НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ “ВАСИЛ ЛЕВСКИ”

ФАКУЛТЕТ “АРТИЛЕРИЯ, ПВО И КИС”

Катедра “Информационна сигурност”

М Е Ж Д У Н А Р О Д Н А
Н А У Ч Н А К О Н Ф Е Р Е Н Ц И Я

КИБЕРСИГУРНОСТТА В ИНФОРМАЦИОННОТО ОБЩЕСТВО

СБОРНИК НАУЧНИ ТРУДОВЕ

ШУМЕН
2017

КЪМ ЧИТАТЕЛИТЕ ...

Сборникът научни трудове е съставен от докладите, изнесени на научна конференция на тема „Киберсигурността в информационното общество", проведена във Факултет "Артилерия, противовъздушна отбрана и комуникационни и информационни системи" към Националния военен университет "Васил Левски" - гр. Шумен, на 20 и 21 април 2017 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

©НВУ "В. Левски" – Факултет "Артилерия, ПВО и КИС"
Шумен, 2017
c/o Jusautor, Shumen

ISBN 978-954-9681-82-6

СЪДЪРЖАНИЕ

ПЛЕНАРНА СЕСИЯ

ПРОАКТИВНО ИЗСЛЕДВАНЕ НА ХИБРИДНИ ЗАПЛАХИ В СЪВРЕМЕННАТА ДИГИТАЛНА РЕАЛНОСТ

Златогор Б. Минчев

Съвместен център за обучение, симулации и анализ, Институт по информационни и комуникационни технологии – БАН, E-mail: zlatogor@bas.bg

HYBRID THREATS PROACTIVE EXPLORATION IN MODERN DIGITAL REALITY

Zlatogor Minchev

Joint Training Simulation & Analysis Center
Institute of ICT, Bulgarian Academy of Sciences, E-mail: zlatogor@bas.bg

Abstract: *Modern digital reality progress is establishing a complex evolutionary process for the society, strongly influenced by joint interactions of technologies, environment and human factors. This emerges numerous innovative and future challenges with hybrid nature. The main idea of the present paper is to outline the identification, analysis and assessment of these new challenges into a holistic methodology, illustrated with some recent practical examples. The achieved results give a possibility for adequate support to human factor successful future challenges meeting in the new information age.*

Key words: *Digital Reality, Hybrid Threats, Proactive Research*

1. Въведение

Динамиката на съвременната дигитална реалност открива редица въпроси за нейното адекватно възприемане и използване [1], [2]. Еволюционните промени в отминаващото второ десетилетие на 21 век, поставиха човешкия фактор в принципно нова ситуация. От пасивен наблюдател в ерата на Уеб 1.0, днес, в навлизащата епоха на Уеб 3.0, обуславяна към момента от концепцията за „интернет на обектите“, свързвани по различни мрежови канали, той се превърна в активен потребител и разработчик на множество дигитални услуги и технологични решения [3]. Ситуация, за която катализатор са социалните мрежи от епохата Уеб 2.0 и бързия достъп до тях чрез по-съвършените и олекотени мобилни технологии. От друга страна развитието на софтуерната среда, позволи естествения достъп до програмни решения и платформи от високо ниво с отворен код (например: Java, Arduino, App Inventor, Unity), чрез които тази активна роля на човешкия фактор

стана лесно изпълнима. При цялата тази палитра от възможности промените в съвременната дигитална среда не спират дотук. Развитието на технологията на изкуствения интелект и полупроводниковата индустрия предоставя „интелигентни“ („смарт“) решения за работа, основани на вградени сензори и интерактивни 2D/3D визуализации, които посредством мултимедийна двупосочна комуникация, откриват нова ера от услуги в човеко-машинната интеракция [4]. Съвременните машини стават по-интелигентни и могат да намират автономни решения на различни задачи, в т.ч. и за независима междумашинна комунакация. Това посредством мултиплатформените, широколентови кабелни, сателитни, радио и мобилни комуникации, открива много възможности и ускорява общото темпо на живот.

Развитието на интерфейса, вече позволява създаването на смарт асистенти, притежаващи различни аватари и осигуряващи допълнителни функционалности, информация и услуги, вградени или достъпни чрез мобилните устройства, към вашия социален профил, дом, офис, транспорт.

Всичко това в комбинация с технологичните стремежи за по-висока интеграция на сензорните системи, вкл. до ниво имплантация (чрез технологии като NFC и RFID), изгражда една нова трансформирана реалност, смесваща все повече живата и неживата част от нашия свят в нова, многомерна дигитална реалност [5].

Създават се качествено нов тип комплексни заплахи с хибриден характер, получени като ефект от сблъсъка и интеракцията между човешкия фактор и технологиите.

Основната идея за проактивното им изследване, с използване на експертни прогнозни данни, модели и анализи, машинна валидация и смесена верификация, са представени накратко в следващия папраграф.

2. Методология на работа

Идейно, методологията е агрегирана около обща интерактивна рамка за човеко-технологично взаимодействие (вж. фигура 1), обхващаща четири основни етапа: (i) *Дефиниране на проблемното пространство*, (ii) *Анализ и оценка на заплахите*, (iii) *Машинна валидация на тенденциите*, (iv) *Интерактивна верификация*.

Фигура 1. Основна идея на методологията за работа, агрегирана около обща човеко-технологична интерактивна рамка за проактивно идентифициране на хибридна заплахи в дигиталното пространство.

Най-общо предложената методология за проактивна работа прилага метода на сценарийното планиране [6], използващ експертни и литературни данни за създаване на изследователска основа, която по-нататък се анализира на базата на структурен [7] и системен анализ [8].

Получените прогнозни класификации, по отношение на направените анализи, биват подложени на машинна стохастична валидация чрез идеите от [9], организирани около методи от типа „Монте-Карло“ с добавяне на елементи на случайност и моделно дефинирани критерии за точност.

Накрая, експертните прогнози, анализи и резултати от валидацията се верифицират и във въображаема интерактивна симулационна игра с реално използване на образци и прототипи на очакваните бъдещи технологични решения и ситуации. Така реакциите на участниците биват оценени многокретериално, като се постига и заключителна оценка на прогнозните очаквания за бъдещи хибридни заплахи и предизвикателства в трансформираната съвременна дигитална реалност.

В следващия параграф ще бъдат разгледани някои избрани практически резултати от предложената методология за работа, свързани с различните нейни етапи и области от очакваното развитие в дигиталната ера.

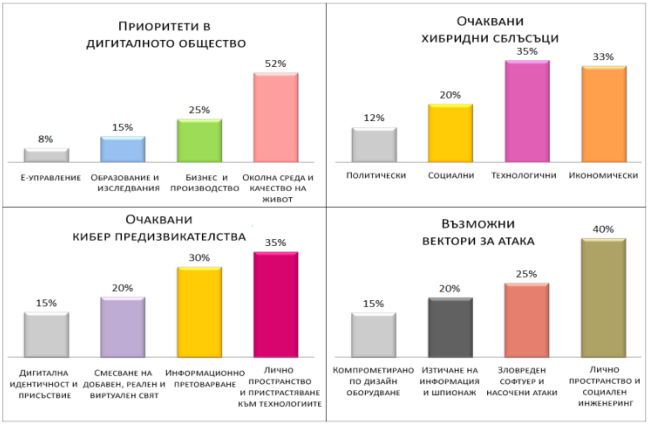
3. Избрани практически резултати

Предвид широкия обхват на предложената методология тук ще бъдат разгледани някои значими резултати от нейното поетапно прилагане, които са допълнително илюстрирани с актуални практически примери.

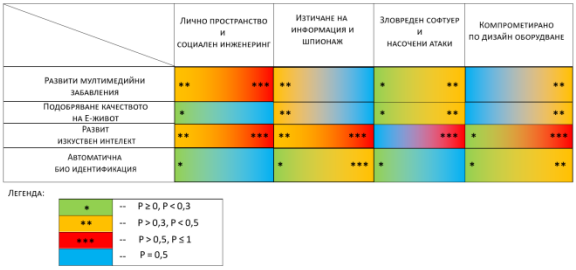
3.1. Дефиниране на проблемното пространство

Осъществяването на този първи етап се извършва на базата на обработка на експертни знания и литературни данни, извлечени с методи като „брейнсторминг“, „Делфи“ и др. [10].

Обобщаването на резултатите, може да бъде направено с различни статистически методи, в т.ч. и с вероятностно оценяване. Някои практически примери за това с използване на експертни и литературни данни за очакваната динамика в дигиталното общество до 2021 [11] и в частност – заплахите за „интернет на обектите“ [12] по отношение на очакваните вектори за атака са показани на фигура 2.



(a)



(б)

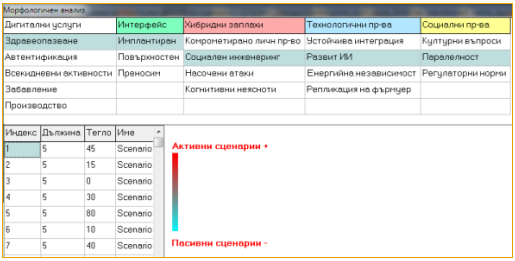
Фигура 2. Обобщена оценка на очакваната динамика в дигиталното общество (а) и вероятностно оценяване на заплахите за „интернет на обектите“ (б) по [11], [12].

Представените резултати, на този етап от прилагане на методологията, дават агрегирана, проактивна оценка на бъдещето в дигиталното общество до 2021, без да се отчитат динамиката на различните сценарии на развитие и възникващи при това, причинно-следствени връзки. В следващата част от настоящия параграф, този аналитичен въпрос ще бъде разгледан по-детайлно.

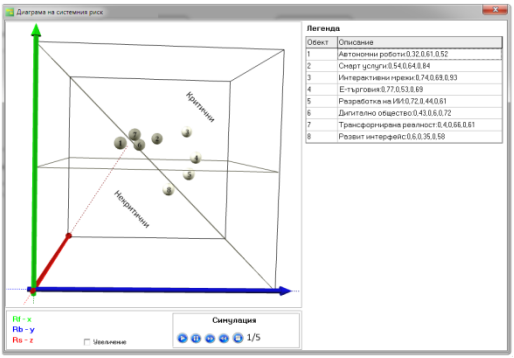
3.2. *Анализ и оценка на заплахите*

Осъществяването на този етап се извършва първоначално на базата на машинна интерпретация на „метода на сценариите“, като се прави цялостна оценка на динамиката в пространството на „възможното бъдеще“ [6]. То е представено като следствие от прилагането на структурен анализ и получаването на „матрица на кросконсистентност“, съдържаща взаимноизключващи се алтернативи, разпределени по измерения. Така биват идентифицирани два типа сценарийни комбинации (фигура 3а): „активни“ – директно управлаеми и „пасивни“ – индиректно управляеми [13].

По-нататък, за дадена сценарийна комбинация се създава системен модел, позволяващ холистична оценка на рисковете [12] и заплахите, интерпретиран на базата на двупосочен, претеглен граф, използващ подхода „обект-връзка“. Получените резултати се представят в 3D диаграма, оценяваща рисковете и заплахите в два базови класа: „критични“ и „некритични“ (фигура 3б). Тук ще отбележим, че могат да бъдат използвани и по-детайлни класификации [14].



(а)



(б)

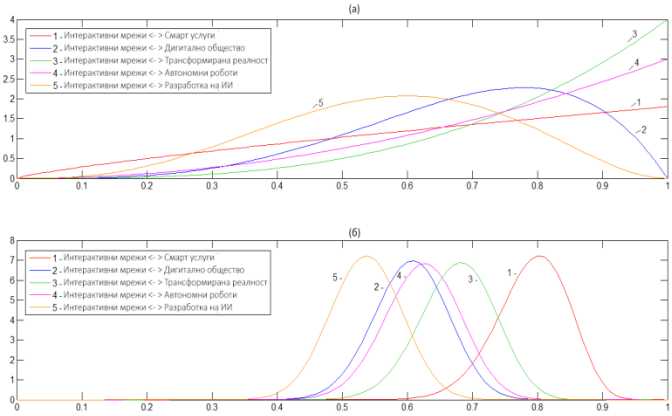
Фигура 3. Резултати от структурния (а) и последващия системен анализ (б) за оценка на динамиката в дигиталното пространство до 2021, по [14], [15].

Ще отбележим, че и двата анализа се реализират с експертно участие при използване на средата I-SCIP-MA-SA-RA [12] - [14], позволяваща бърза и интуитивна работа със силно зашумени входни данни и даваща интегрирана оценка на общата чувствителност в разработваните модели.

Предвид субективния и прогнозен характер на тези анализи, допълнително бе развит и метод за машинна валидация на тенденциите, който е разгледан накратко в следващия параграф.

3.3. *Машинна валидация на тенденциите*

Обективната оценката на прогнозни очаквания за бъдещето е сложен и противоречив процес, който се нуждае и от имплементирането на елемент на случайност. Практически, реализирането на тази идея е базирано на работите на Форестър върху социалната динамика [16], които са представени във вероятностен контекст [9]. Основната идея е да се направи прогнозна оценка на трендовете за бъдещ период, които по-нататък да се коригират чрез модел, използващ методи от типа „Монте-Карло“. В резултат от прилагането на тази идея се постига вероятностно оценяване на бъдещи тенденции за изследваните модели.



Фигура 4. Предварителна (а) и резултантна (б) оценка на тенденциите от модела на трансформирана дигитална реалност до 2021 в средата Matlab, по [17].

Представената идея за машинна валидация на аналитичните резултати от 3.1 и 3.2 дава добра основа за цялостна оценка на направените допускания. Предвид прогнозния характер на настоящите изследвания, тук може да бъде добавена и обща оценка на модела по трендове [13].

Важно е да се отбележи и необходимостта от верифициране на резултатите. Постигането на тази цел бе извършено чрез проиграване на част от изследваните ситуации в лабораторна среда с използване на технологични образци и прототипи в смесена дигитална реалност.

3.4. *Интерактивна верификация*

Реализацията на този заключителен етап се осъществява на базата на идеята за оценка чрез симулационни игри и компютърно подпомагании учения [18]. В дигиталната ера, това е важен момент свързан с реалното идентифициране, след експертните анализи и машинни симулации на нови и бъдещи хибридни заплахи. От съществено значение тук са човешкият фактор и технологичните иновации. Основната идея на този етап е да се оценят потребителските реакции на две нива: психо-физиологично и когнитивно. За целта се използват специализирани решения, отчитащи директно и индиректно динамиката в емоциите и поведението на участниците в интерактивната симулация. В последните три години (2015 – 2017) у нас експериментално се провеждат такива изследвания, в рамките на обучителния курс „Основи на сигурността в киберпространството“, към ПУ „Паисий Хилендарски“. Моменти от международното учение CYREX 2017, за изследване на рисковете и заплахите в дигиталното бъдеще на Уеб 4.0 са показани на фигура 5.

Фигура 5. Моменти от международното учение CYREX 2017 за изследване на дигиталното бъдеще [19].

CYREX 2017 бе организирано от Съвместния център за обучение, симулации и анализ, към Института по информационни и комуникационни технологии – БАН в кооперация с: IFIP, TC 14, ВА „Ген. Михайло Апостолски“, Р Македония, АКИС, УНСС-София. За общото времетраене от 180 минути бяха изследвани сценарии на индустриален шпионаж с използване на социален инженеринг и насосочени атаки от различен тип.

На разположение на участниците (над 30 души) бяха предоставени множество смарт устройства, експериментални средства за пресъздаване на трансформирана реалност и интелигентен био мониторинг в смесена мрежова среда. Оценка на действията на участниците бе извършвана и посредством наблюдение на реакционните времена и електронни анкетни листове.

Като цяло, отзивите за CYREX 2017 са позитивни, като участниците смятат че средата за работа е доста сложна, но много интересна. Това, според тях, изисква и удължаване на времето за симулация, с цел по-добро разбиране и адекватно реализиране на сложни атаки, като социалния инженеринг и действия от типа: декриптиране, вербуване и др. Допълнително, трябва да се отбележи и необходимостта от усвояване на новите технологични прототипи и услуги, които дори и интуитивни, предизвикват множество потребителски неясноти и въпроси.

4. Заключение

Съвременната трансформирана реалност генерира множество рискове, заплахи и предизвикателства с хибриден характер, породени от многопосочната интеракция между технологиите и човешкия фактор. Проактивното тяхно идентифициране е важен момент за повишаване на сигурността в дигиталната ера. Представената методология е разработена в рамките на над петнадесет национални и международни проектни партньорства за последните седем години. Като основен проблем в представените идеи за проактивно изследване е отчетено намаляването на субек-

тивността на човешкия фактор, който с развитието на технологиите в епохата на Уеб 3.0 и Уеб 4.0 се очаква да бъде отслабен с развитието на изкуствения интелект и неговото имплементиране в дигитално трансформираното ни ежедневие.

Литература

1. Floridi, L. The Fourth Revolution (How the Infosphere is Reshaping Human Reality), 1st ed., Oxford University Press, 2014

2. Schwab, K. The Fourth Industrial Revolution: What It Means, How to Respond, World
Economic Forum, May 9, 2017, Available at: https://goo.gl/e1Kc3F

3. Choudhury, N. World Wide Web and Its Journey from Web 1.0 to Web 4.0, Int.Journal of Computer Science and Information Technologies, Vol. 5, No. 6, Nov-Dec. 2014 , pp. 8096 – 8100

4. Boyanov, L., & Minchev, Z. Virtual Assisting Agents & Internet of Things, KSI Journal of Knowledge Society, no.1, pp.3-5, January, 2015.

5. Williams, A. & Nield, D. Where Phone Meets Body: How People are Making Themselves into Machines, Techradar, May 9, 2017, Available at: https://goo.gl/HPBSwl

6. Kosow, H., Gaßner, R. Methods of future and scenario analysis (Overview, assessment, and selection criteria), Deutsches Institut für Entwicklungspolitik, Bonn, 2008

7. Ritchey, T. General Morphological Analysis (A general method for non-quantified modelling), Swedish Morphological Society, 2002

8. Vester, F. The Art of Interconnected Thinking –Ideas and Tools for Dealing with Complexity, München: MCB–Verlag, 2007

9. Minchev, Z., Dukov, G., et al. Cyber Intelligence Decision Support in the Era of Big
Data, In ESGI 113 Problems & Final Reports Book, Chapter 6, FASTUMPRINT, 2015, pp. 85-92.

10. Popper, R. Foresight Methodology,In Georghiou, L., Harper, J., Keenan, M., Miles, I., Popper, R. (Eds.), The Handbook of Technology Foresight: Concepts and Practice, Edward Elgar Publishing, Massachusetts, 2008, pp.44 – 91

11. Minchev, Z. & Dukov, G. Emerging Hybrid Threats Modelling & Exploration in the New Mixed Cyber-Physical Reality, BISEC 2016, Belgrade, Belgrade Metropolitan University, October 15, 2016, pp. 13-17

12. Minchev, Z., Boyanov, L. Predictive Identification Approach for Emerging IoT Hybrid Threats, In Proceedings of ICAICTSEE – 2016, Sofia, UNWE, December 2 – 3, 2016 (in press)

13. Minchev, Z. & Shalamanov, V. Scenario Generation and Assessment Framework Solution in Support of the Comprehensive Approach, In Proc.of SAS-081 Symposium on Analytical Support to Defence Transformation, RTO-MP-SAS-081. Sofia: NATO RTO ST Organization, 2010, May 9, 2017, Available at: https://goo.gl/mFrWNd

14. Minchev, Z. Methodological Approach for Modelling, Simulation & Assessment of Complex Discrete Systems, In Proceedings of National Informatics Conference Dedicated to the 80th Anniversary of Prof. Barnev, IMI-BAS, Sofia, Bulgaria, 2016, pp. 102–110

15. Minchev, Z. Hybrid Threats Identification in the New Transformed Reality, In Proc. of 46 Spring Conference of UBM 'Mathematics & Education in Mathematics', Borovets, April 9-13, Bulgaria, 2017, pp. 194 – 200

16. Meadows, D., & Randers, J., Meadows, D., Limits to Growth: The 30-Year Update, Chelsea Green Publishing Company, 2004.

17. Boyanov, L. & Minchev, Z. Digital Transformation Disruptive Threats Identification, In Proc. of International Scientific Conference "Engineering. Technologies. Education.
Security", Veliko Turnovo, May 31 – June 3, 2017, Bulgaria (in press)

18. Minchev, Z. Cyber Threats Identification in the Evolving Digital Reality, In Proceedings of Ninth National Conference "Education and Research in the Information Society", Plovdiv, Bulgaria, May 26-27, 2016, pp. 011-022

19. Cyber Research Exercise – CYREX 2017 Web Page, https://goo.gl/sBvVWW

INFORMATION SECURITY: FORECAST FOR THE SUBCONSCIOUS INFLUENCE THROUGH INSTANT MESSAGING NETWORK

Col dr hab. Tadeusz Szczurek, prof. WAT
Lt dr Marcin Górnikiewicz

tadeusz.szczurek@wat.edu.pl
marcin.gornikiewicz@wat.edu.pl

Abstract: *The classically understood of information security focus only on technical protection of computer resources. Privacy is just one of the function to counter possible cyberattacks. In order to optimally effective protection against any form of cyber-aggression, it is worth to take to attempt to predict the possible forms of assault within the so called "cyberspace"*[1].

Technological development and interpersonal communication

Leap manifested in a dynamic and almost universal development of information technology has led to the emergence of a global information society, where people have gained the ability to instant exchange of data between each other. The revolution in communication technologies constantly evolving. Today, this leap applies only to external devices that enable the transmission and reception of data between users.

Anyone connected to the global network of information exchange automatically becomes vulnerable to various attacks. It could be an attack on a computer system or phone (which is essentially a miniature computer) or directly on the consciousness of the user. For the purposes of this article the authors proposed a simplified division into three areas of Internet activity, which are specific filters the access to information. For simplicity these mentioned areas hereafter referred to as "gates"[2].

Connecting to a network gives seemingly free access to information, but the huge amount of data processed in a fraction of a second makes the selection very hard, and in fact the "choice" of information depend on the various search engines. This is the first of the "gateways" through which the average user establishes network connectivity. The second gate is a variety of information portals (media, blogs, specialized), where media policy is more to chain user attention than following the facts. Consequently, the information served by so called "the information portals" can distort reality.

The last, the third "gate" is a process of exchange data directly between users, which in practice also does not guarantee reliability. Firstly, due to the fact that a person disseminates information that fit into his system of values. Thus, the message of users is

[1] M. Radochoński, B. Przywara (red.) *Jednostka-grupa-cybersieć. Psychologiczne, społeczno-kulturowe i edukacyjne aspekty społeczeństwa informacyjnego*, Rzeszów, WSIiZ, 2004, pp. 157-184.

[2] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, wyd. Fundacja Postępu Telekomunikacji, Kraków 1999, pp. 42-116.

one-sided, and obtained information also comes in large part from the "Internet". The third gate is the most dangerous for protection user consciousness against that kind of attack, because usually people trust other people they've known. So every intel from "social media friends" usually are more accepted that information from external media sources. These three gates: search engines, information portals and instant messaging are sources of information for any users via the Internet. In case of manipulation that types of intel transfers can be facilitated affect and distort the perception of the viewer. This mechanism has been used in recent years, both by the so-called. Islamic State (Daesh), as well as the separatists of Donetsk and Lugansk, and wider by Russian information warfare teams[3].

The authors attention has been focused on the third of the gates: instant messaging or the so-called. "social media"[4]. Currently, there is already a vast knowledge supported by lots of experimental studies, how to create information in order to gain attention of your audience, as well as the ability to impact on the consciousness and subconscious of users. It is worth to familiarize the scientific definitions of sub- and consciousness first, and next to present specific methods of influence.

Consciousness and sub consciousness

Research in the field of cognitive science[5], (especially in neurobiology and psychology) let to understand how human brain is working. It is truly amazing, how evolution create and make better this astonishing nervous system tissue. Currently human brain consists of three basic kind of brains: reptilian brain, the emotional brain and the rational brain (so called New cerebral cortex, which is also the latest product of evolution). On the other hand, the existence of previous forms of brain's development types still impact on the human patterns of thought, behavior and responses to stimuli. In the state of conscious people perform daily life functions and patterns already functioning in their mind. In the state of subconscious is drawn and processed most of the information from the environment. What is more interesting brain usually operates at the same time capable of conscious and subconscious (some part of brain is active, and other part transferring information from external environment). During sleep, the information gathered during the day are used for creating, recording and modifying existing patterns[6].

Warfare information specialists will create that kind of persuasive messages, that allow them to impact on subconscious recipients: to create and modify their existing patterns of thinking, behavior and emotional responses.

---

[3] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej, Operacja krymska – studium przypadku*, wyd. OSW, Warszawa, pp. 9-16.

[4] *Czarna propaganda Kremla*, http://niezalezna.pl/37348-czarna-propaganda-kremla, 29.04.2014.

[5] Cognitive-science, *Stanford Encyclopedia of Philosophy*, https://plato.stanford.edu/entries/cognitive-science/, 24.07.2011.

[6] According to the evolution process, consciousness state accelerate between 13-30 Hz, sub consciousness 4 to 13 Hz (light: 8-13 Hz and deep 4 to Hz): B. E. Schwartz, *The advantages of digital over analog recording techniques. Electroencephalography and Clinical Neurophysiology*, 106(2), 1998, pp. 113–1117.

Subconscious encoding

Human memory works according to a specific set of rules. Instantly men memorize information that are dynamic, colorful and absurd. Therefore it is easier to remember the plot of several movies than one, even short scientific book[7]. One of the techniques used to encode the subconscious information are called. "Memes". Usually it is an image with a brief content which trigger certain emotions: joy, anger, sadness, fear, surprise, etc[8]. Other methods relate to the creation of persuasive messages is to creation deeply emotional and suggestive: articles, videos, recordings. All combines the desire to elicit attention from smuggling and specific content.

It can apparently seem that to shut out the influence of the subconscious, it will be sufficient to simply restrict access to the Internet and begin to independently select information. In practice, particularly among young people it is almost impossible. At this stage, however, although it is theoretically possible. The future may bring many opportunities, but also challenges and even dangers. Mobile devices like corrugated interpersonal communication may be replaced in the future by implants[9]. Then this type of device could be implanted directly into the human nervous tissue. If we assume that the brain is a kind of very advanced biological computer and the current scientific work aims to create more and more advanced systems of bio-technology, such a prospect is only a matter of time. People will be vulnerable to attacks: both deforming data and distort the function of these devices. That kind of cyber-action could be named as: pure biotechnology attack on a technical level and IT attack on a software level. The strength of the attack will depend on the degree of synchronization between human body, and implanted implants. On the other hand, it may be practically impossible abandonment of these devices considerably facilitate (and perhaps even significantly prolonging) life, like today, it seems almost impossible to function without phone with Internet access. Finally, the phone may be broken or lost, implant however will always be with men, even damaged.

Conclusions

In summary it can be assumed that for the methodology of information warfare during the development of bio-technology will begin a new era. A time when people begin to deliberately distort the biological structure of their bodies striving for perfection, both physical and mental. Thus, the ability to influence will rise to a level that today may seem pure abstraction, at both levels : the technical (IT), as well as states of consciousness (encoding). It is, therefore, ask yourself, at what point is exceeded delicate border, in which human consciousness will lose autonomy in favor of synchronized systems of collective exchange of information.

[7] G. A. Dudley, *Jak podwoić skuteczność uczenia się*, wyd. Medium, Warszawa 1994, pp. 144-175.

[8] B. Hulten, N. Broweus, M. van Dijk, *Marketing sensoryczny*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2011, pp. 33-47.

[9] K. Max, Rahimpour, Shervin; W. Slutzky, Marc; Edgerton, V. Reggie; Turner, A. Dennis, *Enhancing Nervous System Recovery through Neurobiologics, Neural Interface Training, and Neurorehabilitation*. Frontiers in Neuroscience. 10: 584.

Bibliography

1. M. Radochoński, B. Przywara (red.) Jednostka-grupa-cybersieć. Psychologiczne, społeczno-kulturowe i edukacyjne aspekty społeczeństwa informacyjnego, Rzeszów, WSIiZ, 2004.

2. T. Goban-Klas, P. Sienkiewicz, Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania, wyd. Fundacja Postępu Telekomunikacji, Kraków 1999.

3. J. Darczewska, Anatomia rosyjskiej wojny informacyjnej, Operacja krymska – studium przypadku, wyd. OSW, Warszawa.

4. Czarna propaganda Kremla, http://niezalezna.pl/37348-czarna-propaganda-kremla, 29.04.2014.

5. Cognitive-science, Stanford Encyclopedia of Philosophy, https://plato.stanford.edu/entries/cognitive-science/, 24.07.2011.

6. B. E. Schwartz, The advantages of digital over analog recording techniques. Electroencephalography and Clinical Neurophysiology, 106(2), 1998.

7. G. A. Dudley, Jak podwoić skuteczność uczenia się, wyd. Medium, Warszawa 1994.

8. B. Hulten, N. Broweus, M. van Dijk, Marketing sensoryczny, Polskie Wydawnictwo Ekonomiczne, Warszawa 2011.

9. K. Max, Rahimpour, Shervin; Slutzky, Marc W.; Edgerton, V. Reggie; Turner, Dennis A., *Enhancing Nervous System Recovery through Neurobiologics, Neural Interface Training, and Neurorehabilitation. Frontiers in Neuroscience*.

