишаване на осведомеността, знанията и компетентностите и развитие на стимулираща среда за изследвания и иновации в областта на кибер сигурността
9. Международно взаимодействие - кибер дипломация и оперативно взаимодействие

За постигане на набелязаните цели и мерки в стратегията действията са разделени на 3 последователни надграждащи се фази с заповядан срок на изпълнение: **иницииране, развитие, и зрялост.**

Фаза 1: Инициране и постигане на базов капацитет за кибер сигурност (2015-2016 г.)

Основна цел на дейностите е установяване на координиран подход и изграждане на обща национална рамка и принципи за развитие, национална стратегия и план за действие с пътна карта за развитие и приоритети, съгласувани с основните заинтересовани страни, преодоляване на изоставането в ЕС и НАТО и осигуряване на **базово ниво на информационна и кибер сигурност**. През този етап ще бъде постигната необходимата минимална информационна и кибер сигурност на ниво отделни организации и мрежи и реакция при кибер инциденти и атаки, като се реализират следните дейности:

- Финализиране на национална стратегия за кибер сигурност, национален план за изпълнението ѝ с пътна карта за период до 2020 година.
- Установяване на работещ модел за включване и ангажиране на всички заинтересовани страни за **координирани действия по развитие** и непрекъснато осъвременяване на стратегията, политиките и действията.
- Въвеждане и прилагане на **проектен подход** за управление на дейностите по изпълнение на националния план за кибер сигурност и методика за **приоритизиране** на дейностите и проектите, стартиране на проектите с най-висок приоритет или с неотложен характер.
- Създаване на **Национална координационно-организационна мрежа за кибер сигурност (НКОМКС)** по модела на **публично-частните партньорства (ПЧП)**.
- Определяне на роли, отговорности и способности за развитие на държавните и неправителствените участници, установяване на общ механизъм, **дефиниране на процеси и протоколи за взаимодействие и мониторинг** на кибер картината на национално ниво на базата на координирана мрежа от центрове за кибер сигурност (CERT/CSIRT и други органи) и борба с кибер престъпността, развитие и осигуряване на основен изискуем капацитет и способности и интегриране в **Националната система за управление при кризи** [2].

- Преглед на комуникационните и информационни системи в публичния сектор и **критичните инфраструктури** с национално значение по отношение на кибер сигурността, определяне на **минимални изисквания**, подготовка и приоритетно включване в мрежата **НКОМКС** на основни сектори от енергетиката, транспорта, банковия и финансов сектор, мобилни комуникации, както и на интернет доставчици, доставчици на електронни услуги и други от национално значение.

- Подготовка и провеждане на пилотни секторни национални учения/упражнения от типа на CyberShockwave [3] по формулата на ПЧП и в допълнение на упражненията в ЕС и НАТО.

Изпълнение на указанията и директивите на **ЕС и НАТО** за разработване на национална стратегия, план и действия по изграждане на капацитет и способности за справяне с кибер инциденти и кризи.

- Активизиране на **международните партньорства** и ефективното им използване за преглед и развитие на действащи национални точки и звена за оперативно и техническо взаимодействие, развитие на адекватни на международните изисквания капацитет и способности.

- Преглед и организиране (координиране) на наличния експертен и технически капацитет в държавни, неправителствени, академични и частни организации, изработване и валидиране на модел за мобилизиране и включването им в НКМК (национален капацитет за кибер сигурност). Установяване на система от стимули за развитие на общ капацитет в изследователски центрове, технологични паркове, фирми и неправителствени организации.

- Дефиниране на основните **изисквания, стандарти и модели** за проектиране и разработване на комуникационни и информационни системи за системите за държавно управление и администрация, съгласувани и препоръчителни и за бизнеса в посока „сигурност на дизайна“, „поверителност чрез дизайн“, „проектирана устойчивост“.

- Разработване на национална програма за осведоменост (awareness) и ангажираност към дейностите по кибер сигурността с всички слоеве на обществото.

Фаза 2: Развитие – от капацитет към способности (2017-2018 г.)

Развитие на организационен и национален капацитет и подготовка на различни нива – реализиране на **устойчивост на ниво организация/ведомство** и способности за реакция при кибер инциденти и кризи, засилване на дейностите по превенция. При изпълнение на предвидените действия ще бъдат постигнати следните резултати:

- Институционализиране на процесите за **мониторинг и взаимодействие** на **Национална координационно-организационна мрежа за кибер сигурност (НКОМКС)** и поетапно включване на секторни и индустриални центрове за кибер сигурност (CERTS/CSIRT и др.) - фокус върху приоритетни критични инфраструктури и пълната интеграция и осигуряване на функционирането на **Националната система за управление при кризи**.

- Осигуряване и усъвършенстване на адекватна правно - регулаторна рамка;

- Въвеждане на обща методика по оценка на рисковете свързани с кибер заплахи, анализ на уязвимости, въздействие и значимост, потенциални цели, съгласувани и в съответствие с тези в НАТО, ЕС, ООН, ITU.

- разработване на рамка за оценка на споделените кибер рискове по мрежите/вериги за доставка, и определяне на съответни отговорности.

- Развитие на капацитета на националните, секторни и ведомствени центрове за кибер сигурност (CERTS/CSIRT и др.) за следене на състоянието на комуникационните и информационни системи, ранно откриване на заплахи и излъчване в НКМК, както и способности за координирана реакция при кибер инциденти, атаки и кризи до неутрализирането им и предприемане на дейности по възстановяване.

- Развитие на капацитет за симулация на сложни кибер инциденти, атаки и кризи и провеждане на комплексни национални учения/упражнения от типа на Cyber Shockwave по формулата на ПЧП и в допълнение на упражненията в ЕС и НАТО. Организиране на учения с държавите от региона и други международни партньорски мрежи.

- Идентифициране на необходимост и развитие на технологичен и изследователски капацитет и способности в приоритетни области за държавата, гражданите и бизнеса – осигуряване на иновативна и съвременна база за електронни услуги (вкл. за електронно управление), надеждни електронни разплащания (вкл. мобилни), електронно здравеопазване, кибер защита/отбрана, и други възможни ниши за развитие на индустрия, научни и приложни изследвания.

Фаза 3: Зряло и кибер устойчиво общество (2019-2020 г.)

Постигане на ниво на зрялост което осигурява **кибер устойчивост на национално ниво** и ефективно взаимодействие и интеграция на международно ниво (ЕС, НАТО). Чрез ангажиране на всички заинтересовани страни, е планирано България приоритетно да създаде способности както в държавния, така и в частния и изследователския сектор в идентифицирани ниши за постигане на водещи позиции в региона и партньорските мрежи. Очаквани резултати от тази фаза са:

- Пълнен капацитет на **Национална координационно-организационна мрежа за кибер сигурност (НКМКС)** с постигнато ефективно взаимодействие със секторни и индустриални центрове за кибер сигурност (CERTS/CSIRT/CIRC и др.) и пълната интеграция в **Националната система за управление при кризи**, в системите на ЕС и НАТО и международни партньорски мрежи;

- Специализация и утвърждаване на България като водещ партньор в ЕС и НАТО в определени **приоритетни области** на базата на стимулиране и развитие на върхови технологии и процеси, свързани с кибер сигурността и икономиката на знанието;

- Успешно реализирани е-услуги и системи в държавното управление и бизнеса и разкриване на нови направления за развитие на бизнес в регионален и световен аспект;

- Установени специализирани изследователски и приложни центрове с уникални компетентности и технологична база за симулации, обучение, тестване и активна защита на ИКТ системи, системи за управление в индустрията и критични инфраструктури (Industrial Control Systems ICS, SCADA, други).

Реализирането на тази стратегия и изпълнението на 9 мерки и цели ще доведе до подобряването на ефективността на управлението на инциденти чрез създаване на структури на стратегическо и оперативно ниво които ще подобрят координацията а от там и ефективността между структурите в държавния и частния сектор и по точно:

- Развитие на технологиите – повишаване на ефективността при намаляваща цена;

- Сравнително лесно преодоляване на технологична изостаналост;

- Практически неограничен достъп до знание, ноу-хау, добри практики;
- Интензивно сътрудничество с партньорски служби от други държави;
- Привличане на неангажиран човешки ресурс (вкл. и от сивия сектор, хаке-ри, white hats и др.);
- Наличие на добре подготвени кадри с висше образование с ИКТ профил;
- Системно развитие на информационна култура в училищата;
- Повишаване заинтересоваността за информационната и кибер сигурност в компаниите, особено МСП.