ТЕНДЕНЦИИ В РАЗВИТИЕТО НА КИБЕР АТАКИТЕ

Димитрина Л. Полимирова

Национална лаборатория по компютърна вирусология – БАН,
София 1113, ул. „Акад. Георги Бончев“, блок 8, офис 104
dimitrina.polimirova@nlcv.bas.bg

CURRENT TRENDS IN CYBER ATTACKS

Dimitrina L. Polimirova

***Abstract**: This paper is focused on the current trends for cyberattacks. The most popular forms of attacks are also discussed: cybercrime, Denial-of-service attacks and nation-states attacks. An attention is paid on the vulnerabilities, ransomware, smartphones, cloud security and Internet-of-things as the most common attacks in 2017.*

***Keywords**: cybercrime, cyberattacks, vulnerability, ransomware, Internet-of-Things, SmartPhones, Cloud security*

1. ТЕКУЩО СЪСТОЯНИЕ

В съвременното информационно общество въпросите, свързани с развитието на злонамерения софтуер и злонамерените атаки си остават едни от най-наболелите проблеми. През изминалата 2016 година броят на инцидентите, свързани със злонамерения софтуер и отправените атаки към компютри, системи и мрежи нарасна значително. Анализирайки вече докладваните компютърни инциденти за първото тримесечие на 2017 г. можем да предположим, че 2017 г. ще ни донесе още повече от същото.

Забелязва се и голямо развитие и масово приложение на новите технологии, което от своя страна увеличава и полето на развитие на злонамерения софтуер и злонамерените атаки[10].

Независимо от това дали разглеждаме крайни потребители с няколко устройства или голяма организация, разполагаща с устройства за милиони, ние всички сме изложени на риск по отношение на информационната и комуникационна сигурност. А когато говорим за сигурност, промените (независимо от какво естество са) винаги оказват влияние върху риска. И тъй като промените са неразделна част от нашето информационни и технологично общество, то да бъдем осведомени за тях е ключов момент в това да бъдем проактивни в киберсигурността.

Когато говорим за тенденции в киберсигурността трябва да анализираме следните три параметъра:

[10] Основната разлика между злонамерения софтуер и злонамерените атаки се състои в това, че при злонамерения софтуер липсва прякото участие на човек/потребител в момента на атаката, докато при злонамерената атака задължително се предполага неговото присъствие.

- **заплахите**, които могат да бъдат отправени към компютри, системи и мрежи;
- **уязвимостите**, които могат да помогнат на тези заплахи да се реализират. Технологиите се променят по-бързо отколкото потребителите могат да ги усвоят, което е предпоставка за появяване на нови уязвимости, които отварят от своя страна нови възможности за атаки;
- **действията**, които се предприемат от една страна от злонамерените лица (отвън или отвътре), реализиращи атаката и от друга страна на хората, които се борят за намаляване броя на заплахите и увеличаване скоростта на откриване на злонамерени събития.

Моделът на поведение, който се определя от т.нар. злонамерен сценарий на заплахите, проведени през последните няколко години, се свежда до три основни:

- **шпиониране** – в последните години нараства броят на вирусните сценарии, които реализират поредица от предварително планирани действия с основна цел събиране на поверителна или секретна информация в информационни системи, принадлежащи на правителствени и корпоративни институции и организации. Дълбочината на познанията, които се демонстрират при създаване на подобен тип вирусни сценарии, е забележителна. С пълно право понякога се задава въпросът дали е по силите на отделен човек да постигне подобно ниво на компетентност и ако не, кой създава тези супер информационни оръжия. Разпространението на подобни вирусни сценарии обхваща не само отделни региони и държави, а и цели континенти. Неутрализирането на подобни вирусни сценарии е изключително сложна и трудна задача, която е по силите само на добре финансирана правителствена агенция или корпоративна структура;
- **печалба** – срещат се, макар и сравнително рядко, варианти на злонамерени сценарии, които предвиждат и реализират поредица от действия, свързани с манипулиране на информацията по такъв начин, че става възможно да се извлече директна финансова печалба, например от продажба или покупка на акции, ценни книжа и др. Анализът на подобни събития е твърде затруднен, тъй като пряка и достоверна информация за тези процеси се открива крайно рядко. И печелившата и потърпевшата страна в тези взаимоотношения нямат желание да споделят подробности за събитията. Някои от тези сценарии предвиждат сравнително бързо реализиране на идеята за печалба, например в рамките на минути, когато се отнася за борсови или валутни операции, други разчитат на многомесечни внимателно планирани и провеждани поредици от действия, когато се отнася до изкуствено надценяване или подценяване на акции на определена компания;
- **уязвимост** – тази разновидност на злонамерените сценарии има за цел разкриване на уязвимости в създадените и функциониращи системи за сигурност на различни нива в правителствени, корпоративни и лични информационни системи. От гледна точка на практическата полза този тип сценарии помага за откриване на решения, които отстраняват слабости и пропуски в текущите версии на системите за сигурност в информационната индустрия. Известни са и редица случаи, при които конкуриращи се фирми и компании изразяват своето съперничество чрез добре прикрита подкрепа при създаване на подобен тип вирусни сценарии. Щетите при подобен тип атаки не са за пренебрегване и понякога мащабите на действие на вирусните сценарии са значителни. Твърде често точните причини за информаци-

онните загуби не се разкриват докрай и широката публика е в неведение относно характера на определени събития.

Днес най-популярните форми за атака са:

- кибер престъпления. Това са престъпления, извършвани в киберпространството[11]. Киберпрестъпленията включват измами чрез спам, кражба на правителствена или фирмена тайна, като се реализира отдалечен неоторизиран достъп до системи, сваляне на незаконна музика, кражба на пари от електронни портфейли и много други. Киберпрестъпленията включват и действия, чиято първоначална крайна цел може да не е финансово облагодетелстване (например създаване на нови вредителски програми;
- отказ от услуга (DoS) и разпределен отказ от услуга (DDoS). DoS атаките забраняват използването на ресурсите на системата за легитимните й потребители. DDoS използва множество компютри за постигане на тази цел. Атаката се нарича „отказ от услуга“, защото се изпраща голям поток от пакети към компютъра-жертва. За да обработи пакетите, жертвата отделя голям обем ключов ресурс, като по този начин предлаганите от атакуваната система услуги стават недостъпни за законните потребители. В допълнение от казаното на нападателя може да се предостави неограничен достъп до засегната система и по този начин да се нанесат големи щети. Атакуващите машини в общия случай са географски разпръснати и използват различни начини за свързване в Интернет. По този начин контролирането на атаката се затруднява. Това може да доведе до силно неблагоприятни последствия не само за правителствени организации, но и за бизнеса, особено на този, който разчита на постоянно присъствие в Интернет;
- правителствени атаки. Много страни са изследвали начини да използват Интернет като оръжие за атака към финансови организации и правителствени компютърни системи[1]. Още от времето на Студената война остана практиката да се организират тайни дейности от разузнавателните агенции, свързани с периодично тестване на Интернет/Интранет мрежите за слаби места. В тази връзка е необходимо да се отбележи, че техниките за проучване на слабите места в Интернет и глобалните мрежи нарастват лавинообразно с всяка измината година[2].

2. ТЕНДЕНЦИИ В РАЗВИТИЕТО НА КИБЕР АТАКИТЕ

2.1. Уязвимости

И при трите споменати по-горе форми на атака уязвимостите са ключов фактор за реализирането им. Уязвимостите могат да се търсят както в системите за сигурност, така и в софтуера. Не бива да се пренебрегват и човешките уязвимости. Затова намаляването на уязвимостите е важно за отстраняване или минимизиране на щетите от реализирани атаки.

Въпреки, обаче, че новооткритите уязвимости (т.нар. уязвимости с нулев цикъл[12]) се коментират повече в интернет пространството, данни сочат, че атаките, които използват вече известни уязвимости причиняват по-големи щети.

[11] Киберпространството представлява един обобщен израз на изградената от съвременното общество информационна инфраструктура, включваща всички йерархични нива на съвременната глобална мрежа.

[12] Zer-day vulnerability

С развитието на новите технологии ще нараства и броя на уязвимостите с нулев цикъл, тъй като ще се увеличава и броя на новите продукти и използваните операционни системи. Въпреки това с най-висока степен на риск ще си останат вече известните уязвимости.

Методи за превенция в този случай е бързото откриване на уязвимостите в наблюдаваната система/мрежа и бързото им „закърпване“ или заместване с легализиран софтуер. Ако това не е възможно използването на системи за откриване и предотвратяване на проникванията (IDS/IPS) както и на защитни стени (Firewalls) е силно препоръчително. Критични информационни инфраструктури, съдържащи уязвимости, трябва да бъдат под непрекъснато наблюдение.

2.2. Шифроващи вредителски програми (ransomware)

Известни още в публичното пространство като „крипто вируси“ може да се счете за форма на атака от тип разпределен отказ от услуга, тъй като тези програми шифроват критични данни на потребителя и по този начин информационната инфраструктура на една организация може да спре да функционира.

През 2015 и 2016 година шифроващите вредителски програми се увеличиха драстично. Това е вредителска програма, която шифрова информацията на потребителя без неговото разрешение. За разшифроването на информацията авторите искат изплащането на определена сума (откуп). Въпреки, че защитата от тези вредителски програми е доста лесна и се свежда до редовно правене на архивни копия на независим носител, за 2016 година са изтръгнати почти 1 милион долара според доклад на ФБР [3].

За съжаление тенденциите през 2017 г. са шифроващите вредителски програми да продължат да бъдат едни от най-разпространените атаки в кибер пространството. Тенденциите в тяхното развитие се свеждат до промяна в техния сценарий и превръщането им в персонализирани атаки, т.е. да могат да разпознават и правят разлики между корпоративни системи и системи на крайни потребители.

Вектори на разпространение включват използването на:

- спам. 93% от спама е свързан с разпространение на шифроващи вредителски програми, като съобщенията са изкушаващи или заплашващи. Спам съобщението обикновено съдържа прикрепен файл, който може да бъде документ, скрипт или архива. Самият прикрепен файл може и да не съдържа кода на програмата, а само малка програма, която сваля основната;
- компрометирани сайтове;
- експлоатиращи комплекти (например Angler Exploit Kit);
- вредителски реклами, съдържащи активен код (Flash, JavaScript, Silverlight).

2.3. Смартфони (SmartPhones)

Смартфоните са крайно необходими инструменти във всички сектори на нашето общество, обхващащи правителствени организации, бизнеса и крайните потребители. Това е резултат от увеличаващата се функционалност на тези устройства, които се използват за извършване на разплащания, сателитна навигационна система, четене на поща, връзка със социални мрежи, WiFi хот-спот, четене на баркодове и най-накрая за провеждане на телефонни разговори. С нарастване на тяхната

значимост за обществото трябва да се оценят и рисковете, свързани с личните данни и сигурността от използването на тези устройства.

В голяма степен рискът зависи от това как се използва смартфона: като краен потребител, като служител в корпоративна или правителствена организация или като ръководител на високо ниво в корпоративна или правителствена организация. Основните рискове при ползването на тези устройства са [4]:

- изтичане на данни в резултат на загуба или кражба на устройството. Телефонът е откраднат или загубен и неговата вътрешна и/или външна памет са незащитени, което позволява на злонамереното лице да достъпи данните;
- неволно разкриване на данни, съдържащи се в телефона, от потребителя;
- атаки върху излезли от употреба телефони в случаите, когато телефоните са бракувани по неправилен начин;
- Фишинг атака (Phishing). Атакуващият събира данни (като пароли и номера на кредитни карти) като използва фалшиви приложения или приложения за четене на SMS и електронна поща, които изглеждат легитимни.
- шпионски софтуер (Spyware). На устройството има инсталиран шпионски софтуер, което позволява достъпа до данни на него. За разлика от целевото наблюдение шпионският софтуер има за цел нецелево събиране на лична информация;
- Network spoofing атака[13]. Атакуващият използва фалшива точка за достъп до Интернет (WiFi или GSM). В последствие атакуващият прихваща комуникацията на свързания към фалшивата мрежа потребител и я изменя, за да извърши последващи атаки (например фишинг атака);
- наблюдение. Атакуващият осъществява наблюдение на потребителя като използва функционалностите на телефона;
- свързани с телефонните комуникации атаки (Diallerware атаки). Атакуващият краде пари от потребителя като използва вредителски програми, които използват скрито услугите за комуникация с високотарифни телефони или SMS-и;
- вредителски програми, свързани с финансови услуги (Financial malware). Телефонът е заразен със злонамерен софтуер, специално проектиран за краде номера на кредитни карти или банкови сметки;
- задръстване на мрежата. Задръстване на мрежовия ресурс от използването на телефона. Крайният резултат е невъзможността да се използва мрежата от крайния потребител.

2.4. Атаки в облака (Cloud attacks)

Днес почти всеки потребител съхранява данни в облака. Увеличаването на мобилни устройства и услуги в облака накараха корпоративните организации да променят начина на работа. И тъй като влиянието на услугите в облака се е увеличило, сървърите, предоставящи услуги в облака, са също цел за злонамерените лица. Уязвимости съществуват не само за потребителя на облака, но и за предоста-

[13] При тази атака един човек или програма успешно се представя за друг чрез фалшифициране на данни.

вящия услугата в облака, както и за доставчика на интернет, който осигурява връзката между двете страни.

Услугите, свързани със сигурността в облака са се увеличи през последните години и ще продължат да се увеличават и за в бъдеще. Хибридните архитектури, където се съчетава локален контрол на сигурност с облаково-базиран контрол на сигурност ще се превърне в еталон за всички големи организации.

2.5. Интернет на нещата (Internet-of-Things (IoT))

Темата за Интернет-на-нещата е много актуална и има технологично, социално и икономическо значение. Към Интернет-на-нещата се отнасят продукти за потребителя, стоки за дълготрайна употреба, леки и товарни автомобили, промишлени и съставни части, сензори и други обекти от ежедневието, които съчетават функциите *свързаност в Интернет* и *анализ на данни.* Прогнозите за влиянието на Интернет-на-нещата върху Интернет и икономиката са впечатляващи, като очакванията са 100 милиарда свързани устройства и световно икономическо въздействие на повече от 11 трилиона долара до 2025 г.

От гледна точка на сигурността SANS определя четири основни типа устройства, които се включват в термина Интернет-на-нещата:

1) компютри, сървъри, рутери и др. подобни устройства, основно ползващи жична свързаност към Интернет;
2) медицинска апаратура, SCADA, устройства за мониторинг и контрол и други, основно използващи жична свързаност към Интернет;
3) смартфони и таблети, използващи различни форми на безжична свързаност към Интернет;
4) устройства за самостоятелно ползване, използващи единствено безжична свързаност с Интернет.

Тенденциите в развитието през следващите години е в четвъртата група устройства, които се вграждат в инфраструктурата на организациите (интелигентни сгради, автомобили, устройства за наблюдение и т.н.) или се използват самостоятелно от служителите (или от крайните потребители), но често се свързват към мрежата на организацията или в Интернет.

През септември 2016 година атаката от тип разпределен отказ от услуга *Mirai* не зарази компютри, смарфони или таблети. Тези устройства са оборудвани с антивирусен софтуер или друг софтуер, свързан със сигурността. За сметка на това *Mirai* употреби огромен брой други устройства (умни крушки, DVR-и, камери за наблюдение и т.н.), чиято защита не е тривиална процедура.

Голяма част от произведените устройства, влизащи в четвъртата група на Интернет-на-нещата, притежават уязвимости, които не могат да бъдат „закърпени“. Електрически умни крушки на почти всеки производител, например, са уязвими по отношение на сигурността и те са разположени в домовете ни и на практика са в режим на изчакване да бъдат използване за поредната ботнет атака.

Мащабите на използвания ресурс от *Mirai* са огромни и за съжаление това не е единствената осъществена ботнет атака, използваща Интернет-на-нещата за 2016 година от този калибър.

ЗАКЛЮЧЕНИЕ

Организациите и крайните потребители трябва непрекъснато да се адаптират към променящата се обкръжаваща средства по отношение на методите и средства за превенция и защита на устройства, компютри, системи и мрежи, които са неразделна част от ежедневието ни. Това ще продължи да бъде валидно и за следващата 2017 г. дори с още по-голяма сила. През изминалата година се наблюдава значително повишаване на нивото на сложност на осъществените атаки в киберпространството.

Днес да защитим информационна и комуникационна инфраструктура не е тривиална задача. Някои злонамерени лица могат да нарушат или напълно да блокират бизнес процесите докато не бъде платен откуп. Затова организациите трябва да фокусират усилията си в защита на тези ресурси, които са задължително условие за функционирането на организацията.

Важно свойство при защита е да бъдем готови и в състояние да реагираме при регистриран инцидент по отношение на компютърната и информационна сигурност.

Литература

1. McAfee Labs, Threats Report, December 2016 (https://www.mcafee.com/au/resources/reports/rp-quarterly-threats-dec-2016.pdf)

2. Griffiths Peter, "World faces "cyber cold war" threat", Reuters, http://ca.news.yahoo.com/s/reuters/071129/tecnology/tech_britain_internet_col

3. https://blog.malwarebytes.com/threat-analysis/2016/12/security-in-2017-ransomware-will-remain-king/

4. SmartPhones: Information security risks, opportunities and recommendations for users, ENISA, December 2010

TOWARDS SECURITY REQUIREMENTS OF THE SPIDER PROJECT

Nikolai T. Stoianov, Maya G. Bozhilova, Grigor R. Velev

Defence Institute "Professor Cvetan Lazarov",
Bulgaria, Sofia, 1592, 2 blvd. "Professor Cvetan Lazarov",
n.stoianov@di.mod.bg, m.bozhilova@di.mod.bg, g.velev@di.mod.bg

***Abstract**: The need for using sensor systems and networks for intrabuilding situational awareness in urban military operations demands strict requirements for theirs security and reliability. The report defines concepts related to security in accordance with purpose and functions of the sensor system.*

***Keywords**: urban operations, situational awareness, mobile sensor system, sensor network, security requirements*

Introduction

Project SPIDER (Inside Building Awareness and Navigation for Urban Warfare**)** aims to develop an innovative system to support urban warfare operations by providing improved situational awareness inside buildings.

The goal is to provide soldiers with an indoor map and information about the location of opposite forces. This system takes advantage of a sensor network located at both exterior and interior building areas. The proposed system is composed by two distinct sensor subsystems: a static outdoor subsystem and a mobile indoor subsystem. The outdoor subsystem is a network of radiofrequency sensors that aims to recognize humans inside the building. Each sensor node is able to communicate with other nodes, forming a network of sensors around the building in study. The indoor sensor subsystem is based on mobile robots capable of sensing the interior of the building using video camera and range-finding sensors such as depth sensors. These robots are controlled by operators through a secure communication system. A separate station receives all information obtained by both outdoor and indoor sensors to reconstruct an indoor map of the building. By visualizing the indoor map, the soldiers have a crucial awareness enabling them to safely navigate inside the building. The system is designed to be highly robust to endure operation in hostile environments.

SPIDER consortium consists following partners:

- TEKEVER ASDS, Portugal
- ARALIA SYSTEMS , United Kingdom
- TELECOMUNICAÇÕES AVEIRO, Portugal
- BULGARIAN DEFENCE INSTITUTE, Bulgaria.

The project will achieve its aim to support operations in urban environment implementing the following tasks:

- Real-time mapping of the building interior
- Detection and location of human presence inside the building
- Combine information from both indoors and outdoors sensors
- Improve the accuracy of the resulting data using data fusion
- Real-time communication of the information to the relevant forces

- Security of the proposed solution.

SPIDER consortium has identified the following main groups that may take advantage of the project outputs:

- Policy-makers (European Defence Agency, Ministry of Defence of the partner countries)
- Army units of partner nations, responsible for urban warfare operations
- Research institutions in areas, relevant to SPIDER project domain
- Industrial organization
- Educational and training military institutions
- Related projects & initiatives.

SPIDER system requirements

Urban operations span the entire range of possible force applications [3].

The availability of the main part of critical commander's information requirements is a big problem for the planners of urban operation. Detailed information is usually required when planning and conducting operations in built-up areas and especially on individual buildings. The design and construction of buildings within a particular urban area are influenced by numerous factors that include climate, materials available, function, and cultural development of the region.

Requirements for situational awareness in support of the operations described in the SPIDER scenarios are:

- The minimum information that has to be acquired for supporting successful mission execution is:
  - Define the building parameters (location, type, number of stories, date of construction, type of building construction, ownership, occupants, etc.)
  - Locate people inside and outside the building
  - Detect motion
  - Detect presence of weapons.
- Other operational needs for the systems providing the mission support information include:
  - Deployment of the required number of sensors (fixed and mobile) in the specified area in under or 30 minutes.
  - Time taken to collect and deliver required initial information to be at most 5 minutes. Initial information is understood to comprise first mapping information of the inside of the building.
  - Capability to gather and provide the above information in summary form and with appropriate formatting.
  - Providing users with the relevant information through a graphical interface as a minimum.
  - Running time of sensors to be greater than the time needed to gather information (i.e. at least more than 5 minutes).
  - Selection of operating frequency, bandwidth and signal power has to ensure system performance in both the outdoor and indoor areas.
  - Minimization of interference between selected operating frequency and other communications in the area.
  - Minimization of susceptibility of chosen operating frequency to jamming.

Security Requirements of the SPIDER system

Security requirements of the SPIDER system include: defining a set of security requirements for the system, i.e., how information should be exchanged and stored in a secure way and how management of the elements should be executed in a safe and secure way also.

The different aspects are defended in respect to the following requirements to communication and information part of SPIDER system:

- Security (system and data are secure)
- Performance (quick access to data)
- Cost (cost of the system)
- Universality (can be deployed in different environments)
- Reliability (high availability of the system)
- Ease of use (does not require technical knowledge).

The main requirements and functions related to the Information security system defined on SPIDER project are:

- Specification of requirements and solutions for secure information transfer, storage and destruction.
- Definition of procedures and monitoring of access to confidential information.
- Definition of the aspects of the information security and information protection.
- Definition of the architectural framework of the security system.
- Selection of the architectural approach for the whole system's development.
- Definition of methods and means for end users', communication channels' and data storage facilities' protection.
- Transparency for the users during the work with the elements of the system.

This preliminary list of objectives is not structured and is not systematically presented. In this section we approach the security requirements from the global perspective of a system that may become a defence forces tool and under the light of relevant laws, standards and best current practices.

Therefore, we will try to define general security requirements that rely on the set of security aspects identified by ISO/IEC 27000 and ITU X.800 families of security standards.

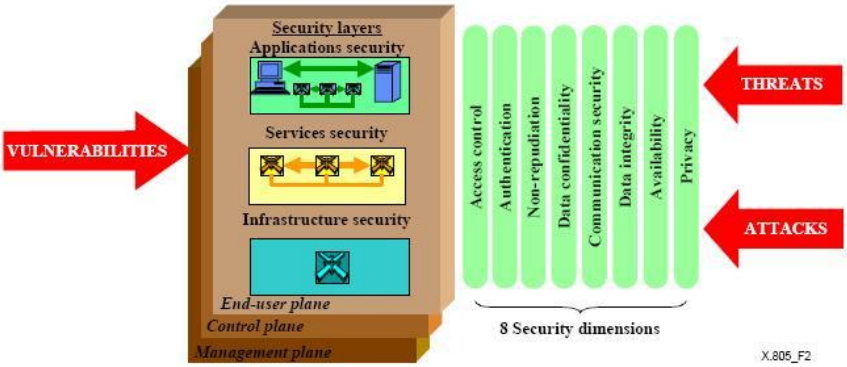


Figure 1. ITU-T X.805: Security Architecture for Systems Providing End-to-End Communications [1]

In particular ITU-T recommendation X.805 [1] (Figure 1) defines a reference security architecture for systems providing end-to-end secure communications, and introduces different security dimensions of a communication system. These dimensions can serve to structure general security requirements of a distributed Defence forces Information system:

- Access Control (Authorization)
- Authentication
- Non-Reputation
- Data Confidentiality
- Communication Security
- Data Integrity
- Efficiency
- Reliability
- Availability
- Privacy.

Each SPIDER component must have built-in mechanisms to address the requirements established for each one of the eight dimensions, and on all the planes through which interaction with them is possible: a) End-User, b) Control/Signalling and c) Management planes. Let us review general requirements for each dimension [2, 4, 5] and define SPIDER specific security requirements.

Access control (*Authorization*)

The ability to control the level of access that individuals or entities have, to both network and information systems must be properly defined by system managers. This strongly depends on the types of users that defence forces define, the respective access capabilities for each user group, and the confidentiality levels established for each piece of information.

There must be appropriate mechanism to enforce such access control (e.g. firewalls, file systems permissions, secure log-in) including physical control of access to drones

(UAV, UGV), and terminals. Furthermore the system must have a mechanism to fully trace and record the actions and the information accessed by each user at all times.

Each SPIDER component must have built-in access control mechanisms in all drones and collecting information system elements through which interaction with them is possible (namely end-user, control and management drones, according to X.805).

A single authorization check can grant access to all the functionalities of an application or system (i.e. login). However access control has a broader definition and can be applied before accessing to each resource of a system. In particular, a good mechanism to avoid cases of abuse of authority is to clearly define what the usage limits of an application are.

Authentication

Authentication must guarantee that the system being accessed is the intended one and that the user is who claims to be. The authentication mechanism in SPIDER systems should combine the use of a solid state-of-the-art Identity Management System (IdMS), including Public Key Infrastructure (PKI), Smart Cards to securely store private keys. However these technologies may be too expensive in order to be employed by every SPIDER element and may hinder the interoperation between different systems. For this reason Federated ID mechanisms that centralize authentication for multiple systems may become very useful in this context.

Therefore SPIDER components must be prepared to work in this type of IdMS environment and the whole SPIDER platform must be supported by an IdMS. Moreover, the federation of IdMSs in SPIDER may be useful in order to support cooperative investigation.

Non-Repudiation

Due to the potential legal value of the digital data managed by SPIDER tools, the capability to prevent system users from denying that data files were accessed, altered or deleted, might be useful for specific SPIDER subsystems to enable highly-secure logging and auditing processes.

Nevertheless, most of the tools and use cases developed in SPIDER are not oriented to obtaining legal evidences by themselves, but to support an investigation with hints or automatic alarms. Therefore, this dimension does not translate into a compulsory general requirement for SPIDER, but only for specific subsystems that may be employed to store evidences in electronic-format.

Data Confidentiality

The protection of information from unauthorized disclosure shall be made by: a) restricting per-user-group access to every type of information dealt with, b) by encrypting the information at least on transmission and possibly on storage, and c) establishing control mechanisms to the methods by which the information can be disclosed outside the group, supported by non-repudiation liability or watermarking techniques. This latter objective is the most complex to implement in practice since the ways of disclosing information are many. a) and b) should be compulsory requirements in SPIDER, and some type of disclosure control is desirable, yet out of the scope of SPIDER, since it must be a built-in feature of the defence forces information systems.

A standard classification of confidential levels (sorted from highest to lowest one) that could be also employed for future SPIDER information systems is:

1. Unclassified
2. Restricted

3. Confidential
4. Secret
5. Top Secret

However it is worth noting that no classified information will be gathered, stored or processed during the duration of the SPIDER project itself. These confidentiality levels are provided just as a reference inside the framework of defence forces information services.

Communication Security

To ensure that communication only flows from a source to the intended destination, all communication must be made with secure tunnels using standard mechanisms for this purpose, always employing encrypted sessions (e.g. TLS/SSL, ssh). Security should be further reinforced with Virtual Private Network (VPN) technology, such us IPSec tunnels, where appropriate (e.g. between physically secure routers or IP cameras), or when employing any kind of wireless link (e.g. WiFi, WiMAX, GSM/GPSR, UMTS).

In order to avoid man-in-the-middle attacks, the aforementioned technologies must support and employ mutual authentication by means of certificates or pre-shared keys.

Data Integrity

The ability to protect data from unauthorized, uncontrolled, or accidental alteration during storage or transmission is another essential feature that must be built-in in a defence forces information system. SPIDER should use checksum and hash functions as well as digital signatures wherever possible to guarantee the consistency of data in transmission and for continuous intrusion detection into file systems.

In order to guarantee the chain of custody, all SPIDER systems that may gather or store electronic information must implement mechanisms to guarantee that this data has not been altered by any system user or any other third party. In the case of processed information to be employed as evidence, both raw data and processed information must be protected from tampering.

Efficiency

Efficiency is one of the requirements which are connected with security. It is defined as a relationship between the results achieved and how well the resources have been used. It means that the aim to be achieved by the secure system also depends on the kind and quality of used methods and services. During the design process of the SPIDER subsystems (security solutions and requirements directly connected with security) this requirements should be taken into account.

Reliability

Reliability is defined as the ability of a system to perform its functions for a period of time. The reliability of the system is one of the “high-level” requirements. It means that it consist of a few different requirements (i.e. availability and communication security). It is a good point to start a design process and it can be a source of another, more specific requirements. This is obvious that this requirement connected with security should be met by the SPIDER subsystems.

Availability

The development of protection or back-up mechanisms for network/software/ hardware is also a desirable property of any IT system, as well as to defend from Denial of Service (DoS) attacks. This falls out of the scope of the SPIDER work plan, but provisions can be made in all the deliverables that describe implementations on how the subsystem can be protected to increase its availability.

Privacy

Privacy may be defined as an entity's ability to control how, when, and to what extent personal information about it is communicated to others. In order to support privacy it is important to understand what "personal information" is and to be aware of the ways that personal information can be controlled and processed.

During the duration of the SPIDER research project no personal data will be employed for the development and test of the systems and tools, unless strictly necessary (i.e. CCTV footage). In this case all people involved in those tests must fill a form to give their informed consent. Even in these cases, all personal data filed in the systems will be fictitious or at least anonymised.

Acknowledgements

This report partially has been funded by the European Defence Agency, Pilot Project on Defence Research, under Grant Agreement PP-15-INR-02_02_SPIDER.

References

1. ITU-T X.805. "Security architecture for systems providing end-to-end communications", 2003
2. Kizza J., Guide to Computer Network Security, Second Edition, Springer-Verlag, London, 2013
3. NATO Standard ATP-99 Urban Tactics (2017), Edition A, Version 1.
4. Obaidat M., Boudriga N., Security of e-Systems and Computer Networks, Cambridge University Press, 2007
5. Wang J, Computer Network Security, Theory and Practice, Springer, 2009

АНАЛИЗ НА КИБЕРСИГУРНОСТТА В МОДЕЛИТЕ ЗА INTERNET OF MILITARY THINGS

Добрин М. Махлянов
Николай Т. Стоянов

София 1092, ул. „Дякон Игнатий“ №3, e-mail: d.mahlyanov@armf.bg
София 1592, бул."Проф. Цв. Лазаров" № 2, e-mail:nik.stnv@gmail.com

CYBER SECURITY ANALYSIS FOR INTERNET OF MILITARY THINGS MODELS

Dobrin M. Mahlyanov
Nikolay T. Stoyanov

Abstract: *IoT is expanding in different areas in our life. IoMT is an almost brand new branch of IoT. Current paper describes in brief main models for IoMT realization, based on sites for information processing. Also, a simple analysis, focused on cyber security for different models is depicted.*

Keywords*: Models for IoMT, Cyber Security in IoMT, Attacks against IoMT*

Интернет на нещата (Internet of Things – IoT) и интернет на военните неща (Internet of Military Things - IoMT).

Въпреки сравнително новата концепция (Спомената за първи път през 1999 година [1]), IoT е едно от технологичните направления на бележещо най-голямо развитие през последните години. Според Дейв Еванс, за рождена година на IoT може да се счита 2008 година, поради факта, че тогава устройствата включени към глобалната мрежа са надминали по брой населението на земята [9]. По прогнозни данни на Gartner през 2017 броят на устройствата включени в интернет ще бъде около 8,4 милиарда [8]. Посочените цифри говорят експанзията на концепцията и може да се предложи, че подобна експанзия би следвала и в технологиите за реализиране на IoT. Въпреки това основната схема за реализиране на IoT не се е променила. Изхождайки от дефиницията за IoT - система от взаимосвързани обекти, механични и цифрови машини, животни или хора, разполагащи с уникална идентификация, притежаваща способност за автоматично предаване на данни по мрежа без да е необходимо въздействие от човешка страна [4], можем да определим основната архитектура на IoT :

- „Нещата” – това са всички елементи, които отговарят за събирането на данни и тяхното изпращане. Също така „нещата” трябва да могат да осъществяват обратна връзка, т.е. да оказват влияние на околната среда.
- Комуникационна мрежа – това е средата, която позволява „нещата” да бъдат взаимно свързани. В общия случай това е интернет средата, но като частни случаи могат да се разгледат всички възможни връзки [5] – Radio-Frequency Identification (RFID), Wireless Fidelity (Wi-Fi), Bluetooth, оптични кодове като Quick Response Code (QR code), Internet Protocol version 6 over Low power Wireless

Personal Area Networks (6LowPAN) и т.н.

- Изчислителни системи – Притежават способността да обработват данните, пристигащи от „нещата" през комуникационната мрежа и да изпращат обработената информация.

Разполагайки с основната структура на IoT, можем да разгледаме неговото частно проявление свързано с военната сфера – IoMT. Интересен факт е, че през двадесети век, за повечето технологии първостепенен, ако не и основен двигател за тяхното развитие са били военните разработки. Такива са били например ракетните технологии, радио комуникациите и дори самият Интернет. При IoT нещата са се развили по друг начин. Неговото развитие е основно на база частен сектор. Причината е повече от очевидна – ниска цена, голямо удобство при реализация и незначителни изисквания към сигурността. Докато за една метеорологична станция е без голямо значение кой е успял да прочете данните предадени от различните сензори, за една бойна част, разполагаща с умни устройства, това може да бъде фатално при изпълнението на поставените им задачи. И тук се проявява основната разлика между IoT и IoMT – това са изискванията за сигурност произтичащи от задачите, които ще се изпълняват. Тази разлика най-общо може да се обобщи със следното твърдение – IoMT елементите следва да оперират в обкръжаваща ги среда, която с голяма вероятност ще бъде неблагоприятна или враждебна към тях.

Модели за IoMT в зависимост от мястото на обработването на информацията

Една от основните операции извършвана върху информацията е нейната обработка и представянето и в необходимия вид. За това е необходима процесорна мощ (за по-бърза обработка), оперативна памет (за по-голям обем на едновременно обработваните данни), постоянна памет (за съхраняване на данните преди обработка и на информацията след обработка) и време. От съществено значение е и изборът на място, където ще бъдат извършвани тези изчисления. По презумпция, изходните данни за обработка в IoMT се генерират от мрежата от сензори. Но технологичният напредък позволява тези сензори да бъдат и миниатюрни компютърни станции с определена неголяма изчислителна мощ. Това предоставя възможност за избор на физическото място за изчисления. Вече не е необходимо това да бъде извършвано в облачното пространство. Може да бъде направено и в периферията на мрежата. В зависимост от избраното място за извършване на изчисленията могат да се определят три основни модела на реализация на IoMT, които ще бъдат разгледани по-долу:

1. Cloud computing (CC) базирани – в стандартната архитектурна реализация на IoT, изчислителните системи са реализирани като облачни технологии. На събраните данни се налага да преминат през няколко гранични устройства преди да достигнат до даден изчислителен център, обединяващ и обработващ огромно количество данни, преди да предостави необходимите резултати до потребителите. Съществуват няколко основни характеристики на моделите с облачно изчисление[6]:

- Огромен запас от ресурс - Облачните технологии осигуряват на всеки регистриран потребител, независимо от коя точка на света или време, в което се свързва чрез интернет връзка, огромен свободно достъпен споделен запас от ресурси. От тук се определя и основното предимство, че всеки потребител може да има достъп до този огромен ресурс и да ползва само толкова, колкото е

необходимо.

- Виртуализация - виртуализираните сървъри са основните технологични единици, които се използват при нужда в облачната структура. Именно тези сървъри представляват огромния запас от ресурс, който е достъпен при нужда. От своя страна, виртуализацията не е нещо ново. Това е технология, която позволява висока степен на оползотворяване на хардуера, като всеки физически сървър е разделен на множество виртуални сървъри. По този начин всеки един виртуален сървър действа като самостоятелен такъв имащ собствена операционна система, набор от софтуерни програми и приложения. Сървъри с много ядра засилват влиянието и значението на виртуализацията, защото всяка виртуална машина може да работи на нейно собствено ядро едновременно с всички други виртуални машини на същият физически сървър.
- Еластичност - представлява динамично мащабиране и дефинира възможността да се отчита колко ресурс е консумиран в отговор на това колко ресурс е бил необходим. Обикновено приложенията при нормална работа изискват минимални системни ресурси, но при пикови натоварвания се нуждаят от многократно повече. За целта, този който предоставя предлагаща трябва да изгради система с достатъчен ресурс, който да поеме пиковите натоварвания, при това с много добра производителност.
- Автоматизация - способност за автоматизирано създаване или премахване на виртуални машини (изграждане, инсталиране, конфигуриране и доставяне на приложения и услуги само през интернет без необходимост от ръчна намеса). Инсталираните на облака приложения могат да ползват нови допълнителни ресурси в случай на нужда и тези ресурси да бъдат активирани в рамките на няколко минути. След преминаване на пиковото натоварване , тези виртуалните ресурси могат да бъдат деактивирани.
- Измерване на потреблението – представлява възможността за отчитане на използваните ресурси, като всеки потребител може да разполага с това което е отпуснато за изпълнение на задачите.

2. Fog computing (FC) базирани – концепцията за изчисления в „мъглата“(„облак“, слязъл на ниско ниво) е противоположна на облачната по отношение на мястото за обработка на данните. При FC възлите за обработка на данните са разположени далеч от централизирания облак и близко до сензорите или по друг начин казано – „на ръба на мрежата“. При някои разработки е възможно дори самите сензори да притежават изчислителен капацитет и да бъде реализирана мрежова структура за обработване на информацията (mesh computing network). Основните разлики от облачната концепция за изчисление могат да се заключат в следното [2] :

- Разпределение по периферията и ниска латентност – основните елементи са базирани по периферията на мрежата и се явяват крайни устройства. Мъглата просто ги обединява в изчислителна мрежа, на която съставните части са разположени много близко един до друг. Това от своя страна води до много ниска латентност при предаване на данни.
- Разпространение върху значителна площ – за разлика от концентрираните центрове за данни в облака, тук елементите са разпръснати на сравнително голяма площ в зависимост от използваната технология.
- Взаимодействие в реално време – при традиционните системи с облачно

изчисление е нормално използването на опашки за обработка на заявките. При преминаване на капацитета, заявката стои и чака. При FC в случай на претоварване на даден елемент, заявката може да се пренасочи към съседен.

- Използване на безжична комуникация като основен тип за взаимодействие – географското разпределение на елементите на FC, както и тяхната мобилност е предпоставка за неефективното използване на кабелната среда за комуникация.
- Федеративност – използването на различни видове елементи в FC не е проблем, ако те могат да се обединят за изпълняването на конкретни задачи

3. Cloudlet computing (ClC) базирани – концепцията заема междинно място между „облака“ и „мъглата“. Реализира се с разполагане на мобилен изчислителен център в близост до мрежата от сензори, притежаващ както необходимия капацитет за извършване на изчислителните операции, така и със способността да бъде преместен на различно място в случай на нужда. Чрез ClC се постига минимално количество на граничните устройства през които минават данните преди обработка и възможност за предаване нагоре по веригата на обработена информация.

Cloudlet структурата може да се разглежда като „изчислителен център в кутия“, чиято цел е да смъкне облака по близо до крайните устройства. За нея е характерно следното [10] :

- Минимални усилия за управление след първоначално инсталиране – не е необходимо присъствие на специалисти за включване на допълнителни крайни устройства или при промяна на мрежовите конфигурации
- Притежаване на значителни изчислителни ресурси, добра свързаност и сигурна среда за обработка и пренасяне на информацията – ClC притежава необходимите компютърни ресурси (CPU, RAM и други) за да може да облекчи ресурсоемките изчисления от крайните устройства, притежава добра свързаност както надолу, така и нагоре, и не е ограничена от захранване.
- Техническата реализация на ClC най-често е реализирана на база софтуерни решения за Cloud computing разположени върху ограничена по капацитет физическа среда. Това е постигнато за сметка на други качества, като мобилност и своевременност.

Въпреки че и при трите модела основната разлика изглежда да е разположението на изчислителните ресурси, не трябва да се подценява и ролята на комуникационната среда. Принципа на реализирането и е че колкото по-надолу (по-близо до сензорната мрежа) е разположен изчислителния капацитет, толкова по-хомогенна остава комуникационната среда.

Киберсигурността в IoMT

Като основен показател за нивото на киберсигурност в IoMT се явява рискът. Рискът, както във всяка друга област, подлежи на измерване и управление. Основните компоненти за измерване на риска са уязвимост, намерение и последствия [7]:

- Уязвимост - представлява способността на атакуващия да придобие достъп и контрол над изчислително устройство, да манипулира или компрометира данни, да контролира или прекъсва услуги. Поради малката компютърна мощ в крайните устройства, същите не винаги могат ефикасно да изпълняват функции на сигурността, което съответно ги прави лесна цел.
- Последствия – ефектът, постигнат при успешно експлоатиране на

уязвимостта.

- Намерение – това, че дадено устройство е уязвимо, че някой ще извърши зловредни действия с него. Атакуващият трябва да прецени дали получените последствия биха оправдали ресурсите, които той изхабил, за да се възползва от дадена уязвимост.

Предвид спецификата на IoMT, а именно опериране във враждебна среда, може да се приеме, че последствията от използването на дадена уязвимост биха били в повечето случаи критични, както и че противниковата страна почти винаги би имала намерение да се възползва от дадена уязвимост. Като критичен фактор остават уязвимостите. По долу е направен опит за класификация на възможните проблемни ситуации, предизвикани от различни уязвимости и съответно техния ефект в зависимост от използвания модел за обработка на информацията:

- Подслушване на комуникационните канали – Изхождайки от факта, че основната комуникация е безжична, може да се предположи, че нейното подслушване не би било особен проблем. За да остане сигурна информацията, е необходимо тя да бъде криптирана преди предаване. Изграждането на защитени комуникационни канали при реализация на FC не е проблемно, заради наличието на подобрени изчислителни ресурси в крайните устройства. Част от тях могат да се пренасочат за изграждането на защитена мрежа. При използването на CC и ClC имаме същата мрежа от устройства, т.е. същия брой комуникационни канали, но вече устройствата не е необходимо да имат такива параметри и е възможно да срещат проблеми с изграждането на защитни канали. Много комерсиални продукти дори не предлагат възможност за използване на криптирани комуникации. В добавка, при CC модела, цялата информация се изпраща за обработка по ограничен брой канали, т.е. компрометирането на някой от тях би довело до компрометиране на голям част от системите изградени по този IoMT модел.

- Довеждане до неработоспособност на изчислителните способности на IoMT системите [3] – основна задача при водене на бойни действия се явява унищожаване на системата за командване и управление на противника (СКУ). СКУ най общо се състои от органи за управление, пунктове за управление и КИС. По своята същност IoMT е една силно специализирана и усъвършенствана КИС, което води до превръщането и в приоритетна цел. От елементите на IoMT, единственото което може да бъде определено като реална цел са изчислителните системи. Нито крайните устройства (множество на брой, разположени върху голяма географска площ), нито комуникационните канали (много на брой и хетерогенни като състав) биха могли да бъдат практически неутрализирани. Същото важи и за изчислителната система при FC реализация. Крайните устройства трудно могат да бъдат редуцирани до брой, от който е невъзможно поставените задачи да бъдат изпълнени. Все пак следва да се отбележи, че определени загуби са възможни, което би понижило ефективността на изчислителната система, за което трябва предварително да се планира резерв. При CC реализация унищожаването на изчислителната система е практически невъзможно поради отдалеченото ѝ разположение в сигурна среда. Сериозно уязвими за такъв такива действия са моделите с ClC реализация. Мобилния облак трябва да е разположен близо до крайните устройства т.е. възможно е неговото физическо унищожаване, прекъсване на комуникационните канали или нарушаване на работоспособността му с други мерки.

- Използване на зловреден код – практиката е показала, че използването на зловреден код е ефикасно срещу системи които не са поддържани от гледна точка на кибер хигиената. Един изчислителен център трудно би бил такъв, въпреки че потенциален ефект на успешна атака срещу него би бил съкрушаващ. Като далеч по реалистична цел могат да се определят крайните устройства. Обикновено крайните устройства или се закупуват или се изработват за изпълнението на дадени задачи Характерно за придобиването на военна техника, е че трябва да отговаря на дадени спецификации в момента на изработването/покупката и след това тези спецификации рядко се променят в жизнения цикъл. Това е перфектната предпоставка за наличието на уязвимости от типа 0-day exploit – уязвимости които съществуват, но ние не сме наясно за тях. Дори и след откриването им, не всички производители могат да пуснат обновления за неутрализирането им. В общия случай и трите модела на реализация на IoMT са уязвими за такъв тип атака, но поради начина на разпространение особено уязвим е FC. При останалите два модела информацията се разпространява чрез една или няколко буферни точки, докато при FC такива липсват. Буферните точки представляват още едно ниво на защита, където разпространението на зловредния код би могло да бъде предотвратено и тяхната липса би довела до ситуации при които на теория е възможно всички устройства, притежаващи дадена уязвимост да бъдат заразени преди да се предприемат каквито и да е било мерки за минимизиране на последствията.
- Недостатъчно ниво на автентификация [11]– може да се разглежда както от страна на елементите, така и от страна на потребителите. Въпроса с потребителите е сравнително ясен – проблемите са добре известни и не възникват нови. Като цяло се използва автентификация на принципа „Нещо, което знам“ (пароли), „Нещо, което имам“ (токен, смарт карта) и „Нещо, което съм“ (биометрия). Ако приложим същите принципи и за елементите, ще получим използване на предварително зададени ключове, допълнителни модули или уникални идентификатори. Използването на ключове е добра политика, до момента в който стане необходимо ключа да бъде подменен в случай на компрометация или изтичане на валидност. Процедурата, която отнема време при нормални условия, се усложнява неимоверно при прилагането и върху географски разпръснати устройства. Това е проблем от първостепенна важност за реализация на FC модел. При него отделните устройства са взаимно свързани и броят на необходимите ключове нараства експоненциално с нарастването на крайните устройства. Аналогична е ситуацията и при използване на допълнителни модули. При използването на уникални идентификатори възниква въпроса какъв трябва да бъде уникалния идентификатор. По аналогия с компютърните мрежи, това трябва да е еквивалента на MAC адреса – най-често използвания идентификатор. Но при използването на хетерогенна среда не е толкова лесно да се определи единен идентификатор и за IoMT. Някои сходни устройства е напълно възможно дори да нямат идентификатори и за системата да бъдат просто едно и също устройство. Отделно, този идентификатор може да бъде узнат, клониран и да се направи опит за подмяна на дадено легитимно устройство с друго. Проблемите с автентификацията касаят едновременно и трите модела за реализиране на IoMT, като една от възможните стратегии за разрешаването им е използване на многофакторна автентификация, както за потребителите, така и за устройствата.

- Ограничена възможност за отдалечено изтриване на чувствителна информация – оперирайки във враждебна среда не бива да се изключва вероятността част от крайните устройства да попаднат в недоброжелателни ръце. Изключвайки опцията за физическо унищожение, следващото което трябва да може да се направи е заличаване на всякаква чувствителна информация. Компонентите на FC модела е силно препоръчително да притежават такава опция. Практическата реализация не е проблем, поради постоянната връзка с елемента и сравнително неголемият обем от данни, необходими за изтриване. Съответно при CC модела, това е неприложимо, поради огромните обеми данни и практическата недостъпност на центровете за данни. При него в повечето случай крайните устройства са сензори и не притежават самостоятелно чувствителна информация. Особено проблемен се явява модела ClC. При него крайните устройства не са застрашени, но центъра за данни може да бъде застрашен. Изтриването на информацията в него би отнело много време, поради голямото и количество.

Съществуват и други проблемни ситуации, но решаването на тези за определения модел би довело до значително повишаване на нивото на кибер сигурността. Също така еднократното решение не следва да се счита като панацея. Нивото на сигурност трябва постоянно да бъде оценявано и подобрявано.

Представяне на проблемите на моделите за IoMT в зависимост от основните аспекти на информационната сигурност

Описаните по-горе проблеми могат да бъдат изобразени и с основните аспекти на информационната безопасност – конфиденциалност, достъпност и цялостност. Всеки проблем може да се асоциира с даден аспект и съответно може да има различен ефект върху различните модели на реализация. В таблица 1 са описани разгледаните проблемни ситуации в различните модели и тяхното проявление върху аспектите на информационната сигурност. Таблицата може да бъде както допълнена с различни проблемни ситуации, така и да бъде разширена с допълнителни аспекти (невъзможност за отказ, отчетност, идентификация, автентификация и оторизация и др.)

<table>
<tr><th></th><th colspan="3">Модели за IoMT</th></tr>
<tr><th>Аспекти на информационната сигурност</th><th>Cloud Computing базирани</th><th>Cloudlet Computing базирани</th><th>Fog Computing базирани</th></tr>
<tr><td rowspan="5">Конфиденциалност</td><td colspan="2">Подслушване на комуникационните канали</td><td>-</td></tr>
<tr><td>-</td><td colspan="2">Сигурно изтриване на данните</td></tr>
<tr><td colspan="3">Използване на зловреден код</td></tr>
<tr><td>-</td><td>-</td><td>Недостатъчно ниво на автентификация</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="3">Достъпност</td><td>-</td><td>Физическо унищожение</td><td>-</td></tr>
<tr><td colspan="3">Използване на зловреден код</td></tr>
<tr><td>Време за достъпност</td><td>-</td><td>-</td></tr>
<tr><td rowspan="2">Интегритет</td><td colspan="3">Използване на зловреден код</td></tr>
<tr><td>-</td><td colspan="2">Недостатъчно ниво на автентификация</td></tr>
</table>

Таблица 1. Проблемни ситуации в IoMT в зависимост от избрания модел и засегнатия аспект на информационна сигурност

Един от вариантите за определяне на общото ниво на сигурност на даден модел е оценяването на различните аспекти на информационната сигурност за дадена ситуация. Чрез него могат да се определят приоритетните направления за решаване на проблемните ситуации.

Заключение

Разглеждайки IoMT като усъвършенствана КИС може да се каже че е налице определен организационен опит при изграждането на някои от моделите за IoMT. Концепцията за CC е еквивалентна на мащабните комуникационно информационни центрове, докато изнесените комуникационно информационни възли отговарят на ClC модела. Единствено концепцията FC е сравнително нова и непозната. Но с навлизането на IoMT активно се използват и трита вида модели за реализация в зависимост от разполаганите ресурси, поставените задачи и възможните проблеми. Всеки един от тях има своите предимства и недостатъци от гледна точка на кибер сигурността, но приоритетна задача при реализацията им следва да се явява осигуряване на предварително зададено ниво на сигурност

Литература:

1. Ashton Kevin, „Linking the new idea of RFID in P&G's supply chain to the then-red-hot topic of the Internet was more than just a good way to get executive attention“ , 2009

2. Bonomi Flavio, Milito Rodolfo, Zhu Jiang, Addepalli Sateesh, „Fog Computing and Its Role in the Internet of Things", 2012

3. Dhanjani Nitesh, „Abusing the Internet of Things - Blackouts, Freakouts and Stakeouts", O'Reilly , 2015

4. Evans Dave, „The Internet of Things. How the Next Evolution of the Internet Is Changing Everything.", Cisco White Paper. Cisco Systems", 2011-04-11

5. Hersent Olivier, Boswarthick David, Elloumi Omar, „The Internet of Things - Key Applications and Protocols", Wiley, 2012

6. Jing Qi, Vasilakos Athanasios, Wan Jiafu, Lu Jingwei, Qiu Dechao, „Security of the Internet of Things: perspectives and challenges", Wireless Networks, Nov 2014

7. Lewis James - „Managing risk for the Internet of Things", A Report of the CSIS Strategic Technologies Program, February 2016

8. Meulen Rob van der, http://www.gartner.com/newsroom/id/3598917, 24.03.2017

9. Recommendation ITU-T Y.4000/Y.2060 (06/2012)

10. Satyanarayanan Mahadev, „The Emergence of Edge Computing", The IEEE Computer Society, 2017

11. Spínola Maria, „The Five Characteristics of Cloud Computing", http://cloudcomputing.sys-con.com/node/1087426, 24.03.2017

ВИДОВЕ КОНТРОЛ – ХАРАКТЕРИСТИКИ

Христо А. Христов, Петър К. Боянов

KINDS OF CONTROL. CHARACTERISTICS

Hristo A. Hristov, Petar K. Boyanov

Abstract: *Each type of control has its own applicable field and its own even comparative autonomy. The variety of control's subjects and objects, goals and tasks, means and forms of social development influences upon the kinds of control. This variety reasons defying the kinds of control as groups that are delimited on the basis of certain criteria in order to reveal their relevant features.*

Keywords: *Security sector, state control, public control, civilian control, the Ombudsman, disputing, an appeal, an administrative act.*

Всеки вид контрол има свое приложно поле, своя макар и относителна самостоятелност. Многообразието на обектите и субектите на контрол, целите и задачите, средствата и формите на обществено развитие, влияят върху видовете контрол. Това многообразие дава основание определянето на видовете контрол да стане по групи, разграничени въз основа на определени критерии, като по този начин се разкриват техните характерни белези.

В зависимост от качествата, които притежава субектът, съществуват държавен, обществен и граждански контрол.

Държавен контрол - функция на държавното управление, която произтича от правото на държавата да управлява своята собственост и да защитава своите интереси.

Държавният контрол е нормативно закрепен в специални нормативни актове и се осъществява от специално създадени институции (организации). Той има императивен, а понякога и репресивен характер, тъй като трябва на всяка цена да изпълни целите и задачите поставени от държавното ръководство и заложени в закони.

Обществен контрол - участие на формированията на гражданите в управлението на различните сектори на държавата, оценка и коригиране на функционирането на публичната администрация.

Общественият контрол е най-висшата форма на контрол. Гради се на общественото начало и традициите и е важен фактор за изграждане на обществото. Този контрол дава възможност на всички граждани да взимат участие в управлението. Упражняването на обществен контрол в много случаи е олеснен и подпомогнат от правно - нормативни актове (Конституцията, Административно-процесуалния кодекс, Закона за административните нарушения и наказания, Закона за предложенията, сигналите и жалбите и др.).Обществения контрол може да се осъществи чрез

обществени организации (партии, неправителствени организации, синдикати, медии и др.).

Граждански контрол - действия на гражданите с цел проследяване и коригиране на управляващите по отношение законосъобразността на решенията и съответствието им с интересите и нуждите на гражданите и обществото.

Контролът на гражданите върху държавното управление и администрацията е абсолютно необходим елемент на демократичната държава. Той е важна действена форма за тяхното участие в управлението на държавата. Способите и процедурите използвани в контрола на гражданите върху държавното управление, са изключително важна гаранция за отстояване на законните им интереси и за защита на техните права.

В зависимост от обхвата и степента на обобщеност контролът може да бъде разграничен като общ и специализиран.

Общият контрол е присъщ на органите на властта и управлението на страната и в отделни обекти на стопанска и социална дейност. Той е насочен към глобалните явления и процеси. Чрез него те се изучават цялостно въз основа на най-важните, главни параметри, които ги характеризират. Подробностите в развитието им не са присъщи на този вид контрол. Резултатите от него служат за изработването на общи оценки за състоянието на държавата и обектите и насочване дейността на контролните органи към контретизация и задълбочаване на тези оценки. Това показва, че общият контрол има в редица случаи първичен характер. Той насочва към нови контролни действия.

Специализираният контрол има точно определено приложно поле. Практическата му реализиция се извършва въз основа на изчерпателността и задълбочеността. Чрез него се осигуряват определени проучвания, в резултат на което той може да има вторичен характер, предопределен от практическите потребности на управленските структури на отделните равнища.

Специализираният контрол, независимо от своята насоченост и конкретност, обхваща цялостната дейност на обектите, но от определени позиции. При този контрол, обектът е точно определен, а целта е ясно формулирана и се осъществява от лица, които са специалисти в областта на съответния вид контрол.

В зависимост от правоотношенията на контролните органи с обекта на контрол, контролът бива вътрешен и външен.

Вътрешният контрол се извършва от органи, чиято приналлежност спрямо обекта на контрол е регламентирана с трудовоправни отношения. Такива могат да бъдат както отделни ръководители и специалисти, така и лица, упражняващи контролни функции в рамките на обекта. Този контрол обхваща само процеси и явления, които се реализират в рамките на конкретния обект.

Вътрешният контрол играе ролята на превантивен контрол. Има възможност да следи отблизо явленията и процесите и да реагира ефективно и адекватно. Този контрол, поради своята зависимост от субекта на управление, понякога има склонност за нарушаване на нормите, правилата и инструкциите на поведение.

Външният контрол се осъществява от органи, които по своята принадлежност се намират извън проверявания обект и не са в трудовоправни отношения с него. Те са специални органи за контрол, определени и оправомощени със закон или друг нормативен акт и са в трудовоправни отношения със специализирани структури за контрол. Това ги прави независими от управленските органи на проверява-

ния обект, което лежи в основата на безпристрастността и принципността при извършването на контролните действия и оценки.

В зависимост от органите, които го осъществяват, контролът се дели на следните видове: ***парламентарен, административен, съдебен и прокурорски контрол.***

Парламентарният контрол започва със създаване на законодателния акт. За всеки отделен обект мерките за контрол и ограниченията върху неговата дейност са вписани в текста на закона за него. Заедно с това законодателният орган не само издава закони, но той ги отменя или внася промени в тях. По този начин парламентът по всяко време може да внесе ограничения в предоставените правомощия, да ги прехвърли на друг орган или да предостави нови, по-широки.

Комисиите чрез различни средства контролират дейността на различни обекти, като търсят признаци за недостатъчно прецизно планиране,за неефективна дейност, за злоупотреба с власт или незаконосъобразно поведение.

Парламентарният контрол дава възможност да се провери наличието на политическо доверие и поддръжка на правителството от страна на парламента. Той е политически, има за цел да установи как МС ръководи и осъществява вътрешната и външна политика в съответствие с Конституцията и законите. Контролът на Народното събрание е насочен за осъществяване на главните направления в държавната политика.

Административен контрол - държавновластническа дейност, чрез която едни държавни органи(административни органи или органи с контролна компетентност създадени със закон) контролират други административни органи (централни или териториални) и дейността на служителите от администрациятакоято ги подпомага.

Административният контрол прониква във всички звена на административния апарат, засяга всички актове, действия и прояви в администрацията.

Институтът на **съдебния контрол** произтича от мястото на съда в системата от държавни институции и отредената му роля в гражданското общество. Съдилищата осъществяват контрол за законност на актовете и действията на държавните служители от различни структури. Съдебният контрол за разлика от административния е винаги контрол за законо-съобразност на административните актове и действията на служителите.

Съдебният контрол е утвърден и авторитетен механизъм за законност в поведението на държавната администрация. Той се оказва един от най-съществените правни фактори за надеждна правна защита на правата и свободите на гражданина при взаимоотношенията му с държавната администрация.