Литература:

1. Национална стратегия за кибер сигурност „Кибер устойчива България 2020” – проект
2. Закон за управление и функциониране на системата за защита на националната сигурност (ЗУФСЗНС), 2015
3. Cybershockwave <http://bipartisanpolicy.org/press-release/cyber-shockwave-shows-us-unprepared-cyberthreats/>

ПРАВЕН РЕЖИМ НА ЗАЩИТАТА НА ИНФОРМАЦИЯТА В БЪЛГАРСКОТО ЗАКОНОДАТЕЛСТВО

Александър Данаилов Куманов Антонио Стоянов Чучуков

Национален военен университет „Васил Левски“, Факултет „Общовойскови“

LEGAL PROVISIONS OF PROTECTION OF THE INFORMATION IN BULGARIAN LEGISLATION

Alexander D. Kumanov

Antonio S. Chuchukov

National Military University “Vasil Levski”

ABSTRACT: *The report deals with the protection of information in Bulgarian legislation. It focuses on several fundamental rights of citizens –provision of the right to information, the establishment of the right to privacy and the realization of the right of access to public information.*

KEY WORDS: *right to information, right to privacy, right of access to public information*

1. Правният режим на защитата на информацията в българското законодателство е свързан с регламентирането на правото на информация като основно право на гражданите и с регламентирането на видовете публична информация и достъпът

до нея. Правата и свободите на човека произлизат от стабилността на човешката личност, от нейното достойнство и социална същност. [3; 96-98] Правото на информация е заложено в Конституцията на Република България. Всеки български гражданин има право да търси, получава и разпространява информация. Осъществяването на това право не може да бъде насочено срещу правата и доброто име на другите граждани, както и срещу националната сигурност, обществения ред, народното здраве и морала. Гражданите имат право на информация от държавен орган или учреждение по въпроси, които представляват за тях законен интерес, ако информацията не е държавна или друга защитена от закона тайна или не засяга чужди права./чл. 41/

От гледна точка на международното и националното право всеки човек е правен субект. Неговите действия представляват модели на поведение /правомерно или неправомерно/ и се разглеждат като юридически факти. Когато фактите се констатираат като осъществени реално те се отчитат като данни. Данните са установените реални факти и се отнасят до сведения от най-ниската абстрактност или сурови входни факти, които, когато се обработват създават един смислен резултат. Те съществуват в група данни или като самостоятелни данни, които имат количествени и качествени атрибути. Информацията съществува като преработен резултат на данни.

Личните данни са обект на защита и трябва да бъдат гарантирани. В днешния глобализиран свят личните данни се предават през все по-голям брой виртуални и географски граници, което налага да се определят личните данни като обект на защита при международните операции по обработване, както и при движението на данни през границите. В България действа Законът за защита на личните данни, приет през 2002 г., който има за цел да гарантира неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните.

След присъединяването си към Европейския съюз през 2007 г. българското законодателство поетапно започва да се съобразява с европейските директиви. [1;133] Европейската система за защита на правото на достъп до обществена информация се основава на Директивата 95/46 ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни.

Американска конвенция за човешките права от 1969 г. също установява право на информация. „Всеки има право на свобода на мисъл и изразяване. Това право включва свободата да се търси, получава и предава информация и идеи с всички средства, независимо от границите, както устно, така и писмено, чрез печатно издание, като форма на изкуството или по какъвто и да е друг начин по собствен избор”./чл.13/

2. Правото на личен живот е основно човешко право и основателна претенция на всеки човек. Смисълът на това понятие се търси едновременно като „усещане за нарушение”[“] и като „усещане за себе си”[“] като водеща нагласа за самоуважение[2; 219-223]. Правото на неприкосновеност на личния живот, се разглежда като нахлуване в личния живот, присъщо на засягане на личното достойнство. То се свързва с концепцията за свободата и уникалната индивидуалност на всички граждани. За-

щита на лична информация се явява цел за защита на правото на лична неприкосновеност.

Правото на неприкосновеността на личен живот е установено във Всеобщата декларация за правата на човека от 1948 г. "Никой не трябва да бъде подлаган на произволна намеса в личния живот, семейството, жилището и кореспонденцията, нито на посегателства върху неговата чест и добро име. Всеки човек има право на закрила от закона срещу подобна намеса или посегателства." /чл. 12/

Правото на личен живот е заложено и в Европейската конвенция за защита на правата на човека и основните свободи от 1950 г., по която България е страна. В нея се предвижда правото на зачитане на личен и семеен живот, на жилището и тайната на кореспонденцията. "Всеки има право на зачитане на неговия личен и семеен живот, на неговото жилище и тайната на неговата кореспонденция. Намесата на държавните власти в ползването на това право е недопустима освен в случаите, предвидени в закона и необходими в едно демократично общество в интерес на националната и обществената сигурност." /чл. 8/

През 1981 г. Съвета на Европа приема Конвенция за автоматизираната обработка на лични данни № 108. Тази конвенция отразява принципите за коректност към личните данни, като определя правила за трансгранично прехвърляне на лични данни и създава механизми за международно сътрудничество.

Конституцията на Република България обявява личния живот на гражданите за неприкосновен, като приема, че всеки има право на защита срещу незаконната намеса в личния и семейния му живот и срещу посегателство върху неговата чест, достойнство и добро име. /чл. 32/ Това право се доразвива чрез забрана за следене, фотографиране, филмиране, записване или подлагане на други подобни действия без знание или въпреки изрично несъгласие на лицето, неприкосновеност на жилището и тайната на кореспонденцията и на другите съобщения. /чл. 33 и чл. 34/

3. Достъпът до публична информация е свързан, от една страна, с предоставянето на обществена информация от страна на държавните органи, а от друга страна, до ограничаване на този достъп, когато се засягат национални интереси. Законът за достъп до обществена информация урежда правото на предоставяне на обществена информация на гражданите. Според неговите разпоредби „обществена информация е всяка информация, свързана с обществения живот в Република България и даваща възможност на гражданите да си съставят собствено мнение относно дейността на задължените по закона субекти. Информация от обществения сектор е всяка информация, обективирана върху материален носител, включително съхранена като документ, звукозапис или видеозапис, и събрана или създадена от организация от обществения сектор“. /чл. 2/

С право на достъп до обществена информация разполагат гражданите на Република България, чуждите граждани, лицата без гражданство и юридическите лица. При осъществяването на това право се налагат ограничения, защото то не може да бъде насочено срещу правата и доброто име на други лица, както и срещу националната сигурност, обществения ред, здравето на гражданите и морала.

Основните принципи при осъществяване правото на достъп до обществена информация са откритост, достоверност и пълнота на информацията; осигуряване на еднакви условия за достъп до обществена информация; осигуряване на законност при търсенето и получаването на обществена информация; защита на правото на

информация; защита на личните данни; гарантиране на сигурността на обществото и държавата.

Обществената информация се разделя на официална и служебна. Официална е информацията, която се съдържа в актовете на държавните органи и на органите на местното самоуправление при осъществяване на техните правомощия. Служебна е информацията, която се събира, създава и съхранява във връзка с официалната информация, както и по повод дейността на органите и на техните администрации.

4. Основната цел на Законът за защита на класифицираната информация, приет през 2002г., е предотвратяването на нерегламентиран достъп до класифицирана информация. Той е дефиниран като разгласяване, злоупотреба, промяна, увреждане, предоставяне, унищожаване на класифицирана информация, както и всякакви други действия, водещи до нарушаване на защитата ѝ или до загубване на такава информация. За нерегламентиран достъп се счита и всеки пропуск да се класифицира информация с поставяне на съответен гриф за сигурност или неправилното му определяне, както и всяко действие или бездействие, довело до узнаване от лице, което няма съответното разрешение или потвърждение за това.