Прокурорският процесуален надзор представлява инициативен контрол. Прокурорът действа не само при сезиране, но и по свой почин. Източниците на информация на прокурорския надзор могат да бъдат и неофициални, важно е да съдържат данни за неизпълнение на законите от обектите на социално управление. Те могат да бъдат и анонимни, стига да са конкретни по обекти и факти.

За разлика от съда прокуратурата има една пряка административна функция - да приема жалби и да проверява оплаквания за извършени самоуправни действия и в резултат на това да изготвя писмени разпореждания за тяхното отстраняване.

Като специфична контролна дейност надзора на прокуратурата се осъществява на практика в няколко форми:общ надзор на прокуратурата;следствен надзор

на прокуратурата;съдебен надзор на прокуратурата;прокурорски надзор над местата за лишаване от свобода;прокурорски надзор при задържане.

В зависимост от вида и характера на проверяваната дейност, контролът може да бъде данъчен, финансов, банков, митнически, застрахователен и др.

Данъчен контрол е финансов контрол, осъществяван от държавни структури в интерес на държавата и обществото. Неговата практическа реализация се постига на основата на две конкретни форми - данъчна проверка и данъчна ревизия. Техен обект е дейността на данъчните субекти, свързана с формирането на доходи и извършването на разходи, начисляването на данъчното задължение, неговото отчитане и внасяне в срокове, определени от действащата законодателна и нормативна уредба.

Финансов контролконтрол има за обект производството, разпределението, преразпределението и производственото потребление на националния доход. В по-ранните етапи от неговото развитие финансовият контрол е известен под наименованието финансово-ревизионен (когатосе отнася до финансова и стопанска дейност), финансово–бюджетен (когато се отнася до бюджетната дейност), а по-късно и сега – като вътрешен финансов контрол, т.е. контрол, който се упражнява от системата на вътрешния финансов контрол в държавните учреждения, организациите, техните поделения и звена.

Митническият контрол има за цел правилното прилагане, протичане и изпълнение на митническия режим в страната.

Този контрол се осъществява чрез Агенция митници и предмета на неговата дейност е да контролира вноса, износа и валутните ценности и операции. Обект на контрол са транспортните средства и гражданите, а обект за контрол са стоките, багажите, парите и валутните ценности, които те превозват или пренасят.

Банков контрол е специфичен и се упражнява като организирана функция в системата на банките. Банков контрол се упражнява и за клиентите на банките (за отпуснати кредити, за доказани източници на парични средства и т.н.), но това не променя неговия характер и цел да усъвършенства банковата система, да оказва съдействие за ефективно провеждане на банковите операции, в т.ч. и кредитните операции.

От една страна, банковият е организиран като потребност за стабилността на цялата банкова система, независимо дали банките са собственост на държавата или на акционери - физически лица. Типичен представител на този вид контрол е банковият надзор.

Втората особеност на банковия контрол се заключава в съвместяването на контролните функции с банковите операции. Контролният процес протича заедно с банковите операции, голяма част от тях имат контролно значение.

Третата особеност е в наличието на специални, задължителни изисквания за организацията на вътрешния контрол във всяка банка.

Застрахователен контрол има за основна цел проверка на законосъобразността на дейността на застрахователите.

Застрахователният контрол се осъществява чрез специализирани органи, законови разпоредби и нормативни актове имащи императивен характер.

Държавният застрахователен надзор се реализира от Национален съвет по застраховане и от Дирекция за застрахователен надзор.

Според предназначението си контролът бива: за законосъобразност и целесъобразност.

Всяко явление и процес в изброените видове контрол - данъчен, финансов, митнически, банков и др. се подлагат на проверка за спазване на законността и целесъобразността, тъй като те се осъществяват въз основа на специални закони и определени норми и са основата на предварително определени цели. С различните видове контрол, чрез прилагането на нормите за законосъобразност и целесъобразност се постига защита на законността в държавата. Резултатът от практическата реализация на контрола може да намери израз в следните варианти на проявление:Законосъобразни и целесъобразни;Законосъобразни, но нецелесъобразни;Незаконосъобразни, но целесъобразни;Незаконосъобразни и нецелесъобразни.

Документален и материален контрол.

Контролът се разглежда като материален и документален въз основа на специфичните особености на обекта и избора на въздействие върху него.

Документалният контрол се състои в проверка на документи или проверка само въз основа на документи, които са носители на информация относно дадена дейност. Документален е контролът върху цялата счетоводна документация и счетоводните записвания по нея.

Материалният (фактически) контрол се изразява в проверка на дадено фактическо състояние на обект, процес и т.н. Обикновено се касае до проверка на количеството и качеството относно реалността на дадена извършена или предстояща дейност, до количеството и качеството на материални и други ценности. С помощта на фактическия контрол се установяват евентуално съществуващите разлики между наличните количества на материални ценности и данните за тях по официалната отчетност. Най-общо казано материален е контролът върху отразените в документите процеси, който може да се разглежда и като инвентаризация.

Дистанционен контрол - упражняваният контрол от дистанция, т.е. без да има контакт на субекта с обекта, е дистанционен контрол. Този вид контрол все повече ще се налага, особено при трансконтинентални транзакции, където само сателитната връзка позволява да се наблюдават и контролират някои процеси. Характеристиката на дистанционния контрол напомня за потребността все повече да се прилагат методите на моделиране, на описание на контролируемите признаци и техните критични точки, за да се проследяват възможните отклонения за явления и процеси на голяма дистанция.

Одит - в научната теория, **одитът** се разглежда като **"независима експертиза"**, чийто инструментариум се състои от независими проверки, анализи и оценки на информация за миналата дейност на оценяваните обекти или за протичане на различни процеси.

По правило одитът следва да бъде локализиран като *крайна и завършваща фаза* на етапа “измерване на фактическото състояние” от цялостния контролен процес в обществените системи.

Според полето на приложение, одитът се разделя на: финансов одит, одит на съответствието и операционен одит.

Финансов одит - Задачата на финансовия одит е да даде точна оценка по отношение на отчетността и вярното отразяване на получените финансови и икономически резултати в счетоводните сметки и регистрите на обществената система.

При *одита на финансовата отчетност* предмет на одита е съответствието на тази отчетност с възприети критерии, които намират израз в съответни стандарти за финансова отчетност. В неговата заключителна фаза този вид одит е *одит на финансовите отчети* на обществената система.

Одит на съответствието е насочен към спазване на определени изисквания регламентирани в нормативни актове. Тези правила и процедури могат да бъдат външни за обществената система и да са регламентирани законодателно или по друг начин, например като общоприети правила.

Операционен одит - предметът на дейност на операционния одит е да търси степента на ефективност и производителност на една или друга обществена или управленска система.

Доколкото целите на обществените системи се дефинират от тях автономно, предметът на операционния одит предпоставя неговото предназначение да обслужва изключително *вътрешни* за обществената система информационни потребности. На основата на изготвените оценки, при операционния одит се генерират препоръки за повишаване на производителността и ефективността на извършваните в обществените системи операции за постигане на поставените цели.

Мониторинг -комплекс от непрекъснато или повтарящо се наблюдение и анализ на определен обект или процес с цел да се открие съответствие с желан резултат.

Мониторинг на обществени проекти и политики - реализацията на различните типове публични политики и проекти са свързани с множество проблеми и редица рискове. Мониторинга има за цел да се определят основните рискови проблеми и подходящите методи и инструменти за набиране, анализ и предоставяне на оперативно значима информация, предназначена за тези, които вземат решение. За да бъдат ефективни, анализът и оценката е желателно да се осъществяват още в ранните етапи на работата по съответната политика/проект и да продължат като постоянен итеративен процес по време на целия мониторинг и заключителната оценка.

Основна задача на мониторинга на публичните политики и проекти е да се следят и измерват постигането на техните цели и на ефективността им в хода на тяхната реализация. В резултат на осъществявания мониторинг могат да се направят своевременни корекции в начина на изпълнение на политиките и проектите.

Мониторинг в обществената система е компонент на вътрешния контрол.Той обезпечава факта, че системата за вътрешен контрол функционира според очакванията. Мониторингът е цялостен преглед на дейността на обществената система, като основната цел е да се оцени състоянието на вътрешния контрол и ръководството да получи увереност, че извършваните контролни дейности функционират според предназначението си и остават ефективни във времето.

Осъществява се чрез текущо наблюдение и специални оценки. Текущото наблюдение се извършва в хода на нормалните повтарящи се дейности в организацията, т.е. непрекъснато в реално време. То реагира динамично на променящите се условия и е интегрирано в ежедневните дейности наорганизацията, докато специалните оценки се извършват след събитията, а техният обхват и честота зависи в

голяма степен от оценката на риска и ефективността на текущия мониторинг. Те могат да се извършват под формата на самооценки, както и от вътрешни и външни одитори.

В заключение може да се посочи, че видовете контрол се намират в тясна връзка с практическата му реализация. Чрез тях се разкрива, кое е главното, определящото при тази реализация.

Литература:

1. Арбатов, Ал., Парламентарен контрол над сектора за сигурност, С., 2003 г.
2. Бакалов, Й., Теоретичен модел на политика за сигурност и граждански контрол на Република България, С., 2011 г.
3. Гражданският контрол в Република България. Принципи, параметри, практики. Асоциация АКСЕС и издателство „Отворено общество", С., 1999 г.
4. Граждански контрол над полицията, Авторски колектив, С., 1996 г.
5. Иванов, Х., Гражданското общество и концепции за граждански контрол, С., 2002 г.
6. Йончев, Д., Демократичното общество и гражданският контрол върху системата за национална сигурност, С., 1996 г.
7. Конституция на Република България.
8. Кындева, Е., Публична администрация, С., 2007 г.
9. Томов, Й., Теория на контрола и одита, Изд. „Ценов", Св., 2002 г.
10. Фотев, Г., Гражданското общество, С., 2002 г.

ОРГАНИ И ИЗПОЛЗВАНИ ТЕХНОЛОГИИ ЗА КОНТРОЛ

Христо А. Христов

AUTHORITIES AND PRACTICED CONTROL TECHNIQUES

Hristo A. Hristov

Abstract: *The main function of authorities responsible for control is to cooperate in accordance with positive process of state management or in other words to create environment frustrating and preventing from negative events (harms) happening as well as the relevant reasons in the country.*

Keywords: *sector of security, National Audit Office, financial inspection, National Revenue Agency, Customs Agency*

Основна задача на органите за контрол е да съдейства в позитивния процес на държавното управление – да създава обстановка, която да не позволява или да предотвратява настъпването на отрицателни явления (вреди)и на причините за тях в страната.

Видовете контролни органи могат да бъдат класифицирани в следните групи:

- Органи за контрол с обща компетентност

Тези органи по право упражняват контрол като продължение на техните управленски функции. Това са Народното събрание, Министерският съвет, областните управители, на местно управленско равнище - кметовете и общинските съвети. С обща компетентност по контрола са и общите събрания на акционерите, стратегическия мениджмънт и други висши управленски структури на организациите. Всички те упражняват контрол по общи, окрупнени параметри наред с основните си функции да вземат решения (в т.ч. и нормативни решения) в рамките на управленския цикъл - социален или конкретен в отделнитеорганизации.

- Специални контролни органи

Те са създадени да упражняват единствено контролни функции. От подобен род са всички специално създадени контролни институции като Сметната палата, Държавната финансова инспекция, Националната агенция за приходите, агенция „Митници" и др. Тези органи имат специален статут, определен от закона, и права за контрол с широк обхват.

- Специализирани контролни органи

Тези органи упражняват единствено контролна функция в определена специфична област. От такъв характер са санитарния и ветеринарния контрол, контрола на КАТ, контролът на ГД „Пожарна безопасност и защита на населението" и др.

Специални контролни органи и технологии за контрол

Обект на разглеждане ще бъдат само типичните представители на тези групи органи като: Сметна палата, Държавна финансова инспекция, Национална агенция за приходите, агенция „Митници".

Сметна палата

Основна задача на Сметната палата е да контролира надеждността и достоверността на финансовите отчети на бюджетните предприятия, законосъобразното, ефективно, ефикасно и икономично управление на публичните средства и дейности, както и да предоставя на Народното събрание надеждна информация за това.

Сметната палата извършва: финансови одити; одити за съответствие при финансовото управление;одити на изпълнението;специфични одити.

Сметната палата може да извършва документални и фактически проверки и други контролни действия по отношение на юридически лица, възложени й със специални закони, само в рамките на одитната си дейност и по реда на закона за сметната палата.

Обхват на одитната дейност. Сметната палата одитира:

- държавния бюджет;
- бюджета на държавното обществено осигуряване;
- бюджета на Националната здравноосигурителна каса;
- бюджетите на общините;
- други бюджети, приемани от Народното събрание.
- бюджетите и извънбюджетните сметки и фондове на разпоредителите с бюджетни кредити по бюджетите и управлението на тяхното имущество;
- самостоятелните бюджети на Българската академия на науките, държавните висши училища, Българското национално радио и на Българската национална телевизия;
- бюджетните и извънбюджетни средства, предоставяни на лица, осъществяващи стопанска дейност;
- средствата от фондове и програми на Европейския съюз, включително управлението им от съответните органи и крайните ползватели на средствата;
- бюджетните разходи на Българската народна банка (БНБ) и тяхното управление;
- формирането на годишното превишение на приходите над разходите на БНБ, дължимо към държавния бюджет, и другите взаимоотношения на банката с държавния бюджет;
- възникването и управлението на държавния дълг, държавно-гарантирания дълг, общинския дълг и използването на дълговите инструменти;
- приватизирането и концесионирането на държавно и общинско имущество, както и на предоставените публични средства и публични активи на лица извън публичния сектор;
- изпълнението на международни спогодби, договори, конвенции или други международни актове, когато това е предвидено в съответния международен акт или е възложено от оправомощен орган;
- други публични средства, активи и дейности, когато това й е възложено със закон.

Правомощия при извършване на одитите

Одиторите, директорите на дирекции и ръководните органи на Сметната палата по време и във връзка с извършваните одити имат право:

- на свободен достъп до служебните помещения и до всички документи, отчети и активи, свързани с финансовото управление на одитираните организации, включително да изискват годишните финансови отчети на дружествата с държавно

и общинско участие, които подлежат на одит, и протоколите от заседанията на техните органи;

- да изискват в определени от тях срокове справки, заверени копия от документи и друга информация във връзка с предварителното проучване и извършването на одитите, включително на електронен носител;

- да изискват устни и писмени обяснения от длъжностни лица, включително от бивши длъжностни лица, по факти, които са констатирани при одитите, както и по въпроси, които са свързани с тяхната дейност;

- да изискват справки, заверени копия от документи и друга информация от физически лица, юридически лица и еднолични търговци извън одитирания обект, свързани с възможни случаи на незаконна дейност, които засягат финансовите и имуществените интереси на одитирания обект или средствата от фондове и програми на Европейския съюз;

- да изискват и да получават информация от всички органи в страната, както и достъп до базите им от данни във връзка с дейността на Сметната палата;

- да присъстват на заседания на органите на одитираните организации и лица, ако дневният им ред е във връзка с провеждания одит.

При упражняване на правомощията достъпът до класифицирана информация се извършва при условията и по реда на Закона за защита на класифицираната информация.

Одиторите на Сметната палата могат да изискват извършване на инвентаризации във връзка с одитите.

Държавна финансова инспекция

Основната цел на държавната финансова инспекция е да защитава публичните финансови интереси.

Целта се осъществява от агенцията чрез изпълнение на следните основни задачи:

- извършване на последващи финансови инспекции за спазването на нормативните актове, които уреждат бюджетната, финансово-стопанската или отчетната дейност, както и дейността по възлагане и изпълнение на обществени поръчки на организациите и лицата;

- установяване на нарушения на нормативните актове, уреждащи бюджетната, финансово-стопанската или отчетната дейност, както и на индикатори за извършени измами;

- разкриване на причинени вреди на имуществото на организациите и лицата;

- привличане към административнонаказателна и имуществена отговорност на виновните лица при наличието на съответните законови основания;

- установяване на измами и нарушения, засягащи финансовите интереси на Европейските общности.

Държавната финансова инспекция се осъществява във:

1. бюджетните организации;

2. държавните предприятия по чл. 62, ал. 3 от Търговския закон, както и в общинските предприятия;

3. търговските дружества с блокираща квота държавно или общинско участие в капитала;

4. търговските дружества, в чийто капитал участва с блокираща квота лице по т. 2 или 3;

5. юридическите лица, които имат задължения, гарантирани с държавно или общинско имущество;

6. юридическите лица по Закона за юридическите лица с нестопанска цел и неперсонифицираните дружества по Закона за задълженията и договорите, в които държавата или общината участват пряко или косвено в имуществото им;

7. получателите на държавни помощи, лицата, финансирани със средства от държавния или от общинските бюджети, по международни договори или програми на Европейския съюз, както и лицата, финансирани със средства от държавните предприятия по Търговския закон - по отношение разходването на тези средства.

Агенцията изпълнява следните функции:

1. ръководи, провежда и контролира осъществяването на инспекционната дейност;

2. планира и осъществява последващ контрол за законосъобразност на дейността по възлагането и изпълнението на обществените поръчки;

3. събира и анализира информация за дейността на лицата по възлагане и изпълнение на обществени поръчки;

4. анализира причините и условията за нарушенията на финансовата дисциплина и предлага мерки за отстраняването им пред компетентните органи;

5. дава методически указания на финансовите инспектори за осъществяване на дейностите по този закон и извършва контрол по качеството на инспекционната дейност;

6. организира обучение за първоначална професионална подготовка на новоназначените служители, за поддържане и повишаване на квалификацията, както и за придобиване на нови професионални знания и умения на служителите на агенцията;

7. осъществява взаимодействие и обмен на информация с други държавни органи;

8. сътрудничи с финансово-контролните органи и организации на други държави и международни организации;

9. оказва съдействие на контрольорите на Европейската комисия, за предоставянето на достъп до помещения и/или документация и носители на компютърни информационни данни, за извършване на контрола и проверките на място - при отказ на проверяваната организация и на лице, финансирани със средства по международни договори или програми на Европейския съюз.

Данъчен контрол. Национална агенция за приходите

Същност и характеристики на данъчния контрол

По своята същност **данъчният контрол** е финансов контрол, но той не изчерпва всички видове финансов контрол, а е само един от неговите видове. Осъществява се в интерес на държавата и общините, което предопределя неговата обществена значимост. Субектите на този контрол не се намират в пряка връзка с организацията и управлението на данъчния субект, което ги изключва от системата на вътрешния финансов контрол. Те се намират в трудово-правни отношения със специално създадена за целта институция на държавата, в лицето на Главна данъчна дирекция към Министерството на финансите.

Следователно данъчният контрол е външен финансов контрол, осъществяван от държавни структури и в интерес на държавата и обществото. Неговата практическа реализация се постига на основата на две конкретни форми - данъчна проверка и

данъчна ревизия. Техен *обект* е дейността на данъчните субекти, свързана с формирането на доходи и извършването на разходи, начисляването на данъчното задължение, неговото отчитане и внасяне в срокове, определени от действащата законо-дателна и нормативна уредба.

Данъчната проверка заема основно, приоритетно място в дейността на данъчните органи. Тя се използва, когато трябва да се установят разходи, приходи, регистрация и пререгистрация за данъчните субекти. Данъчни проверки се извършват и по искане на данъчни подразделения в други райони на страната. Разновидност на данъчната проверка е *делегираната данъчна проверка*, която се извършва във връзка с данъчни ревизии на данъчни субекти от други данъчни дирекции.

Данъчната ревизия се различава от финансовата ревизия. Разликата е в обхвата и обекта. И двата вида ревизии имат за обект финансово-стопанската дейност на контролираните обекти, по което си приличат. Приликата е в това, че те са форми на последващ финансов контрол и се извършват от органи, които не участват пряко в дейността на ревизирания обект.

За разлика от финансовата, данъчната ревизия не обхваща цялата финансово-стопанска дейност, а само онази част от нея, която е насочена към формирането на приходите и разходите и определения въз основа на тях краен финансов резултат. Това е значително стеснен обхват, в сравнение с финансовата ревизия, независимо от общият им обект.

Данъчните ревизии могат да бъдат *планови и извънпланови*. Чрез тях се установяват задълженията на данъчните субекти за изтеклия период от време или за установяване на отделни видове данъчни задължения. Данъчни ревизии се извършват и при ликвидация, приватизация, преоб-разуване и обявяване в несъстоятелност на данъчни субекти.

Национална агенция за приходите

Функции на Агенцията:

- обслужва данъкоплатците, осигурителите, осигурените и самоосигуряващите се лица, като им осигурява необходимата информация, разяснения по правата и задълженията им, осигурява отпечатването и безплатното разпространение на данъчни и други декларации, съдържащи указания за попълването им, на формуляри и други документи, които се изискват или издават въз основа на закон, като ги публикува и в Интернет на страницата на агенцията;
- установява публичните вземания за данъци и задължителни осигурителни вноски по основание и по размер;
- обезпечава и принудително събира публичните вземания;
- събира доброволните плащания на публичните вземания по параграф едно;
- установява административни нарушения и налага административни наказания по данъчните закони, както и по законите, регламентиращи задължителните осигурителни вноски;
- разглежда жалби срещу издадени от нейни органи актове или срещу откази за издаване на актове, както и срещу действия или откази от действия на нейни органи или служители;
- води регистър на лицата, подлежащи на регистрация по реда на Данъчно-осигурителния процесуален кодекс, лицата, които работят по трудово правоотношение, създава и поддържа бази данни за тях, необходими за осъществяване на

дейността ѝ и за нуждите на задължителното социално осигуряване, на Министерството на финансите и общините;

- анализира приходите и приходната практика;

- установява и събира определени със закон частни държавни вземания;

- представлява държавата в производството по несъстоятелност в случаите, когато държавата е кредитор с публични или определени със закон частни държавни вземания;

- организира, ръководи и стопанисва местата за публични разпродажби и поддържа в интернет актуална информация за продаваните вещи и права;

- приема, съхранява, управлява и продава имущества, придобити от държавата в производството по несъстоятелност;

- приема, съхранява, управлява и продава всички конфискувани, отнети и изоставени в полза на държавата имущества;

- осъществява обмен на информация с Европейската комисия и други институции при прилагането на чл. 256 от Договора за създаване на Европейската общност и осъществява обезпечаването и принудителното събиране на вземания по решения на Европейската комисия, Съвета на Европейския съюз, Съда на Европейските общности и Европейската централна банка, с които се налагат парични задължения, подлежащи на изпълнение на основание чл. 256 от Договора за създаване на Европейската общност;

- осигурява и разпределя материално-техническата база за осъществяване на дейността си;

- изпълнява решения за конфискация или отнемане на имущество и решения за налагане на финансови санкции, постановени в държава - членка на Европейския съюз, и признати и подлежащи на изпълнение в Република България;

- осъществява и други дейности, възложени ѝ със закон.

Митнически контрол. Агенция „Митници”

Митнически надзор е съвкупност от действията на митническите органи, предприемани с цел осигуряване спазването на митническото законодателство и на други разпоредби, приложими за стоките под митнически надзор.

Митнически контрол е извършването от митническите органи на специфични действия като проверки на стоки, на транспортни, търговски, счетоводни и други документи на физически и юридически лица, на превозни средства, на багажи и други стоки, пренасяни през държавната граница, и други подобни действия за осигуряване спазването на митническото законодателство и спазването на други разпоредби, приложими за стоките под митнически надзор, както и събирането на митни сборове.

Митническа администрация

Митническата администрация е централизирана административна структура, организирана в Агенция "Митници" към министъра на финансите, която е юридическо лице на бюджетна издръжка със седалище София.

Функции на митническите органи:

- осъществяват митнически надзор и контрол върху стоките, превозните средства и лицата в зоните на граничните контролно-пропускателни пунктове и на цялата митническа територия на страната;

- изчисляват, събират или изискват обезпечаването на митни сборове, определени при внос, износ или транзит на стоки;

- прилагат, в рамките на своята компетентност, тарифните мерки и мерките на търговската политика на Република България;

- защитават икономическите интереси на страната в рамките на своята компетентност;

- осъществяват митническо разузнаване за противодействие на митническите и валутните нарушения;

- организират и осъществяват дейността за предотвратяване и разкриване на незаконния трафик на наркотични вещества и прекурсори;

- осъществяват валутен контрол в рамките на предоставената им със закон компетентност;

- издават решения за прилагането на митническите разпоредби;

- осъществяват дейност по установяване на административни нарушения и налагане на административни наказания;

- участват при осъществяване на оперативно-издирвателна дейност съвместно с органите на Министерството на вътрешните работи при условията и по реда на Закона за Министерството на вътрешните работи и с органите на Държавна агенция "Национална сигурност" при условията и по реда на Закона за Държавна агенция "Национална сигурност";

- прилагат мерки за граничен контрол за защита на права върху интелектуалната собственост;

- осъществяват разследване или отделни действия по разследването на престъпления в случаите, при условията и по реда на Наказателно-процесуалния кодекс.

Литература:

1. Арабаджийски, Н., Основи на публичната администрация, Специална част, София, 2005 г.
2. Арбатов, Ал., Парламентарен контрол над сектора за сигурност, С., 2003 г.
3. Бакалов, Й., Теоретичен модел на политика за сигурност и граждански контрол на Република България, С., 2011 г.
4. Балабанова, Хр., Административен контрол, В., 2004 г.
5. Гарнизов, В., Третият сектор в България: статистика, тенденции, събития. В: „Инициатива за подкрепа на гражданското общество в България", Асоциация АКСЕС, С., 2003 г.
6. Гражданският контрол в Република България. Принципи, параметри, практики. Асоциация АКСЕС и издателство „Отворено общество", С., 1999 г.
7. Динев, М., Контрол в социалното управление, Изд. „Тракия М", С., 1999 г.
8. Закон за митниците, в сила от 01.01.1999 г.
9. Закон за отбраната и въоръжените сили на Република България.
10. Иванов, Х., Гражданското общество и концепции за граждански контрол, С., 2002 г.
11. Йончев Д., Слатински, Н., Трифонов, Т. и др. Демократичното общество и гражданския контрол върху системата на национална сигурност. Сравнителен анализ и културни особености, С., 1997 г.
12. Конституция на Република България.

13. Кындева, Е., Публична администрация, С., 2007 г.
14. Сачев, Е., Културното наследство и националната сигурност, С., 2005 г.
15. Сачев, Е., Цивилизация и социокултурноисторическа сигурност, С., 2010 г.
16. Стойкович, В., Идентичност и толерантност, Сп. „Демократически преглед", 1999 г., с. 20-25.
17. Томов, Й., Теория на контрола и одита, Изд. „Ценов", Св., 2002 г.
18. Фотев, Г., Гражданското общество, С., 2002 г.

КИБЕРСИГУРНОСТТА В „НЕОБЯТНОТО" ИНФОРМАЦИОННО ПРОСТРАНСТВО

Радослав Б. Чалъков, Калоян А. Илиев

CYBERSECURITY "IMMENSE" INFORMATION SPACE.

Radoslav B. Ghalakov, Kaloyan A. Iliev

"В нашето дигитално време въпросите на киберсигурността не засягат само хората от технологичните среди, те засягат всички нас - без значение дали работиш в сферата на бизнеса или политиката, армията или медиите, или си просто гражданин."

Ерик Шмид, Изпълнителен председател на Google

Abstract: *Problems related to information security and successfully countering hackers, cyber threats, cyber terrorism and cyber warfare have long been accepted as one of the greatest challenges of the modern information society, the demand for successful decisions and actions in the field of cybersecurity, already exceed the limits of a single science or state and require complex interdisciplinary approach involving all stakeholders. Cybersecurity is a key element of the national security state. The high degree of use of social networks, which can be viewed as a channel for possible infiltration, espionage and terrorism, is also part of the threats facing it.*

Keywords: ***Hacker*** *- Someone who violates computer security for malicious reasons, kudos or personal gain.*
cybersecurity - The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
cyberspace - The interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Живеем в информационно общество. Тази фраза се е превърнала в клише до степен, че не се замисляме за параметрите на нейния смисъл. Светът започна да става обезпокоително малък, откакто с помощта на средствата за търсене на информация в интернет можем да узнаем подробности от биографията на познати или напълно непознати лица.

Доказва се твърдението, че информацията е мощно оръжие, особено когато съдържа лични данни.

Бурното развитие на информационните технологии позволи създаването, ползването и съхраняването на всякакъв род информация в цифров вид и в интернет-пространството. Основен проблем при нейното наличие в интернет е надеждната й сигурност (киберсигурност) от каквито и да е посегателства – достъп, копиране, модифициране или унищожаване.

Повече от 20 години след създаването на интернет, в него няма нито една дейност, при която с информацията да не може да се злоупотреби, и това е неприемливо. Изненадващо голям брой хора не са наясно какво и как се случва в интернет. Те са просто ползватели, които вярват, че щом не плащат сметките си онлайн или не дават номера на кредитната си карта, нищо лошо не може да им се случи. Никога не трябва да казваме „Това няма да се случи с мен", защото никога не бива да подценяваме киберпрестъпниците.

Темата за киберсигурността може да бъде объркваща, а и терминологията е като взета от чужд език, но въпреки това е важно да сме наясно с рисковете й и какво означават те за нас.

Разширяването на киберпространството създаде нови и нарастващи заплахи за комуникациите. То може да се разглежда като електронна преносна среда на компютърните мрежи, в която се извършват online комуникации и споделяне на информация. Целия набор оборудване с програмируеми елементи или компютри създават нова област за атака от страна на хакерите.