Законът за достъп до класифицирана информация обвързва националната сигурност и достъпа до информация. Национална сигурност е динамично състояние на обществото и държавата, при което са защитени териториалната цялост, суверенитетът и конституционно установеният ред на страната, когато са гарантирани демократичното функциониране на институциите и основните права и свободи на гражданите, в резултат на което нацията запазва и увеличава своето благосъстояние и се развива, както и когато страната успешно защитава националните си интереси и реализира националните си приоритети. Това е уредено в чл. 2 от Закона за управление и функциониране на системата за защита на националната сигурност.

Държавна тайна е информацията, определена в списъка по приложение № 1, нерегламентираният достъп до която би създал опасност за или би увредил интересите на Република България, свързани с националната сигурност, отбраната, външната политика или защитата на конституционно установения ред.

Служебна тайна е информацията, създавана или съхранявана от държавните органи или органите на местното самоуправление, която не е държавна тайна, нерегламентираният достъп до която би се отразил неблагоприятно на интересите на държавата или би увредил друг правно защитен интерес.

ЗЗКИ се отнася до начина на опазване и защита на сигурността на информацията като предвижда нивата на класификация за сигурност на информацията, които се обозначават с гриф "Строго секретно"; "Секретно"; "Поверително"; "За служебно ползване". /чл. 28/

Информацията, класифицирана като държавна тайна, се маркира с гриф за сигурност:

- „Строго секретно“ - в случаите, когато нерегламентиран достъп би застрашил в изключително висока степен суверенитета, независимостта или териториалната цялост на Република България или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от възникване на непоправими или изключително големи вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред.

- „Секретно“ - в случаите, когато нерегламентиран достъп би застрашил във висока степен суверенитета, независимостта или териториалната цялост на Република България или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от възникване на трудно поправими или големи вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред.

- „Поверително“ - в случаите, когато нерегламентиран достъп би застрашил суверенитета, независимостта или териториалната цялост на Република България или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от възникване на вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред. Информацията, класифицирана като служебна тайна, се маркира с гриф за сигурност „За служебно ползване“.

В заключение може да се направи изводът, че правото на информация е регламентирано изчерпателно в българското законодателство. Спазени са основните принципи на международната защита на правата на човека. защитени са данни, свързани с гарантирането на националната сигурност в Република България.

Литература

1. European Union Law, Cambridge, University Press, 2006
2. Rosen J. The Unwanted Gaze: the Destruction of Privacy in America, 2000
3. Неновски, Н. Правата на човека. С., 1994

КОЛАБОРАЦИЯТА И ИНТЕГРАЦИЯТА МЕЖДУ ОБЛАЧНИТЕ УСЛУГИ С ИНТЕРНЕТ НА НЕЩАТА – СИГУРНОСТ И ЗАЩИТА НА ДАННИТЕ

Сунай А. Алиев

Станислав С. Станев

Email: sunay.aliev@yahoo.com

Email: stan_stanev@yahoo.com

COLLABORATION AND INTEGRATION BETWEEN CLOUD SERVICES WITH THE INTERNET OF THINGS – SECURITY AND DATA PROTECTION

Sunay A. Aliev

Stanislav S. Stanev

Email: sunay.aliev@yahoo.com

Email: stan_stanev@yahoo.com

ABSTRACT: This article aims to provide collaboration between cloud services and the Internet of Things, which is becoming increasingly relevant. Both concepts can have a major impact on how we build smart or smarter cities. Cloud computing represents the delivery of hardware and software resources on-demand over the Internet as a Service. At the same time, the IoT concept envisions a new generation of devices (sensors, both virtual and physical) that are connected to the Internet and provide different services for value-added applications. The data gathered from heterogeneous and distributed IoT devices can be automatically managed, handled and reused with decentralized cloud services.

KEYWORDS: cloud computing, open source, internet of things, smart cities, decentralized cloud, smart devices, security

1. Въведение

Краят на XX век и началото на XXI век са белязани с редица фундаментални промени, свързани с развитието на информационните технологии, появата на Интернет и преминаването към икономики, базирани на знания. Свидетели сме на явления като дигиталната революция и глобализацията. Информацията става ключов ресурс за всяка една страна, била тя положителна или отрицателна. Използването и манипулирането ѝ са в известна степен начин на представяне на реалността от технологични устройства, която ни заобикаля. Устройства, които са част от нашето ежедневие, начин на поведение и разбиране. С темповете на развитие и комерсиализиране на иновациите е възможно хората сами по себе си да се превърнат не само в потребители на технологията, но и част от самата нея, т.е. посредници между устройствата.

2. Същност на проблема

С навлизането на облачните услуги се откри възможност за разширяването на една нова индустрия, отново част от дигиталната революция – Интернет на нещата

(IoT-Internet of Things). Концептуално тези две технологии са коренно различни. Разполагат с напълно различни парадигми и начини на имплементиране. Според [5, 6] неуспорим факт е, че водещи компании като Microsoft, Intel, Apple, Google, Huawei, Amazon и т.н. (табл. 1) инвестират изключително големи финансови ресурси в изграждането и функционирането на модел, който интегрира облачните услуги с интернет на нещата като провежда една двупосочна колаборация между тях. От своя страна е посочено в [7], че технологични гиганти като Qualcomm, Arm Holdings, AMD т.н. (табл. 2) също се борят за пазара в отдела на микропроцесорите, които са ключът към управлението на устройствата от ново поколение. В резултат на настъпващите промени се създава взимосвързана екосистема на Интернет на нещата, поддръжката на обекти, мрежи, сензори, микропроцесори, машини, концентратори на данни и програми с високо ниво на изкуствен интелект.

Таблица 1

Име на компания	Абревиатура	Отдел
AMAZON WEB SERVICES	AMZN	Интернет на нещата приложим към облачните услуги – платформени или софтуерни
AT&T	AT&T	Интернет на нещата приложим към мрежови компоненти и оборудване
AXEDA	XEDA	Интернет на нещата приложим към облачни услуги - базирани на софтуерни колекции и анализатори на данни, генерирани от сензори и други устройства
DELL	DELL	Интернет на нещата приложим към ентърпрайз технологии
GE	GE	Интернет на нещата приложим към софтуерна платформа, която интегрира машинно генерирани данни с традиционни и облачни бази данни
GOOGLE	GOOG	Интернет на нещата приложим към ежедневни дейности в реални среди – домашни, административни, корпоративни и производствени
HP	HP	Интернет на нещата приложим към изграждането на споделени връзки от по-високо ниво в рутер и суитч устройства
IBM	IBM	Интернет на нещата приложим към M2M комуникации
INTEL	INTC	Интернет на нещата приложим към осигуряване сигурност на потребителя и данните, с които той оперира
MICROSOFT	MS	Интернет на нещата приложим към ежедневни бизнес дейности
FACEBOOK	FB	Интернет на нещата приложим към създаването на приложения от софтуерни компани
ORACLE	ORACLE	Интернет на нещата приложим към управлението на бази от данни
SAP	SAP	Интернет на нещата приложим към платформа за управление на мобилни приложения
QUALCOMM	QCOM	Интернет на нещата приложим към платформи с отворен код

Таблица 2

Производител	Абревиатура	Отдел
QUALCOMM	<i>QCOM</i>	Микропроцесорна техника за (IoT – интернет на нещата) устройства
ARM HOLDINGS	<i>ARMH</i>	Микропроцесорна техника за (IoT – интернет на нещата) устройства
INTEL	<i>INTC</i>	Микропроцесорна техника за (IoT – интернет на нещата) устройства
AMD	<i>AMD</i>	Микропроцесорна техника за (IoT – интернет на нещата) устройства
RED HAT	<i>RHT</i>	Микропроцесорна техника за (IoT – интернет на нещата) устройства
SIERRA WIRELESS	<i>Swir</i>	Микропроцесорна техника за (IoT – интернет на нещата) устройства
CISCO	<i>CSCO</i>	Микропроцесорна техника за (IoT – интернет на нещата) устройства
GOOGLE	<i>GOOG</i>	Микропроцесорна техника за (IoT – интернет на нещата) устройства
APPLE	<i>APPL</i>	Микропроцесорна техника за (IoT – интернет на нещата) устройства
IBM	<i>IBM</i>	Микропроцесорна техника за (IoT – интернет на нещата) устройства