Цел на кибер атаката може да е *шпионаж, саботиране или физическо унищожение*. Шпионажът е придобиване на сензитивна, лична или класифицирана информация. Физическото унищожение е резултат от атака в киберпространството, при която с цели въздействие върху системите за управление и добиване на данни (SCADA- system control and data acquisition) и по този начин да се наруши процесът на управление на индустриалните и инфраструктурни процеси.

Според професор доктор на науките Евгени Николов, бивш директор на Националната лаборатория по компютърна вирусология при Българската академия на науките *„Всяка заплаха в интернет трябва да се взима на сериозно и на нея да се реагира адекватно"*.

Как ще се почувствате, ако се събудите една хубава сутрин и разберете, че всичките ви лични данни са откраднати? Сценарият е съвсем възможен. В последните години информация за милиони хора бе откраднатa при хакерски атаки, а бизнесът бе лишен от милиарди долари заради киберпрестъпления. Затова сигурността в интернет е по-важна от всякога.

Непрекъснато ескалиращият киберриск и претърпяваните загуби на организациите в световен аспект налагат необходимостта от редовна проверка с цел повишаване и гарантиране на киберсигурността им.

В глобален план, в 80% от хакнатите през изминалата 2016 г. организации, достъпът е получен от хакерите чрез уеб апликации. Наблюдава се зачестяване и на DdoS (*съкращението идва от Distributed Denial of Service и означава едновременна атака от голям брой системи*) атаките, на Ransomware (криптолокер) и Phishing (фишинг атака). Атаките с криптолокери се определиха като една от най-големите заплахи през 2016-та година, тъй като те могат да причинят изключително мащабни щети на атакуваните жертви.

Криптолокерите могат да използват различни канали на разпространение – социални мрежи, имейли, месинджър, подхвърлен носител и др. Самият криптолокер е прикрит като някакъв друг файл, но с вградено съдържание. Той криптира файловете, и достъп до тях не може да се получи, освен ако не бъде платена исканата от хакерите сума. Самият криптолокер освен това може да започне да се разпространява сред контактите, дори без да имаме информация.

Фишинг атаката е един от методите на социалното инженерство. При него се разчита на пробив в човешкото поведение, чрез подвеждане на дадени служители с невярна информация. Фишинг атаката по същество представлява разпространяване на подменено съдържание или изпращач. Това най-често се реализира чрез имейл, макар че се използват различни комуникационни канали за разпространението му. Този имейл може да изглежда съвсем автентичен, но не е, а целта му може да бъде да ви подведе да кликнете върху линк към фалшив уеб сайт, или да отворите прикачен файл със заразено съдържание, или дори да ви бъдат поискани ваши лични данни. Често се среща чрез фишинг атака да се разпространяват криптолокери.

DDoS атаките представляват насочване на прекомерен трафик към системите на жертвата, с който сървърите й не могат да се справят. По този начин се срива дейността й.

Основна цел в сферата на киберсигурността е чрез активни действия да бъдат открити, наблюдавани "напреднали устойчиви заплахи" (APT) и вътрешни опасности като своевременно им се реагира целенасочено.

Успехът в подготовката и в реагирането на всякакви целенасочени атаки са резултат от изключително задълбочени познания и сериозен професионален интерес към настоящата киберситуация в глобален световен аспект.

Като положителна световна тенденция може да бъде посочен стремежът на фирми, организации и държавни институции да търсят сами уязвимости в своите мрежи и системи, с което да се предпазят от ежедневно наблюдаваните днес престъпни хакерски атаки. По този начин те гарантират не само собствената си киберсигурност, но и тази на всички свои партньори, клиенти и крайни потребители, с чиято информация всъщност боравят за целите на своята дейност.

Тази тенденция се наблюдава напоследък, след като бяха извършени многобройни мащабни хакерски пробиви в цял свят, довели до критични загуби на данни и финанси. Ще ви дам само няколко примера, които разкриват огромните щети, които една злонамерена хакерска атака може да нанесе.

През февруари 2016 г. беше хакната Bangladesh Central bank и бяха откраднати 951 млн. долара чрез пробив в SWIFT мрежата й. Освен огромната сума, хакерите получиха достъп и до чувствителна информация за редица банкови трансфери.

В началото на ноември същата година беше извършена атака срещу системите на британската Tesco Bank, при което бяха компрометирани сметките на 40 000 нейни клиенти. От 20 000 сметки бяха извършени реални финансови кражби, но това не е всичко, защото към жертвите можем да добавим и десетки хиляди други клиенти, които са се поддали на фишинг имейл и са кликнали на линк, разпращан цели 24 часа уж от тяхната банка.

Наскоро беше атакуван и AdultFriendFinder, при което хакерите получиха достъп до данните на 400 милиона потребители, а 15 милиона профила бяха изтрити. В рамките на около година това е вторият пробив в системите на AdultFriendFinder. Yahoo призна за откраднати лични данни на негови потребители през 2014-та, когато са били хакнати 500 милиона акаунта. Това спокойно можем да наречем най-мащабната хакерска атака в последните години. Информацията е съдържала имена, имейли, пароли, телефонни номера, рождени дати, данни от кредитни карти и банкови сметки. Този пробив буквално обезцени акциите на Yahoo, който до този момент се котираше доста високо.

Примерите са безкрайни. Но те положиха, според мен, основите на световната тенденция за повишаване на киберсигурността. Защото освен реалните загуби на атакуваните фирми, тези пробиви всъщност пораждат и значителен обществен отзвук, от който трайно страда и имиджът на жертвите.

По-далновидно е да не чакаш да разбереш дали мрежите и системите ти са уязвими, а да провериш сам и респективно – да вземеш нужните мерки.

Допринасят ли например облачните услуги за киберсигурността?

Отговорът е – и да, и не. Основното предимство на облачните услуги е, че чрез тяхното използване се спестяват пари, тъй като се използва готовият продукт, не се налага всяка компания да пише собствен софтуер за нови приложения, които могат да имат от своя страна редица собствени уязвимости. От тази гледна точка облачните услуги работят в полза на повишаването на фирмената киберсигурност.

От друга гледна точка обаче, много фирми ползват облачните услуги на една и съща компания. Представете си, че даден брой фирми съхраняват данните си в компанията Х чрез облачна услуга. Ако компанията Х бъде хакната по един, или по друг начин, данните на всички нейни клиенти ще бъдат компрометирани. Това би било избегнато, ако тази безценна фирмена информация се съхранява на собствен сървър и се взимат адекватни и регулярни мерки за нейната киберсигурност. Така че, както виждате, всяка ситуация има своите добри и рискови страни.

Глобалната мрежа еволюира, еволюираха и заплахите, които тя крие. От начин за дребно вредителство „червеите и вирусите" се превърнаха в сериозен проблем за сигурността и идеално средство за шпионаж.

Киберсигурността е един от най-важните въпроси на деня. Компютърните мрежи винаги са били и ще бъдат обект на престъпниците, опасността от нарушения на сигурността в кибер пространство ще се увеличи, тъй като тези мрежи се разширяват. Необходими са разумни предпазни мерки, така че загубите да бъдат сведени до минимум.

Литература

1. Стоянов Н., Ст. Балабанов, Национален военен университет "Васил Левски" Факултет „Артилерия, ПВО и КИС", Научна сесия 2010, Сборник научни трудове, Част II, Шумен 2011, Кибератаките – новият инструмент в арсенала на армиите, стр. 37 – 42.

2. www.fas.org/sgp/crs/natsec/RL32777.pdf – Fischer E., Creating a National Framework for Cybersecurity: An Analysis of Issues and Options, The Library of Congress, 2005, 12.05.2011

3. Janczewski Lech J., University of Auckland, New Zealand, Andrew M. Colarik, AndrewColarik.com, USA Cyber Warfare and Cyber Terrorism, Information science reference, Hershey • New York, 2008

4. http://www.sans.org/reading_room/whitepapers/warfare/information-warfare-analysis-threat-cyberterrorism-critical-infrastruc_821, Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastruct;

5. http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.

„ИНТЕРНЕТ" – НЕОБХОДИМОСТ И ЗАПЛАХА

Калоян А. Илиев, Радослав Б. Чалъков

"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.

"INTERNET" - NECESSITY AND THREAT

Kaloyan A. Iliev, Radoslav B. Chalakov

Abstract: *In today's dynamic and full of risks world security issues come to the fore. Many aspects of security, the security of the Internet is only one of them and, unfortunately, often overlooked issue, although our lives are increasingly linked to the virtual space. We are constantly on-line, such as via the Internet looking for information, communicate, we carry out financial and other operations, etc. But to what extent are familiar with the risks that threaten us and we have built a culture of behavior on the Internet is a serious matter. Unfortunately, more and more people fall victim to various risks that lie lurking on the Internet.*

Keywords: *security issues, virtual space, information, Internet*

В днешния динамичен и изпълнен с рискове свят въпросите на сигурността излизат на преден план. Много са аспектите на сигурността, като сигурността на интернет е само един от тях и, за съжаление, често подценяван въпрос, въпреки че животът ни все повече се обвързва с виртуалното пространство. Ние сме постоянно он-лайн, като чрез интернет търсим информация, комуникираме, осъществяваме финансови и други операции и т.н. Доколко обаче сме запознати с рисковете, които ни заплашват и имаме ли изградена култура на поведение в интернет е сериозен въпрос. За съжаление все повече хора стават жертва на различните рискове, които ни дебнат в интернет.

За хора интернет се превръща все повече в потребност, като чрез мрежата те черпят познания, споделят информация, комуникират и т.н. Интернет създава сериозен потенциал за развитие, но същевременно крие и сериозни опасности, особено ако хора не ги познават и нямат знанията как да се предпазят. За съжаление все повече се увеличава броят на хората, които са станали жертва на престъпления, започнали или извършени чрез интернет. В същото време, хората не са обучавани и не знаят към кой държавен орган да се обърнат, когато установят неправомерни дейности в интернет.

Държавната комисия по сигурността на информацията използва следните определения за риск и заплаха: „Заплахата е опасност, възможност за поява на нещо неприятно, лошо", „Закана да се причини някому нещо неприятно, зло". При риска няма определено предварително време за настъпването му. Дори да бъде установен достатъчно рано, той си остава принципно невъзможен за неутрализиране. Редица проучвания и проекти в областта на киберсигурността и сигурността обръщат внимание на следните рискове и заплахи за младите хора в интернет като най-сериозни и/или най-често срещани са:

- Порнография, сексуални престъпления и насилие

Все повече хора биват излагани на този риск. Интернет все по-често се използва от потенциални и реални извършители на сексуални престъпления за подготовка на сексуални злоупотреби с деца, по-специално чрез сприятеляване с цел сексуална злоупотреба и детска порнография. Хора могат да станат жертва на т.нар. сексуални хищници, които в днешно време се насочват към социалните мрежи и примамват младежи, демонстрирайки привиден интерес към техните хобита, любими изпълнители, предавания и прочие. Така например педофили лесно могат да се доберат до лична информация - адрес, имена, профили, след което изпращат изображения и видео, които имат сексуално съдържание.

Освен прякото негативно въздействие, сайтове с порнографско съдържание често крият зловреден софтуер, който атакува компютрите при разглеждане на тези сайтове.

- Кибертормоз

Кибертормозът е съвкупно понятие за действия, които могат да навредят на даден индивид в интернет и включват заплахи, злоупотреби, следене или друго агресивно поведение, което е продължително във времето. Кибертормозът може да включва обидни реплики, публикуване на снимки в интернет без разрешението на притежателя им, споделяне на видеоклипове, които могат по някакъв начин да накърнят достойнството и доброто име. Противодействието срещу тази заплаха е особено трудно, тъй като извършителят остава неизвестен, а често използва идентичността на своя жертва и извършва кибертормоз от нейно име.

- Радикализация чрез интернет

Разпространението на радикални идеи или призиви към радикални действия, насочени срещу отделни хора или групи е все по-често явление. Свидетели сме на разпространение на радикални идеологии, насочени срещу малцинствени или религиозни социални групи. Интернет позволява и бързата организация на неограничен брой хора за извършване на радикални противозаконни действия.

Появата на т. нар. Ислямска държава и засилването на други терористични групировки даде тласък на този вид заплаха и доведе до стартирането на интернет кампании за привличането на бойци и симпатизанти. Това става чрез различни мултимедийни материали или обещания за заплащане и просперитет. Използвайки интернет терористите се насочват най-често към деца и юноши от проблемни семейства, т.нар социални аутсайдери, маргинализирани младежи или имигранти и бежанци. Тази заплаха включва и десният радикализъм - дискриминация на мюсюлмани и други малцинства, което се превръща във все по-голям проблем.

- Фишинг

Това е широко използван похват от компютърни престъпници за получаване на важна информация. Те просто създават съобщения или интернет сайт, които "претендират", че са добронамерени, като приканват да се въведе важна лична информация. При фишинга измамници разпращат електронна поща, която претендира, че идва от почтена компания и се опитва да убеди получателя да даде важна лична или финансова информация. Електронното съобщение обикновено моли да се изпрати в отговор или да се въведете на уебсайт, към който има връзка. Тези данни, например потребителски имена, пароли и номера на кредитни карти, после се използват от измамниците, за да се получат пари или услуги от името на пострадалия.

- Кражба на информация и използване на зловреден софтуер

Кражбата на информация е сериозна заплаха, тъй като може да доведе до кражба на идентичността в интернет, в който случай крадецът се представя за своята жертва и по този начин безнаказано извършва престъпления /в реалното и във виртуалното пространство/. Ако не се вземат своевременни мерки (като например докладване за откраднат профил до компетентните органи или администратори на съответния уебсайт), престъпленията могат да се припишат на жертвата. Хората често не обръщат внимание на последиците от споделянето на лична информация в киберпространството и пренебрегват декларациите за поверителност при използването на онлайн услуги. В съчетание с неприлагането на настройките за поверителност, споделената от тях лична информация е лесна плячка за различни видове зловреден софтуер, като тя може да бъде директно откраднатa или да бъде изтеглена без знанието на нейния собствени/автор за това. Тази информация може да се използва за проникване в устройствата за достъп до интернет (компютър, лаптоп, телефон и др.) и така злонамерени лица да се доберат до още по - голямо количество информация като лични снимки, пароли за уебсайтове, кодове на кредитни и дебитни карти.

- Кражба на самоличност

Извършва се, когато някой използва личните Ви данни, като име и фамилия, ЕГН, осигуровки, номера на кредитни/дебитни карти или друга идентифицираща Ви информация без Вашето знание и съгласие, за да извърши измама или други престъпления. В много случаи кражбата на самоличност се установява изключително късно, когато са направени непоправими щети на личността или имуществото.

- Игри, съдържащи насилие

Сред хората и по–често след младите все по-популярни стават видеоигрите, които съдържат насилие. Същевременно те крият риска от приемането на виртуалната реалност за действителна и пренасянето на виртуалния свят в реалния. Това може да доведе както до проблеми в общуването и социална изолация, така и до опити за пресъздаване на виртуалните изживявания. Специалисти все повече отчитат, че игрите, съдържащи насилие, играят важна роля в радикализирането на младежите и приобщаването им към различни терористични и криминални групировки.

- Онлайн финансови измами и други финансови рискове

Все по-голям е броят на пазаруване и разплащане за различни услуги чрез интернет. Въпреки че големите компании обръщат сериозно внимание върху сигурността, не са изключени ситуации, при които хората попадат на неистински търговци. Рискът се крие в извършването на самата транзакция и постигането на различен от очаквания резултат - заплатеният продукт или не се получава, получава се в занижено качество или количество или лицето се оказва обвързан с нежелан абонамент, за който плаща повече. Примерите в това отношение могат да бъдат многобройни.

Сред другите финансови рискове следва да се отбележи незаконният хазарт, което може да се отрази негативно на семейния бюджет, може и да се пренесе в реалния живот като превърне младия човек в редовен посетител на казина или да доведе до неговата задлъжнялост в резултат на онлайн играта. Собствениците на хазартни сайтове физически се намират в офшорни зони; в резултат на това операторите могат да променят, преместват или напълно да отстраняват сайтовете си в рамките на няколко минути. Тази възможност позволява недобросъвестните опера-

тори да вземат номера на кредитни карти, както и пари, депозирани в сметките на играчите, след което да закрият дейността си.

- Хакерство сред младите

Все по-популярна сред хора се превръща „професията“ хакер. Деца и юноши намират забавление и удоволствие, но най-вече усещане за предизвикателство при проникването в сайтове, кражбата на кодове, данни и пр. По този начин те се превръщат в част от проблема и излагат на риск свои връстници. В повечето случай това е невинна игра и не се получава сериозно увреждане на личността или собствеността, но има случаи на сериозни негативни последици.

- Плагиатство

Плагиатството е представянето на нечии мисли, идеи за свои собствени. Съществува целенасочено плагиатство, но в някои от случаите то е следствие от липсата на знания за правилата по използването и цитирането на чуждия труд. Последствията от плагиатството могат да бъдат изключване от образователни институции, съд или глоба. За да се предотвратят неблагоприятните последствия, хората трябва да бъдат запознати с правилата за използване на чуждия труд при техни разработки. Наблюденията показват, че това е изключително силно разпространено явление сред студентите, като повечето от тях не осъзнават или нямат информация, че неправомерното използване на чужд интелектуален продукт е престъпление.

- Рискове при запознанства в интернет

Рискът тук произтича от неспазването на определени правила, като например да не се споделя незабавно личната информация, уверение, че насрещната страна е такава, за каквото се представя (идентичността на другата страна, много престъпници скриват реалната си възраст, пол и намерения, възползвайки се от доверието на хората), срещата да се проведе на публично място, където има много хора и др.

- Пренебрегване на правилата за онлайн комуникация

Хора често не взимат необходимите мерки, за да гарантира своята сигурност при онлайн комуникация. Рискът е свързан с липсата на предпазливост, а донякъде и липса на култура за защита при онлайн комуникация. Това може да доведе до злоупотреба с лична информация, кражба на снимки, видео, нежелани контакти, попадане на неподходящо съдържание и др.

Изброените по-горе рискове са само една малка част от рисковете и заплахите в интернет. Интернет може да създаде рискове или чрез него традиционните рискове да се задълбочат. Необходимо да се засили общественото внимание към тези опасности. Те са многобройни и разнопосочни и същевременно се развиват бързо, еволюират и възникват все по - изобретателни методи, чрез които се застрашава сигурността на хората в интернет. Нека да не забравяме, че интернет създава изключителни възможности за получаване и обмен на информация, за извършване на различни дейности, които ни обогатяват или правят живота ни по - лесен, но в същото време той крие и рискове, които ние трябва да познаваме, за да се защитим.

Нека да вземем за пример тийнейджърите. Те са индивиди, които започват да изграждат свой личен живот и дълготрайни социални контакти, но имат стремеж да водят този живот независимо от своите родители. Всъщност това е процес, при който те търсят своето място в обществото и своята идентичност. В много случаи се сблъскват с обществени нагласи, които не им импонират. Получават се конфликти между установените принципи в обществото, от една страна, и желанието, амбициите на младежите, от друга. Голяма част от хората, които се радикализират

го правят именно на тази основа – те се чувстват неразбрани, не намират място в обществото, не споделят неговите норми и смятат, че то ги потиска. Лица с престъпни намерения, използващи интернет, се възползват от това и атакуват именно тази част от съзнанието на младите хора, като се представят за приятели, разбиращи и симпатизиращи на намеренията и целите им, насърчаващи ги да не слушат родителите си. Постепенно, стъпка по стъпка, те печелят доверие, което улеснява извършването на избраното от тях престъпление.

Друга причина се състои в емоционалната уязвимост. Много деца и юноши се чувстват несигурни, особено когато са поставени в условията да заемат по-ниско социално положение сред своите връстници. Те често изпитват проблеми у дома, което поражда у тях нуждата да търсят тръпка, ново усещане, риск, какъвто може да е случаят при срещата с непознат от интернет. Около 30% от децата в ЕС имат контакти, с които са се запознали онлайн, а 23% от тях се запознават с пет или повече души. Девет процента от тези деца са се срещали на живо със свои онлайн. От друга страна същият риск се отнася и за т.нар. „лидери" на социалните групи или „популярните", за които статистиката показва, че рискуват запознанства на живо поради голямата си увереност. Към списъка с причини следва да добавим и начина, по който в интернет се използва интересът на младите към игри, гатанки, предизвикателства и задачи. В много сайтове с игри често може да се открие зловреден софтуер, а една от тактиките на престъпниците включва привличане на вниманието чрез сложни задачи и загадки. В заключение по този аспект следва да отбележим, че причините за уязвимостта се крият както в самия живот, който младите водят, така и в степента им на запознатост със заплахите, които киберпространството крие.

Посочването на рисковете и причините за уязвимостта на младите в интернет логично води към следващия въпрос, а именно какви са добрите практики в справянето с тези проблеми. В Европа Държавите членки на ЕС са възприели различни подходи и прилагат многобройни решения, ето и някои от тях:

В Латвия впечатление прави проектът Net-Safe, който препоръчва обучението на младите хора по безопасност в интернет да се съчетае с атрактивни за тях дейности. В сайта на проекта посетителите могат да свирят на пиано, да решават забавни и същевременно образователни тестове. Сред една от интересните и иновативни идеи е създаването на форум, в който хората могат взаимно да се образоват по въпросите на интернет безопасността, да споделят полезни идеи и информация, а също така и неприятни преживявания.

Доклад за рисковете и безопасността на младите в интернет във Франция показва, че ролята на родителите в страната е голяма и те са първият източник, към който младите хора се обръщат за помощ и съвети в интернет. Словакия представлява интересен пример, тъй като един от основните рискове се крие в социалните мрежи, риск илюстриран от факта, че 81% от словашките тийнейджъри използват „Фейсбук" всеки ден. Препоръчват се също така съвместни обучения между родители и деца, които от ранна възраст да повишат своята култура на сигурност и така да се установи връзка на доверие между родител и дете по отношение на сърфирането в интернет. Редица проучвания, съфинансирани от институциите на ЕС, сочат, че според родителите някои от най-добрите практики в повишаване на интернет безопасността са обученията на децата и юношите в училище, по-достъпна и разбираема информация, която да запознае самите родители с рисковете, обучения и

курсове за самите родители, които да бъдат организирани от правителствата или местните власти.

В Обединеното кралство се обръща сериозно внимание на мнението на младите хора по отношение на сигурността в интернет, което има принос към политиките, които се развиват в тази област и специфичните проблеми, които могат да възникнат. Акцентира се върху ролята, която училищата и университетите имат в запознаването на деца и юноши с въпросите за сигурността в интернет и е създаден специален сайт с практични съвети за организации различни от училища и университети, които работят с млади хора.

В Германия филтрирането на определено онлайн съдържание е нещо, зад което застават мнозинството родители. Много немски мобилни оператори са създали софтуер, посветен на родителския контрол и същевременно са подписали различни кодекси, свързани със защитата при сърфиране от мобилни устройства.

Европейският съюз взема мерки за подобряване на сигурността в интернет като насърчава саморегулацията и съвместната регулация на интернет пространството и неговата безопасност чрез публично-частно партньорство с IT компании, интернет доставчици и социални мрежи, които доброволно се ангажират с тази задача. Тежестта на превантивните мерки срещу кибертормоза нараства все повече, тъй като голяма част от него се извършва от деца или тийнейджъри и затова е важно в училищата да се работи по този проблем и да се насърчава отделянето на повече време за децата днес, за да не се превърнат в престъпници утре.

Политиките на правителствено ниво трябва да дадат основната насока за развитието на сигурността на младите в интернет. Някои държави членки възприемат цялостни национални стратегии за сигурността на децата в интернет (Великобритания) , други залагат на институцията на омбудсмана за защита правата на децата (Унгария и Полша) или са създадени специални органи, които се занимават с предпазването на младите в интернет и сътрудничат тясно с органите на реда, медиите, мобилните оператори и интернет доставчиците.

В много европейски училища програмата за обучение по онлайн сигурност е съобразена с възрастта на учениците. Във Великобритания много деца се канят на форуми, посветени на онлайн рисковете и политиките за противодействие, за да дадат своето мнение, т.е. на тях се гледа като на активна заинтересована страна. Младите хора, успешно преминали обучения за безопасност в интернет се привличат за работа със свои връстници, които все още не са запознати с тези въпроси.

Европейската стратегия за интернет сигурност препоръчва засилване на интернет сигурността на ниво местна власт и създаване на местни е-правителства, като се прилага принципът на продължителното обучение на служителите, тъй като поради бързите технологични промени, методите за измама се подобряват19.

В България все още не съществува стратегия, насочена към преодоляване на рисковете за сигурността на младите хора в интернет. Компетенциите в тази сфера са разпределени между различни държавни органи, но това е още една предпоставка да се размива отговорността.

Нека не забравяме, че основата в борбата с престъпленията, включително и тези, свързани с интернет, е превенцията.

По данни на Националния статистически институт около 83% от българските граждани на възраст между 16 и 24 години редовно използват интернет. Ако прибавим към тази цифра децата под 16 години, тогава цифрата може да скочи до 90%,

както стана ясно на провелата се кръгла маса по въпросите на защитата на децата в интернет пространството, организирана от Министерството на транспорта, информационните технологии и съобщенията. От друга страна проучване, извършено за Европейската комисия от мрежата European Schoolnet и Университетът в Лиеж показва, че българските осмокласници са сред най-неуверените в ЕС по отношение на своята онлайн безопасност.

В България като цяло проблемите, свързани със сигурността в интернет се подценяват. Затова говори и фактът, че в България няма единен орган, който да се занимава с политиките и мерките в областта на киберсигурността. Все още няма и разработена стратегия за киберсигурност, въпреки че няколко поредни правителства си поставят нейното приемане като приоритет.

Отделни министерства и държавни органи са изградили способности за превенция на рисковете във виртуалното пространство, но това е по-скоро в резултат на реализацията на секторните политики, за които те са отговорни, но не и цялостна визия. Както редица европейски държави и България следва да създаде свой национален орган в областта на киберсигурността, който да гледа глобално на тези въпроси, необходимо е осъвременяване на законодателството и предприемане на конкретни практически стъпки в тази насока.

Като особено уязвима група, каквато са младите, държавните институция трябва да имат един по-широк поглед при информирането за рисковете и представянето на мерките, които младите трябва да предприемат за тяхната лична безопасност в интернет. Отделните инициативи на фирми и неправителствени организации са полезни, но сигурността на младите в интернет трябва да се превърне в устойчива държавна политика, а тъй като младежта е бъдещето на всяка една държава това ще е полезно и за цялото общество.

Изводи:

1. Да се предприемат действия за обучение на хората още от рано детство за работа в интернет. Важно е създаването на култура за работа в тази среда. Най-удачно би било да се включат в училищното образование определени модули, съобразени с възрастта на учениците.

2. Да се приеме Национална стратегия за киберсигурност, като специално внимание в нея да бъде отделено на младите хора като една от най-застрашените групи от кибер-рискове.

3. Да се работи с родителите с цел да се повиши родителския контрол върху ползването на интернет от младите хора, като за целта е подходящо обсъждане на тези въпроси на родителски срещи в училище.

4. Необходима е координация между държавните органи, бизнеса, неправителствения сектор и академичните среди за противодействие на рисковете в интернет и за подпомагане на младите хора да се справят с тях.

Литература:

1. Фондация "Партньори-България" - Безопасно използване на интернет- http://partnersbg. org/2013/03/safe-internet/

2. Държавна комисия по сигурността на информацията, Рискове за интересите на Република България в областта на защитата на класифицираната информация.

3. Сигурност на младите в интернет- http://safe.teacher.bg/html/etusivu.htm

4. Cyber Safety, An Interactive Guide to Staying Safe on the Internet

5. European Internet Security Strategy, European Union, April 2013.

6. https://en.wikipedia.org/wiki/Internet_safety

7. https://www.microsoft.com/bulgaria/press/news_15122010.mspx

8. http://www.ofcom.org.uk/

9. http://www.saferinternetday.org/web/bulgaria/home

10.http://www.saferinternetday.org/web/guest;jsessionid=166DDAEEBB283440677EA1AF49C 1C604

ИЗИСКВАНИЯ КЪМ ПРОГРАМНО ОСИГУРЯВАНЕ ЗА АВТОМАТИЗИРАНА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ОГЪНЯ НА АРТИЛЕРИЙСКИТЕ ФОРМИРОВАНИЯ

Дилян К. Марков

SOFTWARE REQUIREMENTS FOR AUTOMATED ARTILLERY FIRE CONTROL SYSTEM

Dilyan K. Markov

Abstract: *This report introduces software requirements for automated artillery fire control system for taking part of artillery units in Combined Joint Tasks Force operations. It indicates general requirements for software for planning and decision-making process in the preparing of fire, targeting and fire control.*

Keywords *– computer software, automated fire control system, artillery units, fire support.*

1. Въведение

В програмата за развитие на отбранителните способности на въоръжените сили на Република България 2020 се посочва, че планирането на отбраната ще се извършва с цел определяне, изграждане и развитие на необходимите отбранителни способности и на необходимите за тях човешки, финансови, материални и други ресурси и услуги. Планирането и реализирането на проекти за изграждане, развитие и поддръжка на национални отбранителни способности се извършва интегрирано с процесите на отбранителното планиране в НАТО и развитието на военните способности на ЕС, с използване на възможностите за постигане на максимален ефект при оптимален разход на ресурси и с разработване на ориентиран към резултатите програмен бюджет. [11].