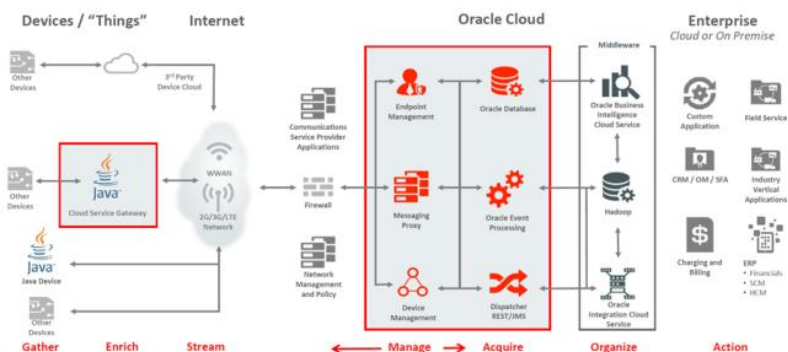
3. Теоретична постановка

След като облачните услуги вече са актуални и част от ежедневието ни, стана ясно, че е на лице необходимостта от сближаване им с интернет на нещата. Тази интеграция между двете технологии (фиг. 1), показва на информационното технологично общество единствено и само, че технологията е поема в правилната посока. Симбиозата между двете е необратима и е следващото стъпало към по-доброто потребление и използване на облачните услуги. В следствие на, което се стига до извода на това, че трябва този модел и парадигми да се съобразят и еволюират до етап на използване зелена енергия и енергия от възобновяеми източници. Причината за това е използването на голяма хетерогенна разпределена сензорна мрежа, огромен брой сензорни потоци. Друг начин е да има паралелно използване на облачните услуги от интернет на нещата. Тези облачни структури могат значително да увеличат изчислителната мощност на продуктите базирани на модела – интернет на нещата и комуникацията между тях. Според [8] на Фиг. 2 може да се види до колко високо е заложен принципа на хибридна в зависимост от колаборацията между двете технологии.



Фиг. 1

Облачните услуги реализират двупосочна връзка между няколко точки на комуникация: Анализ в реално време, Достъп до Облачна услуга и софтуерен програмен интерфейс. Три основни компонента комуникиращи си с дигиталните устройства и многокомпонентните обекти – образуващи интернет на нещата. За реализирането на подобрен комуникационен процес се изисква и висококачествена интернет скорост – 4G/LTE мрежа.



Фиг. 2

4. Проблеми със сигурността

След разглежданите модели на интеграция и колаборация на двете технологии възниква може би най-важният въпрос – Какво е положението със сигурността в цялостния процес? В [5] се твърди, че с развитието на технологията сигурността ще е ключов фактор в използването на интернет на нещата. Всички устройства ще бъдат уязвими сами по себе си от към злонамерени атаки. Атаки, които са проблем и при осигуряването на защитата в облачните услуги. Всички устройства разполагат с уникални идентификатори и могат да предават информация и данни по мрежата. Трафикът е активен нон-стоп. В следствие на което комуникацията идваща от облачните устройства и услуги е използван принципа M2M (машина-към-машина), интелигентните енергийни мрежи и автоматизацията им. В Табл. 3 от [1, 2, 3, 4, 5] се посочват основните видове облачни атаки, които са в сила и за устройствата от тип - Интернет на нещата. Друг фактор са несигурните и не до там сложни потребителски пароли, които самите потребители задават при употребата на приложенияте, които са обвързани с устройства. Това ги прави лесни мишени за атака, извличане и манипулиране на лична, конфиденциална информация. По този начин достъпът и работата на приложенията се нарушава и устройствата могат да бъдат използвани по всички възможни начини с цел незаконни намерения.

Табл. 3

Име на атаката	Засегнати зони
DENIAL OF SERVICE	Хардуер IAAS, PAAS структури
CLOUD MALWARE INJECTION	Облачни инфраструктури
SIDE CHANNEL ATTACK	Облачни инфраструктури, мрежови достъп и комуникация
AUTOTHEMIFICATION ATTACK	Облачни инфраструктури, мрежови достъп и комуникация
MAN IN THE MIDDLE	Облачни инфраструктури, мрежови достъп и комуникация
AUDIO STEGANOGRAPHY	Облачни инфраструктури и мрежови комуникационен достъп
TARGETED SHARED MEMORY	IAAS, PAAS структури
PHISHING	Облачни инфраструктури, мрежови достъп и комуникация
BOTNETS	Облачни инфраструктури, мрежови достъп и комуникация
BACKDOOR CHANNEL ATTACK	Хардуер, IAAS, PAAS структури
FLOODING ATTACK	Облачни инфраструктури, мрежови достъп и комуникация
TRACEBACK	Облачни инфраструктури, мрежови достъп и комуникация
DATA STEALING PROBLEM	Облачни инфраструктури, мрежови достъп и комуникация
THEFT OF SERVICE	Облачни инфраструктури, мрежови достъп и комуникация
PORT SCANNING	Облачни инфраструктури, мрежови достъп и комуникация
ATTACK ON VIRTUALIZATION	Облачни инфраструктури, мрежови достъп и комуникация
STORAGE ALLOCATION AND MULTITENACY	Облачни инфраструктури, мрежови достъп и комуникация

От направеното проучване може да достигнем до следния извод. Интернет на нещата, изглежда, че може да бъде следващото голямо нещо в областта на техноло-

гии. В [6] се посочва фактът, че сме в ерата на индустрия за един трилион долара, индустрия с милиарди долари от капиталови инвестиции се инвестират в нея. Мрежови устройства в дома, офиса, както и вградени в инфраструктурата и производството ще направят света по-ефективен и по-добро икономически място. Както потребителите, така и производителите ще се възползват от по-голямата автоматизация, по-доброто събиране на информация и анализирането и, интуитивен потребителски интерфейс и дизайн. Кибер сигурност е фундаментът, който трябва да подсили облачните услуги и интернет на нещата. Трябва да ги приоритизира като модели и подмодели. [9] Твърди, че е възможно е и таргетиране на уязвимите точки с цел предефиниране на приоритетите на сигурност, които действат сега в момента. Намесват се и фактори от рода на – коя операционна система използват нашите устройства, като платформи и кои софтуерни услуги. Аспект, който малко потребители обмислят за важен. Ако производителят на съответната операционна система е допуснал грешки и оставил вратички образно казано за достъп и манипулиране на самата система и данните, които се съхраняват в нея – това я прави опасна за потребителя и за устройствата, с които тя си комуникира както и с облачните услуги, с които оперира. От своя страна пък това води до достъп и към останалите устройства, които са част от йерархията и структурата на облачните услуги и интернет на нещата.

5. Заключение

Докато този потенциал е на практика неограничен, има много притеснения около личния живот, сигурността и заплахата от хакери или злонамерени действия. И все пак, ако това е следващото голямо нещо, има редица компании, които инвеститорите могат да считат, освен за създатели на устройствата, но и за отговорни лица по пътя на имплементиране на сигурност и надеждност, при нормално потребление от страна на протребители. Те са крайната точка на действие и въздействие, и имат нужда от предоставена сигурност когато оперират с облачните услуги и интернет на нещата.

Литература:

1. Khalil , I., Khreishah , A., Azeem, M. Cloud Computing Security: A Survey
2. Singh, A., Shrivastava, Dr. M. Overview of Attacks on Cloud Computing
3. Siva, T., Krishna, E.S. P. Controlling various network based ADoS Attacks in cloud computing environment: By Using Port Hopping Technique
4. Zunnurhain, K., Vrbasky, V. Security Attacks and Solutions in Clouds
5. <http://www.zacks.com/stock/news/213862/how-to-invest-in-the-internet-of-things>
6. <http://www.computerworlduk.com/galleries/data/12-most-powerful-internet-of-things-companies-3521713/#13>
7. <http://www.investopedia.com/articles/investing/010915/internet-things-2015.asp>
8. <https://thecattlecrew.net/2015/12/06/introducing-the-oracle-iot-cloud-part-i-overview/>
9. <http://www.computerweekly.com/feature/The-internet-of-things-is-set-to-change-security-priorities>

ЗАЩИТАТА НА ОБЛАЧНАТА СИГУРНОСТ И АТАКИТЕ КЪМ НЕЯ

Дениз А. Еминов
Гюнер И. Зекерие

Селиме И. Хасанова
Синан Д. Ниязиев

Шуменски университет „Епископ Константин Преславски“
denyodeniz@gmail.com
sellhasanowa@gmail.com
guner.zekerie@abv.bg

DEFENCE OF CLOUD SECURITY AND ATTACKS AGAINST IT

Deniz A. Eminov
Gyuner I. Zekerie

Selime I. Hasanova
Sinan D. Niyaziev

ABSTRACT: *This work provides an overview of using cloud technology as a model that enables network access to shared resources such as internet networks, servers and software applications with little involvement or control of the service provider. The need to protect the clouds of attacks as cyber attacks, data leakage, data loss, exposure of confidential information to unauthorized access. Types of protection of the cloud, which are used as multiple encryption and protection software(antivirus), mechanisms for access control, and protection from malicious mobile code, etc.*

KEY WORDS: *steganography, information security, cloud computing, protection, cloud security, insiders, encryption.*

1. Сигурност в облачните услуги

Доверието и сигурността на облачните услуги не са нови теми за изследвания в областта на компютърните науки, но са едни от най-значимите. Доверието се обосновава със сигурността на клиента в облачната структура с това неговите данни да останат цели и неприкосновени. Сигурността също се изразява като вяра на клиента в организацията, в неговия морален интегритет, в надеждността на неговото функциониране, в ефективността на неговите механизми за сигурност в опита да спазва всички наредби и закони. Представата за сигурност се отнася за ситуация, в която всички възможни рискове са премахнати или доведени до абсолютен минимум. Според редица организации Cloud Security Alliance (CSA), Cloud Computing Information Assurance Framework (ENISA), Information Security Forum (ISF) и др. част от основните заплахи за информационната сигурност на потребителите в облачна среда са свързани с: оторизацията на потребителя, шифриране на данните, физическата безопасност при работата на оборудването, „вреден“ трафик и др. Сигурността на един облак зависи в голяма степен от избрания модел за управление на данните и приложенията.

Конфиденциалността се отнася само до упълномощени лица или системи, които имат възможност за достъп до защитени данни. Заплахата от компромисни

данни се увеличава в облака, което се дължи на увеличени брой устройства и приложения, които участват, което води до увеличаване на броя на точките за достъп. Ключов аспект на сигурността на информацията е цялостта. Цялостта на данните се отнася до защитата на данните от неототоризирано изтриване, изменение или измислица. Управлението и правата на предприятието над специфичните ресурси на предприятието гарантира, че ценни данни и услуги не се злоупотребяват, незаконно присвояват или открадват. Чрез предотвратяване на неототоризиран достъп, организациите могат да получат по-голямо доверие в цялостта на данните и системата [1].

Cloud Alliance Security (CSA) е организация с нестопанска цел, която насърчава използването на най-добрите практики, за да се гарантира сигурност в облачни среди. CSA е издала и Ръководство с препоръки за осигуряване на идентичности и сигурно управление на достъпа.

Противодействия против изтичане на данни:

Динамични пълномощията - представя алгоритъм за създаване на динамични пълномощията за изчислителни системи мобилен облак. Динамичните идентификационните данни променят стойността си, след като даден потребител се променя местоположението си или когато той е разменила определен брой пакети данни.

Цифрови подписи - предлага да се осигурят данни с използване на електронен подпис с RSA алгоритъм, докато данните се прехвърлят през Интернет. Твърди се, че RSA е най-разпознаваем алгоритъм и може да се използва за защита на данните в облачните среди.

Homomorphic криптиране - Техниката за криптиране може да се използва за сигурността на данните, докато те се прехвърлят в и от облака или съхраняват в помещението на доставчика.

Encryption техники за криптиране са били използвани за дълго време, за чувствителни данни. Изпращането или съхранението на криптирани данни в облака ще гарантира, че данните са на сигурност. Все пак, това е вярно, ако се приеме, че алгоритмите за криптиране са силни. Има някои добре познати схеми за криптиране като AES (Advanced Encryption Standard). Също така, SSL технология може да се използва за защита на данните. Освен това криптирането може да се използва, за да се спирането на нежелани атаки.

HyperSafe - Това е подход, който осигурява цялостен контрол на потока. Целта HyperSafe е да защитава hypervisors тип I, използвайки две техники: не-bypassable Lockdown памет, която защитава срещу страници на паметта да бъдат модифицирани.

Trusted виртуален център за данни TVDc - осигурява изолация и интегритет в облачни среди. Той групира виртуални машини, които имат общи цели в натоварвания именуван Trusted виртуални домейни (TVDs).

Mirage - виртуална система за управление на машино изображение в облак. Този подход включва следните защитни елементи: рамков контрол на достъпа, графични филтри и хранилище като услуга за поддръжка. Въпреки това, едно ограничение на този подход е, че филтрите не могат да бъдат в състояние да сканират всички зловредни софтуери или премахват всички чувствителни данни от изображенията [2].

2.1 Основни принципи на защита на личните данни

Непрекосновеността на личния живот е основно човешко право, получило своето международно признание в редица международни договори и документи, като „Всеобщата декларация на човешките права и основни свободи“, „Международен пакт за граждански и политически права“, „Европейска конвенция за защита на правата на човека и основните свободи“ и др. В рамките на ЕС са приети редица документи за регулиране на обработката на личните данни, поставящи конкретни изисквания за тяхната защита.

В световен мащаб се дефинират няколко основни модели за защита на личните данни [3]:

- Модел на централизирано законодателство - Предвижда съществуване на специален закон, уреждащ изцяло принципите на защита на личните данни в съответната държава. Възприет е в страните от ЕС, включително и в България.
- Модел на саморегулирането - Компаниите и фирмите сами определят правилата и ограниченията при обработка на личните данни (например, чрез етични или браншови кодекси). Подходът е ефективен при поддържане на общи (разпределени) бази данни и отдалечен достъп до информационните ресурси на отделни компании.
- Модел на индивидуална защита - Прилага се от индивидуални потребители на глобалната мрежа, които разчитат на собствени технологични средства (кодиране, шифроване, криптиране, прокси-сървъри, електронни пари, смарт карти и пр.), чрез които се осигурява необходимата конфиденциалност и ограничаване на достъпа до данните.

2.2 Информационна сигурност на приложенията

Информационната сигурност на приложенията е отговорност, която се разпределя в различно съотношение между доставчика и абоната, при различните модели на услугите – софтуер, платформа, инфраструктура[4].

При SaaS модела – голяма част от отговорността за личните ни данни се пада на доставчика. Той определя, внедрява и поддържа контрола и осигурява възможността да се проверява тяхната ефективност.

При PaaS модела – отговорността е споделена, като доставчикът предлага набор от механизми, които могат да бъдат внедрени от абоната.

При IaaS модела – отговорността за сигурността на приложенията е на абоната. Той сам определя какви механизми за контрол да бъдат внедрени и как ще ги управлява и наблюдава.

Криптиране – Доставчика интегрира необходимите механизми за криптиране и декриптиране на информацията и осигурява следните възможности[4]:

- Криптиране на информацията при предвиждането ѝ от и към облачната инфраструктура
- Доставчика осигурява криптирани сесии(SSL/TLS), тунели(SSL/IPSec) и защитени обвивки(SSH) за комуникиране на информацията през интернет мрежата.

Информацията е криптирана не само на входно-изходната точка, а и в облачната структура. Началото на криптираната връзка е информационната система на абоната, а края е приложението в облачната структура.

2.3 Сигурност на центъра за обработка на данни

Според [3] центъра за обработка на данни заедно с технологиите за виртуализация, мрежовите комуникации са основните елементи на една облачна инфраструктура. Това е мястото, където се намират всички хардуерни активи, върху които функционират управляваните услуги в облака и се осигурява физическа сигурност и се гарантира сигурността на обкръжението за хардуерните активи на облачканата инфраструктура.