Отбранителните способности на въоръжените сили са съвкупност от следните елементи: доктрини и концепции; организационна структура; подготовка; материални средства; командване и управление; личен състав; инфраструктура и оперативна съвместимост. Съвкупността от всички посочени компоненти осигурява наличието на отбранителните способности. Необходимите оперативни способности, които трябва да постигнат формированията за осъществяване на огнева поддръжка са способностите, необходими за успешното изпълнение на поставените задачи. Тяхното развитие, определено от приоритетните насоки за повишаване на тези способности на формированията за огнева поддръжка би довело до:

- повишаване на огневата мощ на маневрените формирования;
- повишаване качеството и централизиране на управлението на артилерийските формирования при осъществяване на артилерийската огнева поддръжка;
- повишаване качеството на командването и управлението на артилерийските формирования;
- повишаване нивото на подготовката на артилерийските формирования;
- подобряване на комуникацията между формированията. [12].

Изискванията за рационализация, стандартизация и съвместимост фокусират съвместните усилия за преодоляване на националните различия и повишаване на

съвместния колективен потенциал. Ефективното планиране, добре организираните съвместни дейности, координацията и сътрудничеството на всички нива, тясното взаимодействие и обединяването на усилията са от съществено значение за повишаването на бойната ефективност и бойния потенциал и снижаване до минимум вероятността за получаване на съпътстващи загуби от приятелски огън при провеждане на операциите. Това налага предприемане непрекъснато на необходимите мерки за въвеждане на единни дефиниции и терминология, хармонизиране на действащите доктрини и техники, тактики и процедури и покриване на единни стандарти при използвана на автоматизирани системи за управление на огъня на артилерията.

2. Използване на автоматизирани системи за управление на огъня на артилерията в Българската армия

Използването на автоматизирани системи за управление на огъня на артилерията в БА е от края на 1989 г., когато се извършиха изпитания на първата българска автоматизирана система за управление на огъня на артилерийски дивизион (АСУОАД) „Искра".

Отчитайки нейните недостатъци и внедрявайки новите постижения в тази област през 1999г. започнаха изпитания на АСУОАД „Вулкан" и през 2003 г. беше въведена на въоръжение АСУОАД „Вулкан–С" ПИКИС, която повиши значително бойните възможности на дивизионите за непосредствена огнева поддръжка. [3, 5].

От 2004г. България е равноправен член на НАТО. Въоръжените сили на всички нации в Северноатлантическия пакт могат да работят ефективно заедно, само ако са установени ясни разпоредби, правила и притежават необходимите способности гарантиращи точното разбиране и гладкото сътрудничество между тях.

Анализът на използваната в момента в Сухопътните войски автоматизирана система и възможностите на артилерийските формирования, въоръжени с нея в многонационални съвместни действия показва, че тя не осигурява изискванията за осъществяване на огнева поддръжка на маневрените формирования, съгласно процедурите за огнева поддръжка. Софтуерният продукт е разработен преди повече от десетилетие. Той се използва само от дивизионите за непосредствена огнева поддръжка и ограничава действията им, при което възпрепятства изграждането на необходимите способности за ефективно поразяване на целите и управление на огневата поддръжка. [6].

За да се справи с предизвикателствата при участие в многонационални съвместни операции всяко артилерийско формирование трябва да притежава автоматизирана система за управление на огъня (АСУО), интегрирана с националните комуникационно-информационни ситеми и автоматизираните системи за управление на огъня в страните членки на НАТО. Това може да се постигне преди всичко със съвременно програмно осигуряване и съвместими средства за комуникационно-информационна поддръжка.

Настоящият доклад посочва само изискванията за програмно осигуряване за автоматзирана система за управление на огъня на артилерийските формирования.

3. Изисквания към програмно осигуряване за автоматизирана система за управление на огъня на артилерийските формирования

В следствие на опита от използването на АСУОАД „Вулкан–С" ПИКИС в Българската армия, анализа на АСУО в страните членки на НАТО, насоките за развитие на автоматизираните системи в световен мащаб и възможността да бъде интегрирана една АСУО за нуждите на сухопътните войски на Българската армия, могат да бъдат определени изискванията към програмно осигуряване, което трябва да притежава една АСУО, при участие на артилерийските формирования в многонационални съвместни операции. [1, 2, 15, 20].

3.1. Общи изисквания:

- Да се използва за различни йерархични нива в полевата артилерия – разчет, взвод, батарея, дивизион, елемент на огневата поддръжка на батальон, център за координиране на огневата поддръжка на бригада и център за огнева поддръжка на сухопътен компонент.

- Да осигурява възможност за обмен на информация между АСУО и други системи за управление на огъня в НАТО и информационни системи на БА. [6, 19].

- Автоматично да получава и разпространява от или до други системи и между потребителите, съгласно йерархичното ниво: електронна картина на бойното поле, заповеди, директиви, съобщения и информация, предназначени за елементите на системата за огнева поддръжка, използвайки свободна форма или такава в зададен формат (текстов, графичен или комбиниран), както и друга информация за планиране и водене на бойните действия. [14].

- Да осигурява работа с всички артилерийски системи на въоръжение в Българската армия (2С-1, Д-20, БМ – 21, Б1-10, М-30, 82мм МХ), без ограничение на техния брой, формирования, йерархично ниво и компютърни конфигурации.

- Всички елементи на системата трябва да могат да работят самостоятелно, в случай на пълно или частично откъсване от АСУО. След възстановяване на работата, системата трябва да бъде в състояние автоматично да продължи своята дейност, като запише новите данни от включените потребители и актуализира данните на всички в зададената конфигурация.

- Да осигурява възможност за непрекъснато актуализиране, редактиране, разширяване и персонализиране според действителните нужди на потребителите.

- В случай на автоматично изпълнение на дадена операция, която е лишена от необходимите данни, програмата трябва да уведоми съответния оператор с конкретно искане за въвеждане на липсващи данни.

- Да не възпрепятства работата на системата и да осигурява устойчивост от прихващане и заглушаване. Това изискване се фокусира върху комуникационните устройства, които ще предоставят трансфер на данни. Комуникационните устройства трябва да гарантират обмен на глас и данни в необходимия обхват. [15].

- Да отговаря на изискванията за информационна сигурност. Степента на защита на информация трябва да бъде с определено в заданието ниво на класификация. Да разрешава достъпа само за лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп. [7, 10].

- Да осигурява информацията, която се създава, обработва, предоставя, съхранява и унищожава да се извършва при условията и по реда на Закона за класифицираната информация и подзаконовите актове за прилагането му, както и в съответствие с предвидените видове защита, съответстващи на нивото на класифика-

ция, ако програмното осигуряване бъде класифицирано, с ниво на класификация за сигурност. [7, 10].

- Да може създава, обработва и предоставя форматирани съобщения съгласно NATO STANAG 2434 Compendium of Allied Land Forces Messages – APP-9. [9, 18].

- Да има възможност да изобразява, по стандартите на NATO Joint Military Symbology, APP-6(C) по решение на оператора:

  • бойния ред на собствените артилерийски системи;

  • целите за поразяване;

  • цифров модел на бойните действия с мерките за координиране на огневата поддръжка;

  • тактически знаци - според точното местоположение на елементите от бойния ред, както и да се обновяват автоматично при смяна на координатите на елементите. [21].

- Да отговаря на изискванията за безопасност от поразяване на собствените войски или водене на огън в зони забранени за стрелба или с ограничение за водене на огън, като автоматично изпраща предупредително съобщение, но да разрешава водене на огън в тези зони по зададен код от оператора.

- Автоматично да получава, обработва, съхранява и разпространява данни от работни станции, оръжейни системи и разузнавателни средства и сензори.

- Автоматично да променя настройките си за подател или получател на електронната картина на бойното поле, заповедите, директивите, съобщенията и информацията, предназначена за елементите на АСУО, при загуба на връзка с получателя. Това означава, че системата на изпращане и получаване трябва да има няколко канала за пренос на данни. Такава ситуация би се получила когато стандартните елементи са елиминирани, заглушени или не са функционални по други причини.

3.2. Изисквания при планиране и вземане на решение:

- Да изпълнява ролята на автоматизиран инструмент в помощ на командира при вземане на решение, което предполага включването на стандартни решения и предоставяне на изчисления, необходими за изпълнение на тактически и технически контрол на артилерийския огън, както и възможността от запазване правото на избор при нестандартни решения от страна на командира, при отчитане на неговата отговорност за взетите решения. [15].

- Да осигурява на автоматизираната система за управление на огъня самостоятелна работа без да е необходимо да се потвърждава предложеното решение, за определяне на средсвото за поразяване на целта и данните по нея.

- Да осигурява планиране на бойното и логистичното осигуряване.

- Да осигурява комплексно планиране на огъня и маньовъра.

- Съхранение на пълна бойна документация, която ще се използва по време на процеса на планиране и ще бъде на разположение след утвърждаване от страна на командира. Това са документи, необходими за планиране и водене на бойните действия на разчет, взвод, батарея, дивизион, елемент на огневата поддръжка на батальон, център за координиране на огневата поддръжка на бригада и център за огнева поддръжка на сухопътен компонент. [13].

- Да предостави достъп до документи и информация на всички командни нива в системата за организиране на взаимодействието.

- Да изисква регистриране на потребител в случай на искане за печат за всеки документ. Системата трябва да попълни автоматично други данни, като дата, час, място на създаването на документа, както и серийния номер. За да се постигне това, системата трябва да бъде в състояние автоматично да определи точното местно време, както и местоположението на лицето създало документа.

- За да се определят бойните припаси необходими за поразяване на целите програмата трябва автоматично да получава информация от оръжейните системи, включително брой, видове снаряди, взриватели и заряди. Въз основа на тази информация тя ще осигури реалното обобщение за наличието на боеприпаси. В случай на първоначално планиране на разхода на бойни припаси, както и при намаляването им под зададено ниво, системата автоматично да иска снабдяване чрез изпращане на доклад до пункта за управление на логистичното осигуряване (ПУЛО) на формированието.

- Автоматично да предлага мерките за координиране на огневата поддръжка, при зададени критерии от оператора.

3.3. Подготовка на стрелбата и управлението на огъня:

- Да може да се използва във всички области на земното кълбо, без ограничения. [15].

- Да позволява предварително въвеждане на всички необходими данни и да ги съхранявате в паметта, както и добавянето на други в последствие (придобити по-късно, променени или допълнени) към масивите:

• характеристики на оръжейните системи, боеприпаси, артилерийски разузнавателни средства и други сензори, или информация за действителното местоположение на разузнавателните елементите;

• точното местоположение на средствата за огнево поразяване, както и далекобойността, основното направление, зоните за огнево поразяване и др.;

• местоположението на средствата за артилерийското разузнаване, секторите за наблюдение и технически възможности за разузнаване.

- Да позволява изчисляване, въвеждане и използване на данни за топогеодезическата подготовка на стрелбата:

• Възможност за работа с цифрови карти с координатни системи World Geodetic System 1984 (WGS 84) и координатна система, на основата на Гаус — Крюгерова проекция СК 42. [22, 23]. Системата автоматично да преобразува координатите ако са били въведени при по-рано зададена координатна система, както и при преминаване от зона в зона. Координатите на всички точки, да се съхраняват с пълни правоъгълни координати. Системата трябва да позволява бързото зареждане на картите, както и подновяване при наличие на актуализации.

• Да използва ъгломерни деления, равни на 1/6000 части от окръжността и NATO mils, равни на 1/6400 части от окръжността за мерки за измерване и изчисляване на ъгли.

- Да позволява на всеки потребител на ниво командир на огневи взвод, оператор в тактически оперативен център на дивизион и оператор в център за координиране на огнева поддръжка в маневрено формирование да съставя метеобюлетини по стандарта на METEO 11, METEO 44 и METCM, както и да получава същите от съюзни метеорологични станции, както и да ги обработва и изпраща до всеки потребител от АСУО. Да оценява валидността им, както по време, така и в пространс-

твото. Своевременно да изпраща автоматично предупреждение, когато формированието се нуждае от метеоданни, за да се актуализират метеорологичните условия на стрелбата. [4].

- Да позволява изчисляване, въвеждане и използване на данни за балистическата подготовка на стрелбата:

• за отклонението в началната скорост на снаряда;

• за температурата на заряда, като да има възможност непрекъснато да следи за нейното измерване в артилерийските системи и при изтичане на времето от предходното отчитане да изпраща потребителско съобщение за ново измерване;

• за балистическите характеристики на снарядите;

• за сортирането на снарядите.

- Да позволява въвеждане и използване на данни за техническите поправки на системите.

- Да предлага най-изгодния заряд за стрелба, съгласно правилата за стрелба и управление на огъня, както и въвеждане на постоянен заряд от оператора.

- Винаги да използва най-точният способ за изчисляване на данните за стрелба. Когато няма достатъчно данни за пълна подготовка на стрелбата да уведомява оператора за конкретните липсващи данни. Операторът да може да вземе мерки за допълване на данните или да игнорира уведомлението на система, като използва друг, способ.

3.4. Целеобразуване и целеразпределение:

- Да осигурява извършване на процеса на целеобразуване и целеразпределение.

- Да осигурява използване на данни, предоставени от съюзнически безпилотни летателни апарати, радиолокационни станции, разузнаване на авиацията и др.

- Да осигурява автоматизиране на процесите при засичане на целите и изпращане на данните за тях от разузнавателните групи на маневреното формирование и специалните сили.

- Да осигурява автоматизиране на процесите при засичане на целите и тяхното разпределение за средствата за огнево поразяване (авиация, артилерия и др.) в системата за огнева поддръжка на батальона, бригадата и сухопътния компонент. [8, 16].

- Автоматично да добавя липсващите данни във всички документи, с акцент върху използването на правоъгълни и полярни координати в координатния списък на целите, който да бъде приложение към бойната заповед със следните изисквания:

• да предоставя директно данни за целите, необходими за извършване на изчисления в цялата система;

• да служи като документ при засичането и поразяане на целите.

- Активиране на системата при откриване на цел с висок приоритет за всеки период, задача или фаза на операцията. Тази функция се превръща в решаваща в случай на делегиране на правата от командира към дадено огнево формирование.

- Автоматично да извежда диалогов прозорец за огнева задача при избор на целта от цифровата подложка на екрана.

- При избора на средство за поразяване програмата трябва да провери автоматично, дали средството има свободни огневи ресурси и дали е на огнева позиция

за изпълнение на дадената задача. За да се постигне това, системата трябва да бъде в състояние автоматично да получава доклади за действителната дейност на оръжейните системи.

- Командата за поразяване на цел, предлагана от програмата трябва да съдържа:
  - огнево средство за изпълнение на задачата;
  - номер и характер на целта;
  - вид на огъня;
  - метод за определяне на данни за стрелба;
  - ограничения, съгласно мерките за координиране на огневата поддръжка;
  - продължителност на огъня;
  - метод на поразяване на целта.
- Да дава възможност за засичане на целите от всеки потребител, като въвежда автоматично уникален номер за всяка цел и предлага най-ефективен огън и средство за поразяване.

3.5. Изисквания при управление на огъня и контрол:

- Автоматично да записва хронологично във времето всички дани за поразяването на целите – кой е засякъл целта, кой е заповядал поразяването й, кой е водил огън и времената за това. Това означава, че ще бъде възможно да се определи точно кой, кога и как е бил оторизиран да влезе в системата и какви действия са извършени от този акаунт.
- Да работи със зададени процедури по управление на огъня.
- Да се използва за управление на формирования при изпълнение на тактическите задачи на полевата артилерия – „Непосредствена поддръжка“, „Усилване“, „Обща поддръжка-усилване“ и „Обща поддръжка“.
- Да изчислява времето за началото и края на огневата задача съгласно матрицата на огъня на формированието.
- Да изчислява разхода на бойните припаси по целите, като предлага необходимата степен за поразяване.
- При изпълнение на огнева задача системата автоматично да определя всички изисквания на правилата за стрелба и управление на огъня към поразяването на целта – способ на обстрел, процент на поразяване, размери на целта, разход на бойни припаси. [17].
- В случай на искане на огън по две различни цели по едно и същото време, когато няма достатъчно свободни огневи ресурси, да избере целта с по-висок приоритет, като я предложи за поразяване със свободно огнево формирование.
- Да предлага поразяване на цел с големи размери от две и повече формирования с еднакви или различни оръжейни системи по едно и също време, като отчита разстоянията на стрелбата и времелетенето на снарядите (мините) за попадения по едно и също време.
- Да позволява водене на динамична стрелба, като извършва изчисления за изстрелване на два снаряда от едно огнево средство и получаване на попадения в един и същ момент на тези снаряди в целта.
- Да използва данните от коригирането на огъня от едно огнево средство или едно формирование, като ги изчислява за цялото формирование или за друго в процеса на управление на огъня.

4. Заключение

Едно програмно осигуряване, което трябва да притежава една автоматизирана система за управление на огъня, при участие на артилерийските формирования в многонационални съвместни операции трябва да се развива по начин, който ще подпомага командирите от всички степени и всички други поддържащи елементи по време на всички дейности, свързани с оперативната обстановка, управлението на огъня, планирането на огъня, маньовъра и логистичното осигуряване. Също така не трябва да ограничава по никакъв начин действията на елементите на бойния ред, осъществяването на контрола и координация. Трябва да предостави на потребителя стандартни решения за всяка ситуация и да бъде в състояние за относително самостоятелна работа, по оста цел-средство за поразяване. Да не възпрепятства работата на системата и да осигурява устойчивост от прихващане и заглушаване. За да се изпълнят всички посочени изисквания в доклада, най–важно е тясно сътрудничество между програмисти и експертите в полевата артилерия.

Литература:

1. Автоматизирана система за управление на артилерийски дивизион АСУОАД (Б) „Вулкан – С" ПИКИС. Ръководство за оператора на бордов компютър. София, 2002г.

2. Десев, Х. Интегрираност в съвременните системи за управление на огневата поддръжка на западноевропейските държави. Артилерийски преглед, 3/2009г.

3. Досев, Н. „Вулкан-С ПИКИС – С4I" - системата на БА. //Сборник научни трудове, Шумен: Факултет „Артилерия, ПВО и КИС", 2007г.

4. Евлогиев С. , Д. Марков. Използване на метеобюлетин METCM в артилерийските формирования на българската армия. Международна научна кондеренция. НВУ „Васил Левски", Факултет „Артилерия, ПВО и КИС", Шумен, 09.2016

5. Евлогиев, С., Д. Марков. Полевите информационни системи - настояще и бъдеще. Международна научна конференция, сборник трудове. Командване на сухопътните войски и Асоциация на сухопътните войски на България. София. 2016г.

6. Евлогиев, С., Д. Марков. Управление на огъня на артилерийските формирования с използване на автоматизирани системи за управление. Монография. Шумен 2016г.

7. Закон за защита на класифицираната информация. ДВ. бр.71 от 13 Септември 2016г.

8. Концепция за съвместна огнева поддръжка. МО, София 2016г.

9. Ламбева, М., Драганов, Д., Христозов, И. Оценка на възможността за интегриране на полевите информационни системи. CIO,15.07.2011,<http://cio.bg/3969_ocenka_na_vazmozhnosta_za_integrirane_na_polevite_informacionni_sistemi#!prettyPhoto>достъп на 20.03.2017г.

10. Правилник за прилагане на закона за защита на класифицираната информация. ДВ. бр.64 от 16 Август 2016г.

11. Програма за развитие на отбранителните способности на въоръжените сили на Република България 2020. Министерски съвет на Република България. София. 2015г.

12. Протокол за реализиране на предложенията от дискусия на тема: „Проблеми при интегриране на полевата артилерия в системата за огнева поддръжка при

участие на формирования от Българската армия в многонационални съвместни операции“, проведена от 23 до 24 февруари 2017 г. във факултет „Артилерия, ПВО и КИС” на НВУ „Васил Левски”

13. Ръководство за използване на полевата артилерия – артилерийски дивизион. ВИ 2009г.

14. Ръководство за планиране на операции, част III – тактическо ниво. МО, София 2013г.

15. Blaha. M, B. Přikryl, K. Šilinger, L. Potužák, T. Havlík. Fundamental Requirements for the Automated Fire Control System for Field Artillery. International journal of systems applications, engineering & development, 10.2016

16. Joint Publication 3-60 - Joint Targeting - 31 January 2013

17. NATO Standardization Agency. AArtyP-1 (A) – Artillery Procedures. STANAG 2934. Brussels, Belgium, 2004.

18. NATO Standardization Agency. Compendium of Allied Land Forces Messages – APP-9, NATO STANAG 2434

19. NATO Standardization Agency. AArtyP-5 (A) – NATO Indirect Fire Systems Tactical Doctrine. Brussels, Belgium, 2014.

20. NATO Standardization Agency. Field Artillery And Fire Support Data Interoperability. STANAG 2245.

21. NATO Standardization Agency. Joint Military Symbology APP-6(C). May 2011

22. NATO Standardization Agency. Geodetic Datums, Projections, Grids, And Grid References, NATO STANAG 2211

23. <http://kpfu.ru/portal/docs/F1662326631/metodichka_sk42.pdf> достъп на 25.03.2017г.

ИЗСЛЕДВАНЕ НА РАЗЛИЧНИ АСПЕКТИ НА ПРОСТИТУЦИЯТА И РОЛЯТА Й ЗА НАЦИОНАЛНАТА СИГУРНОСТ

Венелин Терзиев
Национален военен университет „Васил Левски“, Велико Търново
Русенски университет „Ангел Кънчев“, Русе
Висше училище по телекомуникации и пощи, София
Никола Ничев
Национален военен университет „Васил Левски“, Велико Търново
Христо Бонев
Национален военен университет „Васил Левски“, Велико Търново

SURVEY ON VARIOUS ASPECTS OF PROSTITUTION AND ITS ROLE FOR THE NATIONAL SECURITY

Venelin Terziev
Professor, Ph.D., D.Sc. (National Security), D.Sc. (Ec.),
University of Rousse, Rousse, Bulgaria,
National Military University, Veliko Tarnovo, Bulgaria
University of Telecommunications and Post, Sofia, Bulgaria
Nikolay Nichev
Colonel, Associate Professor, Ph.D.,
National Military University, Veliko Tarnovo, Bulgaria
Hristo Bonev
Ph.D. student,
National Military University, Veliko Tarnovo, Bulgaria

Abstract: *The study attempts to present a summary analysis and a historical-psychological review of the prostitution as a problem. The prudential nature of the analyzed and investigated scientific and other sources gives grounds to consider different hypotheses about the impact of these processes and phenomena on the national security system.*

Key words: *national security, prostitution, governance.*

ВЪВЕДЕНИЕ

Много са измеренията на проблема проституция - или предлагането на секс срещу пари. Този проблем генерира не само етична алтернатива, но и въпроси, свързани с безопасността на проституиращите (без оглед на тяхната възраст и пола им), с нарушаването на човешките им права, с връзката им с организираната престъпност. Лицата, предлагащи платен секс, често са определяни като рискова група по отношение на употребата на наркотици, посегателствата срещу личността и разпространението на социално значими заболявания, каквито са венерическите. Проституцията често се определя като модерна форма на робство и се свързва с трафика на хора, което е едно от най-тежките престъпления в световен мащаб [1].

Акцентът на борбата в България срещу тази сексуална експлоатация обикновено се поставя върху международния трафик на хора. Най-често усилията на правоохранителните органи се насочват към разкриване и противодействие на трафикан-

тите, действащи на територията на чужди държави. Не се проследяват обаче криминалните мрежи, с които те са свързани в България. Направените анализи показват, че в повечето случаи проституцията у нас прелива в международен трафик на „бели робини". И това е естествено, тъй като – водена от възможностите за значително по-високи доходи в чужбина – организираната престъпност се е ориентирала към износа на проституция. Паралелно с това престъпните групи развиват и поддържат богата вътрешна мрежа от проститутки и сводници.

Всъщност сексуалната експлоатация и проституцията са се превърнали в една от сериозните социални язви на съвременното българско общество. Учудване предизвиква в такъв случай фактът, че въпреки това този остър проблем е привлякъл твърде слабо вниманието на законодателя. Независимо от големите промени в България през последните две десетилетия, законодателството в тази област не е актуализирано. Нормативните актове, които действат до този момент, са почти архаични и не отразяват по съответен начин действителността. За решаваните проблеми не успява да допринесе дори тълкувателното решение №2 на Върховния касационен съд от 2009 г. относно трафика на хора и експлоатацията на хора.

Не е на необходимото равнище и реакцията на правоохранителните органи. Слабата организация на противодействието в комбинация с неадекватното законодателство позволяват години наред на проституцията да процъфтява и – най-важното – да се контролира от организираната престъпност, която натрупва от нея значителни незаконни доходи. Нещо повече – те улесняват преминаването на вътрешната проституция към много по-доходоносните пазари в страни от Западна Европа, САЩ, даже ЮАР. В резултат на това рязко нараства международният трафик на българки. Според едно изследване на Европол. България е един от шестте основни източника на жертви на трафика на хора. Информацията от изследванията, показва значително припокриване на престъпните структури, контролиращи проституцията в България и износа на такъв вид престъпна дейност зад териториалните граници. За това успешното противодействие на трафика на хора изисква адекватни мерки срещу вътрешната проституция и контролиращите я престъпни структури, които са развили стабилна мрежа в цялата страна [2].

Подчинената роля на жената е известна схема на поведение в историческия дискурс на мъжкия символен ред. Битуването на този предразсъдък е относително консервативен поведенчески модел в патриархалното общество. Въпреки че моралните системи се променят със смяната на културните епохи, очевидно антиженската тенденция остава относително постоянна. Несъмнено важна роля за упоритата дисимилация на жените играе колективното несъзнавано и архитипните инициации на мъжкия пол. Основните предпоставки на това дедуктивно умозаключение се състоят в устойчивостта на мъжките, антиженски по своята същност, нагласи през времето и пространството.

В опита за обяснение на тези мъжки нагласи се натъкваме на страха от женската сексуалност, която се оказва толкова всепоглъщаща, че е склонна да опонира на мъжката сила. Така от мъжка страна се налага унижаването и потискането на жената враг с цел подчертаване на собственото величие като единствена възможност за постигането на „мирно съжителство". Ето как компенсирането на мъжката непълноценност, разбирана като субективно чувство за безсилие пред трансгресията на живота и смъртта, намира израз в омаловажаване на обекта носител на трансгресивната енергия и води до създаване на мъжкия тип фалосна култура. Купуването

на сексуалния обект е най-яркият израз на неговото принизяване, утвърждаващо собствената сила и власт като израз на компенсиращото превъзходство. От друга страна, "борсовата спекулация" или измамната продажба на една имитирана женственост, става реакция на това принизяване и задоволява компенсацията на женската непълноценност в културните модели [1].

В този смисъл проституцията се схваща като реакция на определен стимул, като борба за превъзходство на пола или като „пазарна икономика“, при която търсенето стимулира предлагането. Именно условно-рефлекторният характер на явлението определя неговото постоянно регенериране, т.е. проституцията би могла да съществува дотогава, докато продължава да бъде стимулирана. Поради комплицираността на стимулите тя се очертава като константна наличност в човешкото битие. Като излезем от значението на антонимите морално - аморално, се натъкваме на метонимията морално - обществено, противопоставена на аморално - проститутско. Проследявайки парадигмата на трите корелативни двойки, можем да предположим наличие на конфликт на социално-нравствена основа.

Неоспорим факт, съпътстващ историческото развитие на човечеството, е съществуването на едно явление, което в различните култури и епохи придобива различни стойности и значения, но остава относително постоянно и дори не променя името си през вековете. Интересно е почти универсалното наименование на това явление. В повечето езици номинализацията включва латинския корен на думата и продължава да битува с него. *„Prostitutio“,* така изписано и произнесено сякаш е еднозначно в целия свят, но не толкова с пряката си семантика (оскверняват, развалям, покварявам), а с придобилото впоследствие тъждествено значение на „развратна жена, която търгува с тялото си“.

ПРОУЧВАНЕ НА ИСТОРИКО-ПСИХОЛОГИЧЕСКИЯ АСПЕКТ НА ПРОСТИТУЦИЯТА И РОЛЯТА И ЗА НАЦИОНАЛНАТА СИГУРНОСТ

Анализирайки историческите аспекти на културите, се натъкваме на най-разнообразни предпоставки и форми на проституцията. В римската култура такава предпоставка бил всеобщият промискуитет – случайни, лишени от чувства връзки и оргийни церемонии в чест на бога Мутун Титин. По-късно се е разпространил обичаят купуване на съпруга, на която мъжът ставал властелин и господар. Именно по този начин в хода на човешката история се осъществява първоначалното разгръщане на еротизма, т.е. той бива означаван от наличието на обект на желанието [1].

В оргията такъв обект не се откроява, тя е завършеното отричане на индивидуалния аспект. В бурния и' поток не само бива потопена собствената индивидуалност на отделния човек, но и всеки участник отрича индивидуалността на останалите. Привидно това е пълно премахване на границите, но то е постижимо само ако не оцелее нищо от отликата между съществата. Поради това оргийният тип култури е присъщ, както на най-ниско развитите общества, където няма откроване на индивидуалността, така и на най-висшите слоеве, където тази индивидуалност задължава и ограничава, в следствие на което се стреми да бъде преодоляна.

Осъзнаването на индивидуалността в един далечен исторически период е свързано с разгръщането на символиката, което оказва своето влияние върху еротизма. Еротизмът се разглежда като сливане, което измества интереса по посока към преодоляване на личното битие и на всяка граница постигане на някакъв вътрешен интерес. Това действие може да се изрази като обекта на желание, притежаващ индивидуална отлика. В резултат се наблюдава обективна отлика, подчертаваща

стойността на един обект, сравним с други обекти. Така в сексуалния живот първоначално и най-често се обективизира това търсене от страна на мъжа към жената. Налага се схващането, че жените не са пожелани, те предлагат себе си на желанието. Предлагат се като обект на агресивното желание на мъжете. Да предлагаш себе си е основната женска нагласа, но първоначалният жест – предлагането, бива следван от престореното негово отказване [2].