2.4 Управление на идентичността и контрола за достъп

Според Съвремените облачни инфраструктури са немислими без стриктен процес за управление на идентичността и контрола за достъп (Identity and Access Management – IAM)[4].

- Динамиката при IAM в облака се свежда до:
 - o Осигуряване/премахване на идентичност
 - o Идентификация
 - o Федерация
 - o Оторизация
 - o Управление на потребителски профил
- Доставчика предлага различни технологии за автентификация
 - o One-Time Passwords – еднократни пароли
 - o Биометрични данни
 - o Tokens
 - o Смарткарти
 - o Цифрови сертификати
 - o Kerberos

2.5 Сигурност в облака от физическа гледна точка

Достъпа се ограничава само за упълномощени служители и също така всеки център за данни използва противопожарни, водни и електрически системи, осигуряващи физическата сигурност на данните и непрекъснатата работа на сървърите [5].

Вградени средства за информационна сигурност [3] (апаратни, програмни, криптографски) - съвкупност от апаратни, програмни и криптографски средства, които осигуряват най-висока степен на защита и се явяват последна преграда пред данните срещу опитите на външни потребители за неправомерен достъп до тях. Апаратните средства се използват за разпознаване на легитимния потребител, за защита на процесора и външната памет, за шифроване на предаваните съобщения и т.н. Програмните средства се прилагат при разпознаване на правилно въведена от потребителя парола или ПИН, за ограничаване на достъпа до части от диска, за проверка на наличие на вирусни програми и активиране на антивирусни програми и др. Криптографските средства се реализират апаратно или програмно, като осигуряват шифроване на данните със симетрични или асиметрични алгоритми. Използват се системи с различно предназначение – за засекретяване на необходимите данни и съобщения, за автентификация (проверка на достоверност), електронен подпис и пр.

Физически средства за защита – технически средства за предотвратяване на достъпа на външни лица до помещения с работни станции и сървъри на бази данни, заключване на информационни носители и архивни данни, въвеждане на отли-

чителни знаци, охрана и осигуряване на защитна сигнализация, сегментиране на локалната мрежа и изолиране на сървъра от Интернет, осигуряване на резервно запазване и др.

Организационни мерки за административен контрол – допълват и разширяват функциите на физическите средства за защита, като особено внимание се обръща на правилното използване на предвидените апаратни и програмни средства. Включват: периодични проверки на потребителския достъп до информационните ресурси и спазване на изискванията относно периодична смяна на паролите; съхраняване на копия на данните; дефиниране на нивото на секретност на данните и определяне на права на достъп на служителите; определяне на пълномощията на администратора на БД за контрол на достъпа до съответните данни; допълнителна квалификация на персонала и др.

Законови и нормативни средства за защита – най-външно ниво на системата за сигурност на личните данни, основаващо се на въведени специални закони, гарантиращи сигурността на компютърните системи и предвиждащи санкции за нарушителите.

3. Атаки в облачните услуги и облачните системи

Всяко злоумишлено действие на трети лица, което би застрашило данните или сигурността на облачните системи и услуги може да се нарича атака. Тези действия понякога са много организирани и могат да нанесът много големи поражения на облачните системи. Но атаките могат да бъдат няколко вида: за вреда, за кражба на информация или пренасяне на непозволена информация чрез клауд. Ето и някои видове атаки насочени към облачните услуги:

- **Denial-of-Service attack(DoS)** Cloud е по-пропускливи за DoS атаки, защото толкова много потребители са привлечени в използването на облачните услуги и ресурси, следователно DoS атаките могат да бъдат по-вредни. Когато има натовареност започне увеличаване на облачните изчисления, операционна система започне да предоставя повече изчислителна мощност под формата на повече виртуални машини, повече пуснати услуги, за да се справят с допълнителното натоварване. Така сървърът хардуерно слага граници за повече натоварване започва да слага ограничение. В този смисъл, системата Cloud се опитва да работи срещу нападателя (чрез предоставяне на повече изчислителна мощност), но актуално това е голям проблем защото се позволява на нападателя да си направи възможно най-много щети от наличността на услуги, като се започне от единна входна точка и се стигне до засягане на абсолютно всичко. По този начин, нападателят не трябва да засяга всички н сървъри, които осигуряват определена услуга в целта му, той просто залива един-единствен, после всички Cloud-базирани адрес, за да се извърши пълна загуба на наличността на желаната услуга.

- **CLOUD MALWARE- INJECTION ATTACK** е първият значителен опит за атака, която се инжектира при изпълнение на зловредна услуга или виртуална машина в облака. Целта на зловредният софтуер в облака е да бъде така, че противникът да се интересува от това данните да бъдат верни, но пък да се включват изменения на данни, пълна промена във функционалността връщане на назад или блокиране изцяло. В тази атака противник създава своя собствена зловредна модулна услуга за изпълнение (SaaS или PaaS) или виртуална машинна инстанция (IaaS), и да го добави към системата Cloud. Основният сценарий зад Injection атаката на Cloud Malware е, че нападателят прехвърля манипулирани / грешни копия на

жертвите, които се обслужват например прави така, че зловредителят може да се постигне достъп до заявки за услуги на жертвите, които се обслужване. За да се постигне това, атакуващият трябва да извлече контрол върху данните за жертвата в облака. Според класификация, тази атака е основният представител на използване на атака чрез повърхностна услуга до облак.

- **Side Channel attack** Един хакер се опитва да компрометира системата на облака чрез поставяне на зловредна виртуална машина в близост подобие на системата мишена облачен сървър и след това дебютира Side Channel attack. Side Channel attacks са като един вид ефективна заплаха за сигурността, представлява насочена система за прилагане на криптографски алгоритми . Ето защо е важно да имаме защитена система за проектиране . Side Channel attack използват две стъпки, за да създават атаки VM CO - Residence и настаняването т.е. „, атакуващият често може да поставя своя инстанция на същата физическа машина като целева инстанция и VM Extraction т.е. , способността на зловреден софтуер да използва странични канали, за да се науче информация за ко - резидентни случаи.

- **Authentication attack** е слаб за виртуални услуги и е много често целенасочено. Там има толкова много начини за удостоверяване на потребителите, които могат да се основават на това, което един потребител знае. Най- честите механизми и методи, които се използват за осигуряване на процеса по удостоверяване са насочени най-вече от нападатели. Неотдавна, по отношение на архитектурата на облачните изчисления, SaaS, IaaS и PaaS, има само IaaS, която е в състояние да предложи този вид защита, информация и криптиране на данните. Ако на предаваните данни конфиденциалността им е висока във всяко предприятие, обслужването на облачните изчисления въз основа на IaaS архитектура ще бъде най-подходящ и възможно решение за сигурно предаване на данни. В допълнение, разрешението на процес или управление на данни за тези данни принадлежи на предприятията, но се съхраняват от страна на доставчика на услугата трябва да бъде разрешено от страна на потребителя (предприятия), вместо услуга на доставчиците.

- **Man-In-The-Middle Cryptographic Attacks** Тази атака се извършва, когато атакуващият се поставя между двама потребители. По всяко време от страна на атакуващите има опит да се поставят на пътя на комуникациите, има възможност те да могат да се намесят и да модифицират комуникациите между двамата потребители [6].

Източници:

1. http://mmu2.uct.edu/mmjournal/files/6_1_P%20Halachev_cloud%20surveces.pdf
2. <http://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5>
3. <http://nauka.bg/a/пазпределено-информационно-обслужване-и-защита-на-личните-данни>
4. <http://www.slideshare.net/danielachudomirova/security-in-cloud-computing-17857629>
5. <https://www.securityforum.org/tool/supplier-security-evaluation-tool-sset/>
6. Shikha Singh, Binay Kumar Pandey, Ratnesh Srivastava, Neha rawat, Poonam rawat, Awantika(2014r.). Cloud Computing Attacks: A Discussion With Solutions. OPEN JOURNAL OF MOBILE COMPUTING AND CLOUD COMPUTING

ЗАЩИТА НА ИНФОРМАЦИЯТА В ОБЛАЧНИТЕ ТЕХНОЛОГИИ

Стефани А. Петкова

НВУ „В. Левски”, Факултет „А. ПВО и КИС”

PROTECTION OF INFORMATION IN CLOUD COPUTING

Stefani A. Petkova

ABSTRACT: *Cloud computing is a new vision about the needs of information technology (IT). It provides a comprehensive concept for building a homogeneous environment through services offered in the cloud – software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS).*

KEY WORDS: *cloud computing, SaaS, PaaS, IaaS, protect information*

Увод

Облачната технология е модел, който прави възможен мрежовия достъп до споделени ресурси като интернет мрежи, сървъри, хранилища за масиви от данни и софтуерни приложения с минимално участие или управление от доставчика на услугата.

С навлизането на този технологичен бизнес модел потребителите могат да достъпват тежки по отношение на разхода на ресурс приложения чрез леки преносими устройства като мобилни телефони, лаптопи и PDA устройства.

Облачните технологии преместват изчислителната мощ и информацията от десктоп компютрите и преносимите устройства в мега мощни дата центрове, което намалява разходите и формира нов по-гъвкав подход за правене на бизнес.

Облачните технологии имат много предимства за да бъдат предпочитано IT решение за организациите като най-важното от всички е преминаване към заплащане само на изразходваните ресурси като значително се намаляват или дори елиминират разходите за инвестициите в IT структура.

1. Същност на облачните технологии

Облачните технологии или изчисления в облак са модел за предоставяне на IT под формата на услуга, а не като продукт [1]. В основата му са залегнали идеите за споделеното използване на ресурси, заплащане според потреблението, непрекъснат достъп, лесна скалируемост и гъвкавост на използваните ресурси. Обработването на информацията и съхранението на данните са балансирано разпределени върху цялата инфраструктура на облака, без да има пряко назначаване на какъвто и да е ресурс към който и да е потребител. Основните групи участници в процеса са три – разработчици, доставчици и потребители на облачни услуги.

2. Облачни услуги

Предоставянето на ИТ като услуга е в основата на облачните технологии. За да бъде обхванат пълният спектър и за да бъдат напълно задоволени нуждите на потребителите в облачните технологии, се дефинират три нива на услуги [2, 9]:

- Инфраструктура като услуга (IaaS) заимства и доразвива идеята за виртуализация на дейта центровете, като осигурява на потребителите виртуална инфраструктура от сървъри и пространство за съхранение на данни. Най-популярният доставчик на инфраструктура като услуга е облака на Amazon – EC2.

- Платформа като услуга (PaaS) осигурява на потребителите среда, в която те могат да разработват своите приложения, като Windows Azure, Google App Engine, Apple iCloud и други.

- Софтуер като услуга (SaaS) предоставя на потребителите възможността да ползват през Интернет софтуерни продукти без да се налага да инсталират приложения на компютрите си.

3. Сигурност на информацията при облачните услуги

Важно значение при ползването на облачни услуги има осигуряването на защита на информацията, което е свързано с идентифицирането на заплахите и набяляване на възможните решения за осигуряване на информационна сигурност на данните и приложенията на потребителите в облачна среда насочване на усилията за преодоляването им в конкретни направления. Според редица организации Cloud Security Alliance (CSA) [3], Cloud Computing Information Assurance Framework (ENISA), Information Security Forum (ISF) и др. част от основните заплахи за информационната сигурност на потребителите в облачна среда са свързани с: оторизацията на потребителя, шифриране на данните, физическата безопасност при работата на оборудването, „вреден“ трафик и др. [4].

Оторизация на потребителя

При ползване на облачни услуги най-широко разпространен способ за оторизация на потребителите е защита с парола. Доставчиците осигуряват на потребителите по-висока надеждност, като прилагат и средства като сертификати и електронни подписи. Прилагат се стандартите LDAP (Lightweight Directory Access Protocol) [5], SAML (Security Assertion Markup Language) и др., които осигуряват взаимодействие на доставчика със системата за идентификация на потребителите и определяне на даваните пълномощия. Благодарение на това доставчикът разполага с актуална информация за оторизираните потребители. При ползване на облачни услуги потребителите могат да се свързват към данните или приложенията от всяка точка, където има интернет. Вместо стационарно работно място с точно определен набор от програмно осигуряване и местоположение (IP), потребителят може да се включи към виртуално работно място посредством IaaS, чрез използване на устройства като смартфон, тънък клиент и др.. Идентификационната информация предавана по мрежата за общо ползване може да бъде лесно прихваната. Правилата на достъп не трябва да се свързват към физическата топология, например към IP-адреса на потребителя или услугите. Затова безопасната идентификация, разграничаването на пълномощията (separation of duties) и контрола на всички събития е много важен, тъй като освен пряко увреждане на данните, може да има и кражба на данни. Администраторът управлява услугата, а данните са под контрола на организацията потребител.

Отделяне на данните на потребителите

Проблем при облачните технологии е отделянето на данните и приложенията от потребителите. Най-добър вариант е когато всеки потребител използва индивидуална виртуална машина (Virtual Machine – VM) и виртуална мрежа. Разделението на VM между потребителите се осигурява от хипервизори (хипервайзор или монитор на виртуални машини е компютърен софтуер, фърмуер или хардуер, който създава и управлява виртуални машини), а разделението между виртуалните мрежи се осигурява чрез прилагането на стандартни технологии като VLAN (Virtual Local Area Network), VPLS (Virtual Private LAN Service) и VPN (Virtual Private Network). Някои доставчици разполагат данните на всички потребители в единна облачна среда и чрез допълнителни приложения изолират данните на различните потребители. Такъв подход не е подходящ и не е надежден, тъй като от една страна е възможен пробив от хакери в допълнителните приложения, а от друга страна е възможно да има грешки, при които даден потребител случайно да види данните на друг.

Шифриране на данните

Повечето потребители считат, че каналите за връзка и данните поместени в облака е по-добре да се шифрират. При обмен на данни по мрежата обикновено няма проблеми, тъй като доставчиците в повечето случаи предоставят достъп до данните по защитен протокол HTTPS. При контрол на данните в облака обаче съществуват проблеми във връзка с използването на шифриране на всички акаунти с 1 ключ и хакерът получавайки достъп до ключа би могъл да получи достъп и до всички данни.

Освен това остават традиционните атаки, които биха могли да доведат до изтичане на информация - SQL injection, слаби пароли и др. Проблем при шифрирането на данните е разпределението на ключовете. Такава технология би било добре да е гъвкава и не свързана с конкретен доставчик на услуги. Най-популярно решение осигуряващо шифрирането на данните и управлението на ключовете е Trend Micro Secure Cloud, надстройка на Free OTFE и др., в които се използва специална технология позволяваща да се проверяват съвърите, да се контролира достъпа до затворени данни, да се отстранява ненужната информация без възможност за възстановяване. В случаи на смяна на доставчика на услуги, всички данни се пренасят без проблем и се поддържат от Amazon EC2, Eucalyptus и vCloud.

Hyper jacking

При предоставянето на допълнителни услуги с облачни технологии съвърите могат да бъдат лесно уязвими или пък неправилно настроени. Нерегламентиранят достъп до хипервизорите позволява да се контролират всички системи, работещи във виртуалните машини избягвайки многобройните системни защити. Една от специфичните хакерски атаки е получила името “hyper jacking”, което означава подмяна на хипервизорите с такива, които позволяват нерегламентиран достъп до предлаганите услуги. В същност заплахата за хипервизорите си остава хипотетична, тъй като за реализация на атака срещу тях е необходима висока квалификация, физически достъп до съвъръра, а също и процесор, който да поддържа виртуализация на апаратно равнище. Microsoft работят съвместно с водещи производители на процесори като Intel и AMD с цел разработване на средства за апаратна защита (шифриране на процесорно равнище) и намаляване опасността от hyper jacking.