Тази нагласа борави с типично женски средства - привличане на вниманието чрез украшения, флиртуване и разголване. В основата на обичая купуване на съпруга са залегнали всички тези аспекти, конкретизиращи жената като обект на желанието. Жените стават такива обекти в брака, като се превръщат в инструменти за домашен труд, а в същото време индивидуално, стойностни и сравними с другите обекти. Женският тип нагласа ги превръща в обекти на мъжкото желание. Видимо проституцията първоначално е била просто форма, допълваща брака.

В качеството си на преход трансгресията на брака въвежда в организираността на подчинения на правила живот, а от тук нататък става възможно разделението на труда между съпруга и съпругата. В резултат: подобна трансгресия не може да се посвещава на еротичен живот – вече започналите сексуални отношения просто рутинно продължават. Наличието на рутина в сексуалните отношения обуславя съществуването на привилегированата или т.нар. подбрана проституция. Това била една изискана и фина форма на предлагане и приемане особено популярна в индуизма и тантризма, където половото съжителство се сравнява с изтънчена борба, в която мъжът е активен, а жената му се противопоставя. В този си вид куртизанката, тъй като притежавала известна сдържаност, не била обречена на презрение и почти не се отличавала от другите жени. Свянът у нея трябвало да бъде притъпен, но тя следвала принципа на първия контакт, изискващ жената да изпитва страх от отдаването, а мъжът да очаква от нея да реагира с отбягване. Така престореното „трудно спечелване“ на куртизанката носело удовлетворение на ловджийския инстинкт у мъжа [1].

Друг аспект, изтъкващ психологическата услуга, извършвана от този вид проституция спрямо мъжкия пол, е т.нар. „престъпване на забраната“. Тъй като обикновено за мъжа е пагубно да изпитва върху себе си престъпването на закона, се налага макар и престореното смущение от страна на куртизанката. Точно чрез срама, престореният или не, жената приема върху себе си престъпването на забраната, което е основата на нейната човешка и романтична трагичност. Именно като израз на всеотдайност, изкупление и мистично съединяване с богинята се обуславя култовата проституция, наричана още „сакрална“ или „храмова“. Потвърждение за религиозния аспект на проституцията се получава от свидетелствата на Херодот. Разцветът на храмовата проституция е през третото хилядолетие пр.н.е. Формите и са различни: хетеросексуална, бисексуална, хомосексуална, орална и содомия. Най-стари са традициите в шумерската култура, по-точно в град Урук, в който се намирал храм на бог Ану. Проститутките служели на богинята Ищар и живеели в специална къща до храма, наричана „гарум“. Освен професионалните проститутки по подобен начин служели на богинята Ищар препоръчвали всяка жена поне веднъж в годината да се отдава в храма на чужд мъж. За тези действия свидетелстват паметниците на Помпей, където светилищата били люлка на римската проституция. Тя била подчинена на култа към богинята Изида и бога Приап. Освен мистичното съединяване на „всеотдайните“ жени с бога, в този култ били въвличани и девствениците с оглед доброто на техните бъдещи семейства. Има сведения за дефлорация

с фигурката на бог Приап. Индийските храмове все още изобилстват с еротични изображения, в които еротизмът се представя като нещо основополагащо, като божествено. Многобройни индийски храмове тържествено ни напомнят неприличието, дълбоко заровено в нашите сърца.

Раждането на проституцията в смисъла на „оскверняване“ очевидно е свързано с раждането на мизерстващите класи, избавени – поради окаяното си състояние – от грижата си за скрупульозното съблюдаване на забраните. В този смисъл мизерията, заличава всеки срам и морал и довежда до същинското „оскверняване“, което освобождава хората от забраните, които са основа на тяхната човешка същност. С появата на имущественото неравенство се налага робският и наемният труд, което представлява достатъчно основание за възникване на професионална проституция – като принудителни работни задължения жените отдавали себе си срещу заплащане. Социалното основание на проституция, е същото като за морала - неравенство между класите и мизерията. Това предизвиква първата революция в Египет и довежда около VI век пр.н.е. в цивилизованите райони до затруднения, с които е възможно да свържем освен другите движения в това число и юдейското пророчество.

Анализът на фактите дава основание да приемем разделянето на проституцията на светска, долна и улична, чието възникване в гръко-римския свят е в интервала по време през VI век пр.н.е., което съвпадение е парадоксално. Изпадналата класа съвсем не се стреми към издигане на смирените и смъкване на властващите. Именно като първоизточник на падението на проститутките се сочи тяхното примирение с мизерията. Съгласно каноните на християнството е изработило идеалния свят, от който е изключило ужасяващите и нечисти аспекти, то проституцията се явява допълнителна спрямо създадената от него ситуация. Тя сътворява, в допълнение на идеалния свят, профанния свят, където дори скверното в упадъка става безразлично. Учудващо е, че едно такова явление, влязло в пълно противоречие с християнството, през 1033 г. бива благословено от папа Бенедикт IX, който създава първата регламентация на проституцията, като открива първите публични домове в Рим. Градските власти определят специални квартали, в които разполагат публичните домове, облагат ги с данъци и издават устави, регулиращи порядките в домовете.

През XII и XIII век проститутките представляват особен кръг на обществото и притежават силна романтична окраска, поради което в епохата на ранния Ренесанс вдъхновяват много произведения на изкуството и културата. По времето на Реформацията обаче – XVI-XVII век, започва тяхното преследване, тъй като това явление е противоречало на лозунгите на реформистката идеология. Въпреки всички забранителни мерки проституцията се увеличава, тъй като е растяла бедността, нищетата, безправието.

През XVI-XVIII век вече почти всички цивилизовани страни имат регламентирана проституция. Интересно е, че независимо кога и в коя страна са били откривани публичните домове, регламентацията е била една и съща. Дори в Япония регламентацията по нищо не се е отличавала от тази в Англия и Франция. Общият регламент е бил следният: градските власти и полицията определят местата за публичните домове, издават специални разрешения на собствениците, срещу което те се задължават да плащат данъци и такси на общините. Проститутките са били завеждани на отчет в полицията и са получавали специално удостоверение вместо личен паспорт, също така са били длъжни няколко пъти в седмицата да минават на медицински преглед.

От края на XVIII век публичните домове биват управлявани от синдикат, наречен „Сдружение на собствениците на мебелирани квартири във Франция и прилежните й колонии“. Тази организация е разполагала с много средства, имала е вестник, медицински персонал и политически покровители. По настояване на някои прогресивни организации публичните домове във Франция биват закрити и от този момент нататък синдикатът се бори за ново откриване. Голям растеж има проституцията в Азия и Япония, където е имало цели квартали с проститутки. В колониалните страни това явление също получава широко разпространение – в Тайланд например легалната проституция е имала долна възрастова граница 15 години, в Ирак – 13 години. Според „Revue abolitioniste“ в Холандия съществувал цял лагер на веселието, където били събрани 1800 проститутки, сред които най-младите били на 13-14 години.

Любопитното е, че регламентацията на проституцията в България била приета без ни най- малка степен на „побългаряване“, т.е. точно в същия вид, в който съществувала и в другите страни. Тук се откроява един парадоксален факт, а именно появилата се проституция в България малко след Освобождението. Възможно ли е скептичният и консервативен, изстрадал българин да мисли и да приема толкова противоречащо на неговия патриархален морал явление. Получава се така, че България преди още да е определила по кой от световните модели да състави своята конституция, същият този патриархален българин вече е прозрял, че в света има само един модел на проституция и той би могъл да бъде приет. Подобен факт би могъл да бъде обяснен най-вече, ако изхождаме от българското любопитство като предпоставка за тази любознателност, която във всички случаи означава отворени пътища за българската душа към предприемчивост и възприемчивост на онова, което вече е сътворено по света.

Друго обяснение на този факт би могло да бъде видимо устойчивият характер на проституцията поради индивидуално-психологическите и' основания, както и поради обществената и' необходимост. Всяко общество има нужда от такава пробойна в своята морална система, която да се противопоставя на този морал, за да осигурява бягството на индивида от него. От друга страна, тази антиморална структура е необходима на обществото с нравствено-охранителната си функция, т.е. на принципа на отричането и психологическото си отхвърляне проституцията подчертава стойността на морала и предпоставя към неговото съхраняване.

Освен това периодът на османското владичество представлява силен стресогенен фактор за целия български народ и в частност за българката. Пред страха, че тя ще е поредната жертва на ширещата се бруталност и сексуално насилие, българката блокира своята сексуалност. Тя възприема мъжкия модел на полова идентичност и започва да мисли себе си в категориите на мъжко преживяване дори когато става въпрос за много интимни аспекти от живота на тялото. Тук може да предположим още, че радушното приемане на проституцията от страна на българския мъж е продиктувано от продължителното задържане на сексуалната енергия. За отбелязване е, че първите проститутки в България са били предимно чужденки: сръбкини, австрийки, чехкини и др., което, освен че дава обяснение за сексуалното функциониране на българката по онова време, също така свързва България с международния трафик на жени [1].

В протоколните книги на Видинския градски общински съвет за времето от Освобождението през 1878 г. до 1909 г. може да се види, че това социално явление е

свързано с опазване на моралното и физическото здраве на населението, което много често е разглеждано в дневния ред. Тъй като "публичните жени" работели предимно в центъра на града, необезпокоявани от закона, нито контролирани, г-н Видинският губернатор на заседание от 15.02.1880 г. с протокол №23 поставя въпроса за преместването на публичните жени вън от центъра на града. За целта е предложено общината да поправи на свои разноски бившите военни караули край града, като след това ги отдаде под наем на онези, които биха пожелали да държат публичен дом. В резултат на 15.03.1880 с журнално постановление №43 и след повторно обсъждане на предложението съветът решава „поменатите проститутки да си изостанат все на тези места, където се намират и понастоящем“. В архивите могат да се видят последователни протоколи в които се отчита, че е позорно за една община да черпи доходи от едни нещастници, които са принудени да продават тялото си. Ако има жени, които продават тялото си, то срамно е за един общински съвет да поддържа тази позорна търговия и да се ползува с доходи от нея. В много държави е премахната регламентацията, защото с нея се разпространяват повече венерическите болести.

Действително най-големият социален отзвук, който някога проституцията е получавала, е в началото на XX век. Във връзка с разпространилата се фобия от сифилис в цял свят започва да се тръби против регламентацията и да се обмислят всевъзможни мерки за прекратяване на проституцията. Тъй като досега регламентацията била мотивирана като загриженост за населението и ограничаване разпространението на венерическите болести, изведнъж се оказало, че заболеваемостта расте въпреки постановените мерки. По този повод във Видинския периодически печат се появява поредица от публикации под заглавие „Против регламентацията“. Публикуват се предимно съобщения, преведени от световната преса, като изявлението на проф. А. Форел и на д-р Луи де Пильор, в което се казва: "За всички, които искат да си дадат отчет за нещата и които не са с предубеждения, той (медицинският преглед) е съвършено неефикасен и това поради самото естество на венерическите болести“ [2].

ЗАКЛЮЧЕНИЕ

Конфликтът, разгледан в този аспект, следва да се възприеме като трайно отрицателно отношение на проституиращите към обекти и страни от социалната действителност. Тъй като отношението към нормата предполага винаги наличие на социално-психологически елемент, можем да възприемем проституцията като продукт на „социалната ситуация на развитието“, която представлява особено съчетание на вътрешните процеси на развитие на личността и външните условия на нейното формиране, което е типично за динамиката на всеки възрастов етап и обуславя както динамиката на психичното развитие за времето на съответния възрастов период, така и качествено своеобразните психологически новообразувания, възникващи към неговия край.

Литература

1. Адлер, А. Практика и теория на индивидуалната психология. София, 1995.

2. Arsova, T. Prostitution and Sex Workers in Bulgaria: Analysis of the Situation and the Risk with Regards to HIV/AIDS/STDs. Sofia: Health and Social Development Foundation. 2000.

ИЗСЛЕДВАНЕ НА ИСТОРИКО-ПСИХОЛОГИЧЕСКИЯ АСПЕКТ НА ПРОСТИТУЦИЯТА И РОЛЯТА Й ЗА НАЦИОНАЛНАТА СИГУРНОСТ

Венелин Терзиев
Национален военен университет „Васил Левски“, Велико Търново
Русенски университет „Ангел Кънчев“, Русе
Висше училище по телекомуникации и пощи, София
Никола Ничев
Национален военен университет „Васил Левски“, Велико Търново
Христо Бонев
Национален военен университет „Васил Левски“, Велико Търново

STUDY OF THE HISTORIC-PSYCHOLOGICAL ASPECTS OF PROSTITUTION AND ITS ROLE FOR THE NATIONAL SECURITY

Venelin Terziev,
Professor, Ph.D., D.Sc. (National Security), D.Sc. (Ec.),
University of Rousse, Rousse, Bulgaria,
National Military University, Veliko Tarnovo, Bulgaria
University of Telecommunications and Post, Sofia, Bulgaria
Nikolay Nichev
Colonel, Associate Professor, Ph.D.,
National Military University, Veliko Tarnovo, Bulgaria
Hristo Bonev
Ph.D. student,
National Military University, Veliko Tarnovo, Bulgaria

Abstract: *The study attempts to present a summary analysis and a historical-psychological review of the prostitution as a problem. The prudential nature of the analyzed and investigated scientific and other sources gives grounds to consider different hypotheses about the impact of these processes and phenomena on the national security system.*

Keywords: *national security, prostitution, governance.*

ВЪВЕДЕНИЕ

Много са измеренията на проблема проституция - или предлагането на секс срещу пари. Този проблем генерира не само етична алтернатива, но и въпроси, свързани с безопасността на проституиращите (без оглед на тяхната възраст и пола им), с нарушаването на човешките им права, с връзката им с организираната престъпност. Лицата, предлагащи платен секс, често са определяни като рискова група по отношение на употребата на наркотици, посегателствата срещу личността и разпространението на социално значими заболявания, каквито са венерическите. Проституцията често се определя като модерна форма на робство и се свързва с трафика на хора, което е едно от най-тежките престъпления в световен мащаб [1].

Акцентът на борбата в България срещу тази сексуална експлоатация обикновено се поставя върху международния трафик на хора. Най-често усилията на правоохранителните органи се насочват към разкриване и противодействие на трафикан-

тите, действащи на територията на чужди държави. Не се проследяват обаче криминалните мрежи, с които те са свързани в България. Направените анализи показват, че в повечето случаи проституцията у нас прелива в международен трафик на „бели робини". И това е естествено, тъй като – водена от възможностите за значително по-високи доходи в чужбина – организираната престъпност се е ориентирала към износа на проституция. Паралелно с това престъпните групи развиват и поддържат богата вътрешна мрежа от проститутки и сводници.

Не е на необходимото равнище и реакцията на правоохранителните органи. Слабата организация на противодействието в комбинация с неадекватното законодателство позволяват години наред на проституцията да процъфтява и – най-важното – да се контролира от организираната престъпност, която натрупва от нея значителни незаконни доходи. Нещо повече – те улесняват преминаването на вътрешната проституция към много по-доходоносните пазари в страни от Западна Европа, САЩ, даже ЮАР. В резултат на това рязко нараства международният трафик на българки. Според едно изследване на Европол. България е един от шестте основни източника на жертви на трафика на хора. Информацията от изследванията, показва значително припокриване на престъпните структури, контролиращи проституцията в България и износа на такъв вид престъпна дейност зад териториалните граници. За това успешното противодействие на трафика на хора изисква адекватни мерки срещу вътрешната проституция и контролиращите я престъпни структури, които са развили стабилна мрежа в цялата страна [2].

В опита за обяснение на тези мъжки нагласи се натъкваме на страха от женската сексуалност, която се оказва толкова всепоглъщаща, че е склонна да опонира на мъжката сила. Така от мъжка страна се налага унижаването и потискането на жената враг с цел подчертаване на собственото величие като единствена възможност за постигането на „мирно съжителство". Ето как компенсирането на мъжката непълноценност, разбирана като субективно чувство за безсилие пред трансгресията на живота и смъртта, намира израз в омаловажаване на обекта носител на трансгресивната енергия и води до създаване на мъжкия тип фалосна култура. Купуването на сексуалния обект е най-яркият израз на неговото принизяване, утвърждаващо собствената сила и власт като израз на компенсиращото превъзходство. От друга страна, "борсовата спекулация" или измамната продажба на една имитирана женственост, става реакция на това принизяване и задоволява компенсацията на женската непълноценност в културните модели [1].

Неоспорим факт, съпътстващ историческото развитие на човечеството, е съществуването на едно явление, което в различните култури и епохи придобива различни стойности и значения, но остава относително постоянно и дори не променя името си през вековете. Интересно е почти универсалното наименование на това явление. В повечето езици номинализацията включва латинския корен на думата и продължава да битува с него. *„Prostitutio",* така изписано и произнесено сякаш е еднозначно в целия свят, но не толкова с пряката си семантика (оскверняват, развалям, покварявам), а с придобилото впоследствие тъждествено значение на „развратна жена, която търгува с тялото си".

ИСТОРИКО-ПСИХОЛОГИЧЕСКИЯ АСПЕКТ НА ПРОСТИТУЦИЯТА И РОЛЯТА Й ЗА НАЦИОНАЛНАТА СИГУРНОСТ

С редица международни актове и спогодби на 02.12.1949 г. ООН одобрява „Международна конвенция за забрана трафика на жени и експлоатацията на проститутки“, ратифицираната от почти всички страни. С посочените мерки световната общност се надява, че ще победи „естествения спътник“ и враг на своето добродетелно съществуване, но чия е победата, е излишен въпрос, с чийто отговор се сблъскваме в нашето актуално пространство и ежедневие. Историческото съжителство с проституцията предизвиква и първите опити за нейното научно обосноваване. Още през XIX век се отбелязва, че една четвърт от проститутките са сираци или изоставени от много малки, което е основание на тяхната мизерия и ниска култура, благоприятстващо тяхната безкрупулност, което се оказва фундаментална крачка към оскверняването (prostitution). Тук не може да не отбележим, че сега, приблизително век и половина по-късно, проблемът за безнадзорните и депривирани деца и техните противообществени прояви не само съществува, но и се разраства все повече.

През 1890 г. се появява изследването на П. Тарновски към FAY (FAY- Международна асоциация на аболюционистите) за психо-физиологичната природа на проститутките, което налага следната дефиниция: „Проститутката е особен антропологичен вид жена, която се различава рязко, в някои случаи анатомично и винаги психологично, от нормалния човек, от нормалните жени. Тя е особено същество с ненормални физични и психични качества“. Тук се забелязва първоначалната идея за атавизма на престъпника и проститутката, разработена в учението на Ч. Ламброзо. Атавизмът представлява пробуждане на първобитни инстинкти у индивида. Физиологическият атавизъм се изявява чрез физични аномалии, в строежа на черепа, а нравствено-умствения атавизъм – с деградирала душевна конструкция. Така се стига до тезата за генетичната предопределеност на социалното поведение. Ламброзо диференцира вродени и случайни проститутки. У вродените определящ е физиологичният атавизъм (аномалии на черепа, тялото и особено на половите органи), а у случайните определящи са външни явления, които благоприятстват разгръщането на психичния атавизъм (проява на психопатични черти). След анализ на структурата на престъпните родове се стига до извода за „порочната наследственост“.

За разликата от съотношението вродени/случайни атависти при престъпниците, тук процентът на вродените проститутки е много по-малък в сравнение с този на случайните. Като основни психологично-дегенеративни черти у проститутките се откриват: пълна липса на майчини чувства, склонност към скитничество, раздразнение, озлобление, склонност към алкохолизъм, алчност, фантазиране, лъжливост, прекомерна страст към разни труфила и бижута. Както се убеждаване при анализа, чертите на проститутките изобщо не са се променили, само научното знание за тяхното обяснение е напреднало. Обяснението е, че тези черти водят атависта към предаване на порока, тъй като неговата нервна система е притъпена и наред с телесната анестезия той е и морално нечувствителен. Мозъчните му центрове бързо се изтощават, интелектът му е слаб, затова не е способен за системна работа. Така у проститутката се развиват паралелни стремежи – чрез предлагане на собственото тяло да се печелят лесни пари. Според други изследвания дефиниращи максимумата „жената престъпничка и проститутка“ намира и добро социално основание на

стремежа към паразитизъм, като се изтъква, че дегенератите паразити от богатите класи по законен начин могат да експлоатират малоимотните и така да се превръщат в обикновени насилници, без да е необходимо да стават престъпници или проститутки, с което се обяснява и незначителният процент, който имотните групи представляват в тези категории. В този дух на разсъждения като препоръка за справяне със социалните недъзи от страна на привържениците на тезата за проституцията като вродена диспозиция се изтъкват толкова антихуманни средства, като социалната и расовата хигиена, които по-късно намират израз в нацистката идеология.

В отговор на анализираната теза можем да обобщим, че когато неуки лаици, в желанието си да останат верни на обществените си задължения и тяхната професия, като една огромна чувственост, като същества които са постоянно възбудени. Въпреки това такива възгледи често се срещат в научните изследвания, най-често свързани с твърдението за вродения характер на проституцията. Затова основателите на индивидуално-психологическия подход си поставят за цел да докажат, че тя е продукт на социално-психологически влияния още от ранно детство. Ключовото понятие, описващо психологическия характер на проституцията, е „мъжкият протест“. Това е понятие, характеризиращо индивидуалните прояви на женската психика. В основата му е залегнало чувството за непълноценност на женския пол, породено от констатиране на междуполовите различия още в началните стадии от развитието на индивида. В зависимост от средата и възпитателните въздействия това чувство може да се преодолее леко и без да оставя следи и да прерасне в комплекс. Решаващо значение за този процес имат семейните отношения: когато фигурата на бащата е надарена с господство и силен авторитет, а този на майката е ужасяващ пример за раболепно поведение, ако братът е издигнат до ранг достоен за уважение и завиждане, то собствената женственост дава само повод за упреци и търсене на недостатъци. В случаите на липса на родителски авторитет той бива заместен от „уличен авторитет“. Това предизвиква протест срещу утвърждаваната мъжка сила и бягство от социалната женска роля.

В случая, когато се струпват много допълнителни социално-икономически фактори като нищетата, ниската култура и т.н., една жена, която търси оттегляне от женската роля, го намира в прекрачване на нормите и утвърждаване на порока, вместо в характерната женска добродетел – майчинството. Протестът срещу мъжката сила и превъзходството намира своя израз в търговския елемент – задължителен при проституцията. Самият факт, че жената се занимава с такава приоритетно мъжка дейност, каквато е търговията, вече сваля неговото превъзходство. А изпадането му в дълбока заблуда относно купуването на "нейната любов" го прави глупак и слага край на мита за мъжката сила, тъй като се купува нещо, което отдавна не е нейно, т.е. тя го продава без да го притежава, понеже е останала далеч от ролята на жена – тя е продавач и остава фригидна.

При такова бягство от женствеността е нормално сексуалността на проститутката да се изявява в хомосексуални нагласи, продукт на които са дрезгавият глас, вулгарният език и грубите маниери, а в секса се проявяват като перверзия. Това снижаване на мъжкото превъзходство и всъщност компенсаторна линия на „мъжки протест“. Компенсацията на женската непълноценност се осъществява чрез „мъжка направляваща линия“ в поведението, която се задължава от мотива: „искам да бъда превъзхождащ мъж, а не пасивна жена“. Оттук нататък е в сила тенденцията за омаловажаване на мъжа чрез доминация в сексуално отношение (или отказ от

полов живот, или хипоактивно полово желание, което да утвърждава нейните умения и неговата невъзможност) чрез използване на типично женски средства в общуването- кокетиране, флиртуване, ревност, пренебрежение и т.н.

Принципите на възпитанието, които се утвърждават в хода на формиране на индивидуално-психическия подход до голяма степен оборват твърдението, че родителският алкохолизъм, престъпност и проституция са наследствени. В други анализи се смята, че те не са вродени, а провокирани и след това придобити. Въз основа на отрицателните социални и възпитателни въздействия се придобива чувство за малоценност, което поражда агресия, и като компенсация се провокират алкохолизмът, престъпността, проституцията и др. По такъв начин индивидуално-психологическият подход ни дава възможност да видим в проституцията търсене на субективно чувство за превъзходство или естествена реакция на организма – да насочи агресията към фрустратора. Впоследствие изследванията се насочват към проблема свързан с растящия процент на проститутките сред домашните прислужници и на момичетата от разведени семейства или пък такива, в които липсва родителски авторитет. Тази констатация обръща внимание върху механизмите на полова идентификация, върху кастрационния и Едиповия комплекс. Според психоаналитичните разработки по въпроса за кастрационния комплекс в известна степен се установява, че Едиповият комплекс на момичето е възможен и е въведен от кастрационния подход [1].

Преживяването на Едиповата драма има голямо значение за по-нататъшното засилване на завистта към пениса. Стига се до ситуация, при която жената съзнателно се отдава на другите мъже, за да отмъсти на баща си, че не я е предпочел, а когато иска пари от мъжете, утвърждава своята сила и власт, т.е. извършва символична кастрация. Логично е да предположим, че случаите на констатиран от Елис липса на родителски авторитет се свързват с невъзможността за фиксиране върху бащата и със задълбочаването на чувството за малоценност. Още повече липсата на възпитателни въздействия от страна на родителите ограничава възможността за развитие на суперегото „суперегото на детето в действителност не е изградено върху модела на родителя, а върху този на родителското суперего".

Именно неговото функциониране става отговорно за разбирането на социалните норми, което обяснява склонността към отклоняващо се поведение у социално неравностойни деца. Така ефективната структура на проститутката изглежда много особена и доминирана минало разочарование.

В други теоретични разработки се изхожда от разликите в мъжката и женската сексуалност, определящи женския характер с понятието „контректационно влечение" – потребност от съприкосновение, без значение върху коя част от тялото е съсредоточено и независимо от обекта на желанието, което означава, че жената е преди всичко и най-вече сексуална. Като върховна изява на нейното съществуване е половият акт и размножаването, поради което се диференцират два основни типа: майката и проститутката. Строго казано и двете не предявяват никакви изисквания към личността на своето полово допълнение. Едната взема, който и да е мъж, стига той да й даде дете и когато това дете е налице, друг мъж е излишен. Другата се отдава на всеки мъж, който може да й даде еротично наслаждение той за нея е самоцел. В тези разсъждения бихме могли да забележим първообраза на идеята за необходимостта от запълване на продуктивното женско вътрешно пространство.

В изследванията се абсолютизира същността на описаните характери и се смята, че те отразяват основата на жената въобще, поради което могат да се срещнат у всяка представителка на пола в различна степен. Абсолютния майчин характер се разглежда като илюзия за любов и нравственост, тъй като в основата си жената е аморална, безнравствена и неспособна да разбира и преживява истинските чувства, по причина на своята свръхсексуалност. Затова жената проститутка поне изглежда реална и заслужава, ако не възхищение, то поне уважение. Това ни дава основание да игнорираме мерилото за ценност на мъжа, който отхвърля идеала за девственост. Всичко това дефинира най-различни форми, като в открита форма на светска дама, в по-слаба форма на метреса и най-последна с степен на градация е уличната проституция. С това се обяснява изключителното положение на проститутките в обществото, което е поставя вън от правата, законите и всички сфери на социално уважение [1].

Не можем да отминем извода, че проституцията е вътрешно присъща на целия женски пол. Следователно този тип жени живеят безсъзнателно, те са лишени от всякакво аз и индивидуалност, т.е. налице е безименна, безпринципна, алогична, аморална, лишена от гениалност и способна на истинска обич. Факт е, че много такива възгледи се открояват в анализите и се възприемат като престъпване на всякакви граници и пълно вмешателство в психичния живот на женската аудитория, което слага край на женската търпимост, предизвиква реакцията на феминизма. Първоначално феминизмът се обявява за премахване на стигмите по въпроса за междуполовата психологическа обособеност и за постигането на равноправие. Във втория етап се препоръчва подчертаване на половите различия с цел побеждаването на фалическия култ. Именно чрез подчертаването на половите различия се стига до разглеждане на женския полов орган като „множествен“. Вследствие на тази множественост жената е автоеротична, жената „се пипа“ непрекъснато, без някой да може да й го забрани, тъй като половият й орган е направен от две устни, които непрекъснато се целуват и не изпитва желание за заместване на този вид еротизъм с хетероеротизъм [3]. Поради този факт на култура и възпитание, се научава да придава значение единствено на отдавна определяемата форма на фалосът – митът за кастрацията. По този начин женското сексуално насаждение се описва като мазохистична проституция с тялото за удовлетворяване на желание, което не е женско. Тук отново проституцията се свежда до типичната женска нагласа, насочена саморазрушително, която дори определя типологията на женските характери. Механизмите на проституцията се обясняват с множествеността на женското желание, т.е. множествеността на женския полов орган, обуславя множественост на женското желание и след като е отхвърлен автоеротизмът, тази множественост се проявява като женското „всичко“ или „още“, което намира израз в желанието да се притежават всички мъже.

ЗАКЛЮЧЕНИЕ

Интересна са двете хипотези, свързани с възникване на проституцията и женската сексуалност, или от анализа на женската сексуалност се стига до проблема за проституцията. Очевидно двата аргумента са „по женски“ взаимосвързани и неделими. По-впечатляващото обаче е, че ако феминизмът и маскулинизмът имат спорове относно превъзходството на един от двата пола, то по въпроса за проституцията мнението е почти единно базиращо се на наличието на проституцията само в

общество, поставило си за цел задоволяване нуждите на мъжа. Митът за свръхмъжа или фалическия култ са отключващ фактор спрямо женската сексуалност, множествеността на женското желание, съвпада с контрекционното влечение, което е основа на женската сексуалност към проституиране. Проституцията може да се приеме извън прекия си смисъл, като черта на женския характер или на женска нагласа съчетана със склонност към предлагане на себе си като обект на харесване, посредством което се удовлетворява желанието за себеутвърждаване, изява и власт.