Физическа безопасност

От особено значение при предоставянето на облачни услуги са мерките по физическа безопасност при достъп в центровете за данни. При облачните технологии все по-големи количества информация се концентрира на все по-малко физическо пространство, което прави центровете за данни още по-привлекателно място за проникване. Организацията Rackspace [6] определя някои стандартни мерки, които биха предотвратили възможността за получаване на информация на клиентите от чужди или подкупени свои сътрудници (биометрична идентификация, смарт-карти, видеонаблюдение, редовна проверка на журналите за достъп и др.). Организациите пренасочват своята ИТ-инфраструктура в облака, тъй като искат да постигнат по-голяма ефективност в управлението на данните си и да имат постоянен достъп до тях. В следствие на това се появява заплахата от липса на пълен контрол над данните и кой получава достъп до тях. Този проблем се опитват да решат организации, „стартъпи“, като Private Core и др. [7], целта на който е защита на данните непосредствено в процеса на тяхната обработка чрез апаратно осигуряване от трети страни. Дори данните да са шифрирани, то при тяхната обработка те трябва да бъдат разшифровани. Целта на Private Core е да отстрани необходимостта от разшифроване на данните или в крайна сметка да изпълни тази операция по най-безопасен начин. Private Core разработва собствен безопасен хипервизор, който позволява на клиента да управлява защитени виртуални машини, публична инфраструктура, използвайки технологията Intel TXT (Trusted Execution Technology - технология на доверения достъп на изпълнение). Безопасността се осигурява чрез шифриране на всички данни в паметта на физическата машина, като се оставя много малка сигнатура с възможност за атака. Данните се разшифроват и съхраняват в нешифрован вид само в кеш-паметта на процесора, който поддържа технологията на доверените изчисления. Така ако апаратната мощност на публичната платформа поддържа такива технологии, то организациите разполагащи своите данни в облака не зависят повече от мерките по безопасност на физическите сървъри – всички операции се изпълняват на виртуалните машини в зашифрован вид.

Подобна схема на организация на безопасност на сървърите има и торент-трекера The Pirate Bay. Допълнително преимущество е това, че изпълнението на жизнено важни операции с помощта на виртуални машини може да бъде пренесено на няколко отделни физически сървъри в различни райони на света. В случай на отказ на 1 от сървърите работата може да бъде пренесена бързо на резервен. По такъв начин системата става достатъчно устойчива към хакерски атаки. Въпреки това както и във всяка друга криптографска система сигурността зависи от качеството на кода на хипервизора, както и от липсата на грешки в системата за управление на крипто-ключовете.

Вреден трафик

Разполагането на услугите при доставчика усложнява задачата по осигуряване на безопасност при трафика между приложенията и виртуалната машина. Ако хакерите, намерят уязвимост в един виртуален компютър, могат с лекота да получат достъп и до останалите. Отсъствието на контрол при трафика може да доведе до изтичане на данни, заразяване с вируси и др. Възможен е вариант на разположение на всички виртуални машини, принадлежащи на 1 собственик на 1 физически сървър, но такава стъпка намалява ефективността от използването на ресурсите на сървъра. Много разработчици на антивирусни системи предлагат свои версии

продукти за защита на виртуалните среди. Например Kaspersky Security за виртуални среди не изисква разполагане на антивирусен агент на всяка виртуална машина, което способства за по-висока производителност на виртуалните машини на хост-сървъра.

Фалшива услуга

С цел привличане и повишаване на приходите и привличане на конфиденциална информация некоректни доставчици създават т.нар. „лъжливи облаци“ - Exploits as a Service (EaaS), поради което е необходимо при избор на доставчик, организациите да се доверяват само на проверени такива. Използват се и понятията “false cloud” или “cloud washing” [8], когато доставчикът на услуги се опитва да продаде във вид на облак услуги, който по своята същност не са облачни, а по-скоро са аутсорсинг или виртуализация. Когато обаче потребителят е платил само за използване на ресурсите, а не за лиценза има по-големи възможности по управлението на облачната услуга и по оптимизиране на основните операции за автоматизиране, той може да достигне необходимото равнище на мащабиране на услугата.

Бездействия VM

На неработеща виртуална машина е невъзможно да бъдат инсталирани и въведени в експлоатация програмни приложения за защита, поради което е необходимо да бъде реализирана защита на равнището на хипервизора.

Носене на лични вещи (Bring Your Own Device)

Все повече се увеличава тенденцията BYOD (Bring Your Own Device) – носенето на лични смартфони, таблети, лаптопи и др. от служителите на работа, което води до нарастване на рисковете към информационната сигурност на организациите. Причини за това са не добро управление на самото устройство, външна манипулация на софтуера и инсталиране на недостатъчно тествани и ненадеждни бизнес приложения.

Internet of Things

Приложението на технологията Internet of Things (IoT) и възможността на различни предмети, машини, превозни средства, животни, растения и хора, снабдени с уникални идентификатори, да се свързват и разменят данни помежду си, без това да изисква взаимодействието на човек към човек или на човек към компютър увеличава риска за сигурността на информацията. Технологията IoT все повече ще способства за увеличаване на броя на обектите, които се свързват към интернет чрез реално зададени IP адреси и размяната на информация помежду им. Проучвания показват, че до 20 години всеки един от нас ще бъде заобиколен от 3000 до 5000 свързани устройства. От една страна IoT ще способства за събирането и анализиране на големи обеми информация и ИТ автоматизация, но от друга все повече ще изисква повишаване на стандартите за сигурност на информация.

4. Облачни модели

Идентифицират се четири различни модела на облачните технологии според вида на предоставяне на услугата [9, 10]:

- Публичен облак - предоставяните услуги са достъпни за всички потребители, като могат да бъдат платени или безплатни.
- Частен облак - услуги се предоставят като споделени ресурси между различни отдели в рамките на една организация, която има пълен контрол върху данните и системите.

- Общностен облак - услуги се предоставят и използват от група потребители или организации, споделящи общи идеи и цели.
- Хибриден облак – при този модел се комбинират услуги предоставяни от публични и частни облаци.

Заключение

В днешния бързо променящ се свят облачните технологии не са отговорът на всичките ни въпроси, но са сред основните фактори за постигане на устойчиво развитие. Те изместват фокуса от предоставянето на продукт (сървър, софтуер или др.) към предоставянето на услуга. Благодарение на това се постига по-добро ниво на ИТ, като за това се използват в пъти по-малко от и без това ограничените ни ресурси. Облачните услуги са лесно достъпни и за ползването им не се изискват допълнителни познания. Предоставяните услуги осигуряват хомогенна среда за намиране на творчество, чието развитие не е ограничено от хардуерни, софтуерни или мрежови изисквания. В облака лесно и бързо може да се увеличи капацитетът или да се добавят технологии в движение, без да се инвестира в нова инфраструктура, обучение на служители или лицензиране на нов софтуер. Макар да са сравнително нова технология, облачните системи са реализацията на един дългогодишен стремеж за превръщане на ИТ в полезна и достъпна услуга. Използването и налагането на облачни технологии може и да не е на дневен ред за всички към настоящия момент, но е технология, чието развитие трябва внимателно да се следи и да се има предвид за в бъдеще.

Литература

1. Plummer, D., et al. Cloud Computing: Defining and Describing an Emerging Phenomenon. Gartner Inc. 2008. p. 1–9.
2. Marks, E., Lozano, B. Executive's Guide to Cloud Computing. John Wiley & Sons. Hoboken, New Jersey. 2010.
3. <https://cloudsecurityalliance.org/>
4. <http://www.enisa.europa.eu/>
5. [http://msdn.microsoft.com/en-us/library/aa367008\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/aa367008(v=vs.85).aspx)
6. <http://www.rackspace.com/blog/cloud-security-gets-physical/>
7. <http://privatecore.com/>
8. <http://www.cloudcomputinginsights.com/security/cloud-washing>
9. Rittinghouse, J., Ransome, J. Cloud Computing: Implementation, Management and Security. CRS Press. 2010.
10. Shubert, L., Jeffery, K., Neidecker-Lutz, B. The Feature Of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010. Expert Group Report – European Commission. 2010. p. 1– 66.

**НАУЧНА КОНФЕРЕНЦИЯ
с международно участие**

**ОБЛАЧНИТЕ СТРУКТУРИ
И ЗАЩИТАТА НА ИНФОРМАЦИЯТА**

СБОРНИК НАУЧНИ ТРУДОВЕ

Б ъ л г а р с к а . И з д а н и е п ъ р в о . Т и р а ж 3 0

Предпечатна подготовка - Факултет „Артилерия, ПВО и КИС“ - Шумен