Литература

1. Адлер, А. Практика и теория на индивидуалната психология. София, 1995.

2. Arsova, T. Prostitution and Sex Workers in Bulgaria: Analysis of the Situation and the Risk with Regards to HIV/AIDS/STDs. Sofia: Health and Social Development Foundation. 2000.

3. Бартол, К. Психология криминального поведение. 7-е изд. Прайм Евро-Знак, 2004.

ИНФОРМАЦИОННА СИГУРНОСТ

КОМПЮТЪРНА СИМУЛАЦИЯ НА TCP SYN АТАКИ

Ивайло Д. Николов, Пенчо К. Пенчев

5300, гр. Габрово, ул. Х. Димитър 4, Технически университет - Габрово

COMPUTER SIMULATION OF TCP SYN ATTACKS

Ivaylo D. Nikolov, Pencho K. Penchev

5300, Gabrovo, 4 H. Dimitar, Technical university of Gabrovo

Abstract: *Information security includes protection of information resources belonging to any type of network without concerning its purpose, topology or way of implementation. Following this point of view, the theoretical study, analysis and research of information security therefore should be considered out from the general to the particular and specific application to any information resource.*

Keywords: *information security, education, high education,*

Информационната сигурност е важен елемент при опазване на информационните ресурси в организацииите. Информационната сигурност обхваща опазване на информационните ресурси във всеки вид мрежа без значение какво е нейното предназначение, топология или начин на реализация. Изхождайки от тази позиция, теоретичното изучаване, анализиране и изследване на информационната сигурност следва да бъде комплексно от общото към частното и конкретно приложение спрямо всеки един информационен ресурс.

Настоящият доклад има за **цел** създаване на симулационен модел за изследване на атаки от типа „отказ на обслужване“.

За реализиране на поставената цел са решени следните **задачи**:

- избор на симулационна среда за реализиране на атаките;
- създаване на симулационен модел (експериментална постановка);
- симулиране на атаки от типа „отказ на обслужване“;

1. Избор на симулационна среда

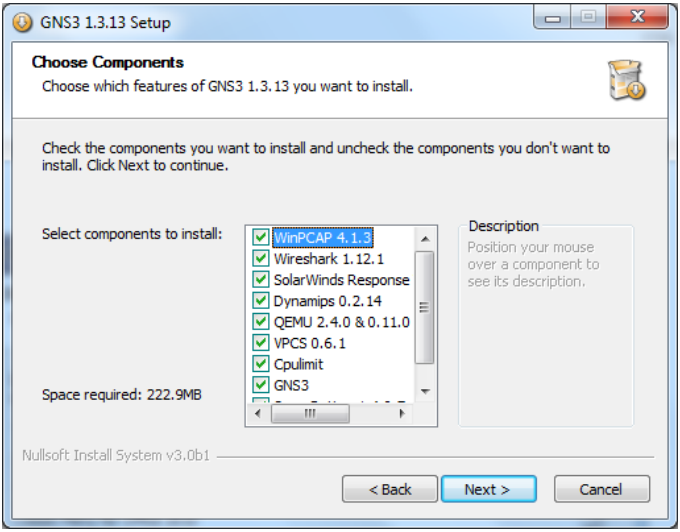
Съществуват редица емулатори на програмно-апаратни средства с възможност за симулиране на мрежов трафик за целите на изучаването на компютърни атаки от тип „отказ на обслужване” за целите на информационната сигурност. Най-широко разпространените са Cisco VIRL, Cisco Packet Tracer, GNS3, UNetLab и други. Причините за избор на GNS3 за среда за симулиране на изследванията са следните:

- GNS3 позволява емулиране на различни мрежови устройства, включително маршрутизатори на Cisco, Mikrotik, Jupiter, CheckPoint и други като предлага пълен достъп до всички функционалности на устройствата, докато при Cisco Packet Tracer например голяма част от функциите са недостъпни;
- Възможността за емулиране на устройства на различни производители позволява изграждане и симулиране на хетерогенни мрежи в графичен режим със изключително голямо приближение спрямо функционирането им в реални условия;
- GNS3 позволява включване в симулациите на напълно функциониращи виртуални машини с различни операционни системи, чиито функции са напълно достъпни по време на симулацията. Причината за това е пълната съвместимост с VirtualBox, Virtual PC и софтуерните продукти на VMware. Безпроблемно симулационната постановка може да бъде конфигурирана за работа паралелно с реални устройства, осигуряване на достъп до Интернет, изграждане на VPN и т.н.
- GNS3 е софтуерен продукт с отворен код за разлика от Boson NetSim, Cisco VIRL и други, като това му предимство наред с предлаганите функционалности го прави предпочитан при симулиране на различни топологични мрежи и изследване на трафика;

Въз основа на описаните предимства за изследване на информационната сигурност от гледна точка на компютърните атаки от типа „отказ на обслужване“ е избрана симулационна среда на базата на GNS3 (Graphical Network Simulator 3).

1.1. Описание на мрежовия симулатора GNS3

GNS3 (Graphical Network Simulator 3) е графичен симулатор на компютърни мрежи с отворен код, който позволява емулация и обучение на различни по сложност мрежи. GNS3 поддържа работа със виртуални машини като VMWare, VirtualBox и Virtual PC, което позволява използване на различни операционни системи във виртуална заобикаляща среда. GNS3 поддържа емулация на Cisco IOS във виртуална среда посредством Dynagen. GNS3 поддържа освен маршрутизатори на Cisco, но и Juniper, Mikrotik, CheckPoint и други. GNS3 е в състояние да осигури около 1000 пакети в секунда във виртуална среда, докато един нормален рутер осигурява сто до хиляда пъти по-голяма пропускателна способност. GNS3 не би могла да заеме мястото на истински рутер, въпреки възможността за използване в реална мрежа, но се явява безценен инструмент за обучение и тестване в лабораторни условия. GNS3 е разработен предимно от Jeremy Grossmann, като при неговото развитие и усъвършенстване са работили още David Ruiz, Romain Lamaison, Aurélien Levesque, и Xavier Alt. GNS3 използва следните софтуер:



Фиг. 1. Включени мрежови инструменти
в пакета на Graphical Network Simulator 3

WinPcap (Windows Packet Caption) е инструмент с отворен код за улавяне и предаване на мрежови пакети в MS Windows базирани операционни системи. Поддържа се за операционни системи Windows XP, Vista, 2008, Win7 и 2008R2 . Версията за MS Windows 10, която поддържа NDIS драйвер версия 6.x е Win10PCap. WinPcap има допълнителни полезни функции, включително пакети за филтриране, мрежова статистика и дистанционно улавяне на пакети.

WinPcap се състои от драйвер, който се инсталира на операционната система, за да се осигури достъп на ниско ниво на мрежата, и библиотека, която се използва за лесен достъп до трафика на ниско ниво от мрежата. Тази библиотека съдържа libpcap Unix API Windows.

WinPcap поддържа протоколни анализатори, мрежови монитори, системи за откриване на проникване в мрежата, подслушване, генератори на трафик и мрежови тестери, класифицирани по следния начин:

- улявяне на пакети, както на тези, предназначени за машината, където той се движи и тези, които се обменят с други източници;
- филтриране на пакетите според потребителски дефинирани правила, преди да ги разпрати на заявлението;
- предаване на потребителски пакети към мрежата;
- събиране на статистическа информация за мрежовия трафик.

WinPcap получава и изпраща пакетите независимо от използваните протоколи. Това означава, че тя не е в състояние да блокира, филтрира или манипулира трафика, генериран от други програми на същата машина: WinPCap прочита уловените пакети, които преминават през мрежовия адаптер. Поради това WinPCap не

предоставя необходимата поддръжка за приложения за ограничаване на трафика, QoS и защитни стени.

Някои от широко популярните мрежови инструменти, които са разработени на базата на WinPCap са Wireshark , Tcpdump, Nmap, Snort, NTop и др.

Wireshark (www.wireshark.org) е пакетен мрежов анализатор, който предоставя подробна информация за трафика на мрежовите пакети. Wireshark е с отворен код и е предназначен за отстраняване на проблеми в компютърни мрежи, изследване на инциденти по сигурността на мрежата, както и в процеса на обучение и изучаване на мрежите. Wireshark се поддържа за Windows и UNIX операционни системи. Той е разработен на базата на WinPCap и притежава функции за графично изобразяване на пакетите, филтриране и търсене на пакети.

Dynamips е емулатор, който поддържа Cisco маршрутизатори. Той е създаден от Christophe Fillot в началото на 2005 г. Dynamips работи върху FreeBSD , Linux , Mac OS X или Windows и посредством него може да се емулира хардуера на серия маршрутизатори на Cisco чрез директно зареждане на Cisco IOS софтуера изображение в емулатора , Dynamips емулира Cisco платформи 1700, 2600, 2691, 3600, 3725, 3745, и 7200.

От октомври 2007 г. развитието на Dynamips продължава благодарение на усилията на проекта GNS. Към момента актуалната версия на Dynamips е 0.2.14-Dev за Windows, Linux и OS X, и версия 0.2.8-RC2 на Solaris. Изходният код се разпространява под GNU GPL .

2. Експериментална постановка

За целите на настоящата разработка е използвана насложена IP базирана мрежа, изградена на базата на VMWare ESXi сървър [https://www.vmware.com/support], инсталиран върху физическа машина [3] със следните параметри:

Manufacturer: FUJITSU

Model: PRIMERGY TX 120 S3p

CPU Cores: 4 CPU x 3.092 GHz

Processor Type: Intel (R) Xeon (R) CPU E3-1220 V2 @ 3.10 GHz

Основна част от изследванията са проведени в сегмент 1 от фиг. 2. – Схема на опитната постановка. Използването на виртуален сървър за реализиране на изследването в процеса на обучение предоставя редица възможности като динамична промяна параметрите на виртуалните машини, спиране и пускане на различни виртуални машини в зависимост от конкретните задачи, които следва да бъдат решени и др.

За достъп до VMWare ESXi е използван VMware vSphere Client (фиг. 1). Необходимо е задаване на IP адрес на сървъра, потребител и парола за достъп. Същите се указват от администратора на системата при инсталиране на VMWare ESXi.

За достъп до виртуалната машина се използва VMware vSphere Client чрез оторизация.

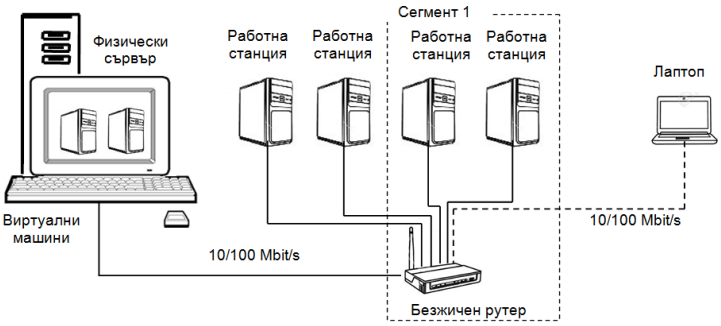
VMWare ESXi сървър поддържа създаването множество от виртуални машини, в зависимост от параметрите на използвания физически сървър и параметрите на виртуалните машини, които е необходимо да бъдат създадени. Тези параметри следва да бъдат планирани внимателно при създаване и управление на виртуалната мрежа.

При конфигуриране на виртуалната машина, задължителните параметри са име на виртуалната машина, съвместимост с версия на VM Ware ESXi сървъра, тип и

версия на операционната система, брой ядра на виртуалния процесор, оперативна памет, използване на съществуващ или създаване на нов виртуален диск, капацитет на твърдия диск.

По същия начин могат да бъдат създадени и други виртуални машини с различни операционни машини.

Графичният вид на схемата на опитната постановка е показан на фиг. 2.

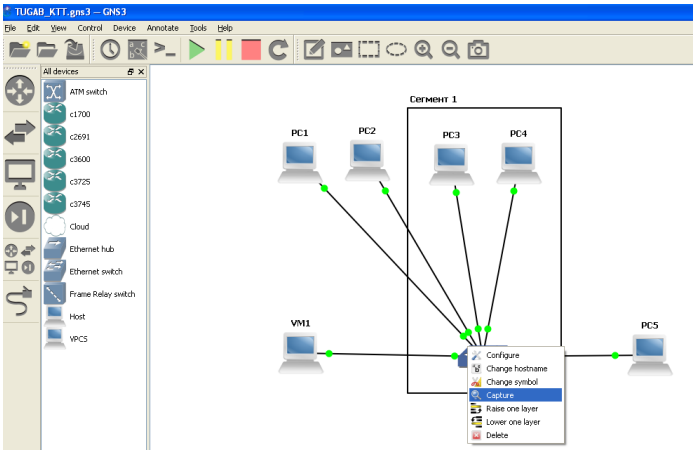


Фиг. 2. Схема на опитната постановка

В средата на мрежовия симулатор GNS3 опитната поставка е реализирана посредством наличния набор от емулатори за изграждане на представената на фиг. 2. схема на опитната постановка.

На фиг. 3 е показан изграденият симулационен модел въз основа на графичния вид на опитната постановка в среда GNS3.

Наблюдението на трафика е реализирано посредством мрежовия анализатор Wireshark, който е интегриран в средата на GNS3.



Фиг. 3. Симулационен модел в среда GNS3

За наблюдение на трафика е реализирана последователност от компютърни атаки от тип „отказ на обслужване“ в симулационната среда, като за всяка от тях е показан табличния вид на преминаващите пакети в Wireshark и графичния вид на трафика в съответния сегмент на мрежата.

3. Теоретична постановка на TCP SYN атака

По статистически данни за първо и второ тримесечие на 2015 г. атаките от типа TCP SYN атаките заемат около 50 % от всички компютърни атаки в Интернет. Като цяло атаките от типа „отказ на обслужване“ са основен проблем на информационната сигурност в световен мащаб. Въпреки, че историята на TCP SYN атаките датира от 1996 г., и до днес този тип атаки е една от най-често използваните за привеждане на огромен брой уеб хостове в състояние „отказ на обслужване”.

TCP SYN атаките са най-често срещаните атаки в транспортния слой на OSI модела [2]. Те се основават на стандартен комуникационен механизъм в TCP протокола, поради което тяхното филтриране или елиминиране се оказва изключително трудно. TCP SYN атаките се основават на механизма на установяване на TCP сесия (three-way handshake) или т. нар. „трипътно установяване”.

Комуникационния протокол TCP (от англ. Transmission Control Protocol) принадлежи към т. нар. връзково-ориентирани протоколи, т.е. преди да започне предаването на данни, се изгражда "връзка" между комуникиращите хостове, наречена сесия. Този подход гарантира надеждност на предаваните данни, тъй като механизма разчита на потвърждения, които удостоверяват, че данните са пристигнали до своето местоназначение. TCP протокола е един от основните мрежови протоколи, който осигурява управлението и обмена на информация между два или повече свързани хоста. Важно е да се отбележи, че TCP протокола е многозадачен, т.е. проектиран е за управление на един или повече процеса, без оглед на това дали са стартирани на едно или на няколко устройства. Многозадачността при TCP е реализиране посредством използването на различни портове. В процеса на комуникация се назначава пореден номер за всеки предаден байт, респективно получаване на потвърждение от приемащия хост за броя на получените байтове. Този подход забавя доставката на данни в сравнение с безвръзково-ориентираните протоколи, но за сметка на това гарантира надеждност при получаване на данните. Осъществяване и синхронизиране на комуникацията в TCP протокола се осъществява посредством следните флагове в структурата на TCP:

Source Port е 16 битово поле, което идентифицира изходния порт на хоста-изпращач;

Destination Port е 16 битово поле, идентифициращо входния порт на хоста-приемник;

Sequence Number е 32 битово поле, съдържащо поредния номер на първия октет от данни в сегмента;

Acknowledgment Number - 32 битово поле, съдържащо поредния номер на началния октет на следващата последователност от данни;

Data Offset – 4-битово поле, указващо началото на данните, следващи TCP хедъра. Налага се поради променливата дължина на хедъра.

Reserved – 3-битово поле, винаги е запълнено с 0.

Flags - съдържа 9 флага от по 1 бит

ECN (Explicit Congestion Notification) - уведомление за претоварване.

NS (Nonce Sum) - едно битово поле, използва се при ECN уведомление за наличие на претоварване (RFC 3540).

CWR (Congestion Window Reduced) е едно битово поле и се определя от изпращащия хост, за да покаже, че не е получила сегмент TCP с набор на ECE флаг и е отговорила на механизъм за контрол на претоварването (добавен в RFC 3168).

URG (Urgent) – едно битово поле, задаващо висок приоритет на данните. Активира Urgent Pointer указателя, сочещ първия байт от сегмента след спешните данни;

ACK (Acknowledgment) - 1-битово поле, задаващо сегмента като потвърждение;

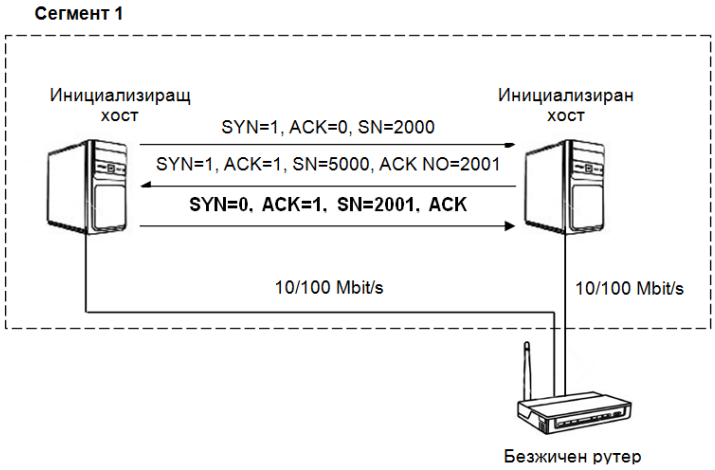
PSH (Push) – едно битово поле, което при стойност 1 задължава приемащия хост да не задържа пристигащите данни, а да ги изпрати към приложния процес от по-горен слой;

RST (Reset) - едно битово поле, задаващо стойност 1 ако е необходимо прекъсване на сесията;

SYN (Synchronization) – едно битово поле, задаващо инициализирането на сесия;

FIN (Finish) – едно битово поле, задаващо финализирането на сесия от изпращащия хост;

При „трипътното установяване" инициращия хост изпраща SYN (Synchronization) флаг към хоста получател, което представлява първа стъпка в механизма за установяване на сесия. При втората стъпка получателя отговаря на хоста-източник с ACK/SYN. Третата стъпка е свързана с ACK потвърждение от инициализиращия хост. Флаговете SYN и ACK приемат единствено стойности „0" и „1". В реални условия трипътното установяване може да бъде илюстрирано по следния начин:



Фиг .4. Схема на трипътно установяване на връзка

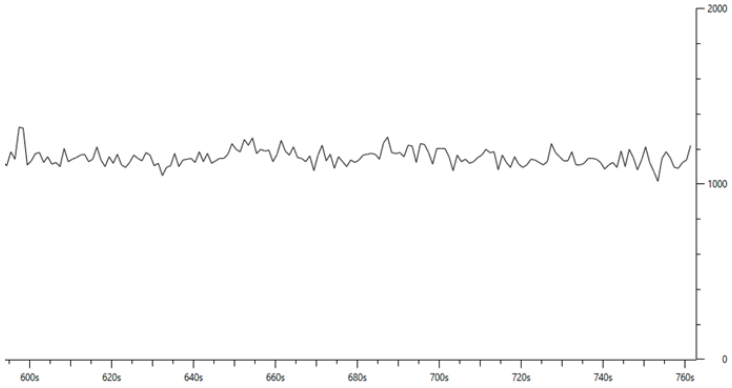
Инициализиращият хост изпраща TCP съобщение, съдържащо примерни стойности за флаговете SYN = 1, ACK = 0 и SN = 2000, където SN е Sequence Number и

може да бъде произволно число в размер на четири байта. Полето SN определя началния номер от който започва предаването на данните.

Хостът получател (инициализиран хост) на TCP съобщението отговаря на подателя с флагове, както следва: SYN = 1, ACK = 1, SN = 5000 и ACK NO=2001. Инициализиращият хост изпраща второ съобщение (трета стъпка) със следните стойности на флаговете: SYN=0, ACK=1, SEQ NO=2001, ACK NO=5001.

4. Симулиране на TCP SYN атака

При генериране на TCP SYN атака, атакувания хост е с IP адрес 192.168.1.102. Атаките са генерирани с произволни IP адреси, на фиг. 5 е показан графичният вид на трафика по време на TCP SYN атаката за период от 160 сек.



Фиг. 5. Графично изображение на Wireshark при генериране на TCP SYN атака

5. Изводи

При генериране на атака от типа TCP SYS се наблюдава запълване на канала за времето от 160 sec. с над 1000 пакета/sec. след което системата изпада е състояние „отказ на обслужване“.

Идентифицирането на инциденти, дължащи се на компютърни атаки от тип „отказ на обслужване” е изключително трудно, тъй като в общия случай атаките използват стандартни начини за комуникация между хостовете. Атаката не може да се разглежда като комуникация между няколко хоста, а като целенасочено иницииране на заявки от множество хостове към конкретно атакуван хост чрез подмяна на IP адресите на атакуващите хостове. Множеството от атакуващи хостове са от порядъка на сто и повече хиляди в зависимост от мащаба на атаката. В общия случай това не са 100 000 човека работещи на компютър, които отправят легални заявки към атакувания хост. Атаките от тип „отказ на обслужване” се инициира от т.нар. „botnet”или мрежа от ботове, и често представлява съвкупност от „заразени” уеб сайтове, който стартират скрипт към атакувания хост в определен момент. По този начин съвсем случайно заразени сайтове (хостове) могат да се окажат част от botnet атака. От реализираните симулации става ясно, че атаката може да бъде

генерирана от точно определени хостове с конкретни IP адреси, но и от случайни или маскирани IP адреси. Следователно не достатъчно условие при разработване на алгоритъм за предотвратяване на атаки от типа „отказ на обслужване” може да бъде достъпността до конкретен атакуващ хост, в общия случай, той може реално да съществува, но да не е инициатор на атаката.

Проверката за установяване на връзка, която не е осъществена от конкретен хост и осъществяване на повторна заявка за иницииране на трипътно установяване от същия хост би било достатъчно основание за съмнение относно легитимността на заявките. Това обаче е малко вероятно, изхождайки от направените симулации, тъй като всяка една заявка за трипътно установяване се получава от маскиран IP адрес, т.е. няма критерии за повтаряемост на IP адреса на атакуващия хост.

Литература

1. Николов, И., 2016, Изследване и анализ на информационната сигурност от гледна точка на понятията риск, заплаха, уязвимост, инцидент и несигурност, Научна конференция с международно участие "Право и интернет", БСУ, стр. 302-307, ISSN 1311-3771

2. Николов, И., 2016, Някои инструменти за изследване и анализ на информационната сигурност при симулиране на атаки от типа "отказ на обслужване", Международна научна конференция "Съвременни заплахи за сигурността на Европа", Висше училище по сигурност и икономика, Пловдив, ISBN 978-954-92776-0-9

3. D. Izvorska, B. Stoynova, 2013, Digital Libraries in Support of Web - based Training in Calculus,IJETCAS,New Delhi - 110016, India,,issue 4, vol1, pp 121- 124, ISSN(ONLINE): 2279 - 0055, ISSN(PRINTED):2279 - 0047

ДОСТЪПЪТ ДО ОФИЦИАЛНИ ДОКУМЕНТИ НА ИНСТИТУЦИИТЕ - ЕВРОПЕЙСКА ПРАКТИКА И ПРЕДИЗВИКАТЕЛСТВО В ГЛОБАЛНОТО СЪВРЕМИЕ

Лилия Цв. Лозанова

EMALL : LLOZANOVA72@ABV.BG

THE ACCESS TO OFFICIAL DOCUMENTS OF THE INSTITUTIONS – EUROPEAN PRACTICE AND CHALLENGE IN THE GLOBAL MODERNITY

***Abstract**: The ubiquitous invasion of the globalism in a various aspects of our life is combined with new challenges. Emerging communication and information systems and the Internet already identified new standards for access to different pieces of information. There have been irreversible changes not only in the individual but also in the collective consciousness under which the transparency of the information has a leading role in the democratic societies. Its assertion is independent of the provocation in the security field in an international sphere. In this way one of the global contradictions at the transparency level today is providing a protection of various forms of terrorism, including cyber threats.*

***Keywords**: access to information, transparency, European regulations*

В европейските страни все по-силни са тежненията за по-голяма прозрачност в работата на официалните институции. Този процес тече паралелно със здравословните усилия за повишаване на сигурността във всевъзможни планове, включително и киберсигурността. Новите заплахи в световен мащаб налагат преосмисляне на политики, така че превенцията се утвърждава като водещ подход.

Големият проблем не е дали да бъдат съвместени тези две противоположни тенденции, които условно са „ограничаване" и „разширяване" на свободния достъп до информация, как точно да се случи това. Според мен глобалните процеси в света са необратими - световната общественост изисква все повече прозрачност. Безспорно въпросът „Как да се постигнат едновременно и прозрачност, и сигурност?" има своите основания на фона на заплахите в международен мащаб.

В 21 век въпреки трудната международна ситуация, достойният и официален избор на институциите може да бъде само един - повече откритост и публичност на дейността.

В нормативните актове (както във всяка правна материя) обаче е заложена и противоположната тенденция – ограничаването на достъпа и публичността при определени случаи, обстоятелства и др.

В подкрепа на международната сигурност и борбата срещу тероризма са приети т.нар. Патриотични закони в САЩ [3]. Въпреки разнопосочните мнения за тях, събирането на лични данни се приема вече като необходимост. В България през декември м.г. беше приет Закон за противодействие срещу тероризма. В него са заложени и някои ограничения върху публикуването на информация, както и за спиране на уебсайтове и др. при съмнение, чието съдържание подбужда към тероризъм или чрез

което се разпространяват познания за извършване на тероризъм [закон].Предвидена е изключително бърза съдебна процедура в рамките на 24 ч. от получаване на сигнала за публикуване на такава информация. Заложено е изискване към „предприятията, предоставящи електронни съобщителни мрежи и/или услуги", които са длъжни да спрат достъпа до съответните интернет страници незабавно [4].

В статията са разгледани някои основни положения в Препоръка на Комитета на министрите към държавите-членки относно достъпа до официални документи (2002); Конвенцията за достъп до официални документи (2008 г.), както и отражението им в Трети национален план за действие в рамките на инициативата „Партньорство за открито управление (2016-2018) на Република България.

Тези нормотворчески текстове са създадени в отговор на глобалните процеси за прозрачност в работата на официалните институции, които ръководят обществеността на ЕС и намират отражение и у нас.

Базирани са на чл. 19 от Всеобщата декларация за правата на човека и чл. 10 от Европейската конвенция за правата на човека и основните свободи. Съдържанието им е близко, като и двата основополагащи документи прокламират, че „всеки човек … има право да търси, да получава и да разпространява информация и идеи чрез всички средства и без оглед на държавните граници [1]. Това базисно право е имагинентно свързано със „свободата на изразяването на мнения" [чл. 10, 2].

Тези права намират отражение и в основните принципи на Европейския съюз – прозрачност при вземането на решения и диалог с гражданското общество, както постановяват Лисабонския договор (Дял II) и консолидирания Договор за функционирането на ЕС.

Така през 2001 г. пример в тази насока е обнародван Регламент № 1049/2001, който гарантира публичния достъп до документи на Европейския парламент, на Съвета и на Комисията. Основните мотиви за приемането му са, че „откритостта дава възможност на гражданите да участват в процеса на вземане на решения и е гаранция за по – голяма законност ефективност и отговорност на управление на гражданите в демократична система.Откритостта допринася за засилване на принципите на демокрация и за спазването на основните права.." [11].

Същевременно е отбелязано, че „ някои документи поради изключително чувствителния им характер следва да бъдат обект на специална обработка" [11], като не е уточнено каква е тя. По отношение на мястото на регламентите в европейското право, трябва да се отбележи, че те « имат задължителен характер се прилагат в своята цялост във всички страни от ЕС [13].

На следващата година (2002 г.) е приета Препоръка (2002)2 на Комитета на министрите към държавите-членки относно достъпа до официални документи, която въпреки препоръчителния си характер очертава насоки на бъдеща работа на европейските институции. В нея се аргументират три ползи от „широкия достъп до официални документи" на институциите.

Първата е, че по този начин се предоставя „възможност на гражданите да си съставят адекватна представа и да формират критично становище относно състоянието на обществото, в което живеят и органите, които ги управляват, като същевременно се насърчава информираното участие на обществеността по въпроси от общ интерес" [8].Втората е, че се „повишава ефективността и ефикасността на администрацията и спомага за утвърждаването на нейната почтеност, като предот-

вратява риска от корупция”[8]. Третата е „утвърждаване легитимността на администрацията като служба в услуга на обществото и за укрепване на доверието на обществеността в публичните институции” [8].

В документа се акцентира, че «публичните институции трябва да се ангажират с осъществяването на активна комуникационна политика с цел да предоставят на обществеността всяка информация, която се смята за полезна в едно прозрачно демократично общество” [8].

Под «официални документи» се разбира «всяка информация, която е записана в каквато и да е форма, разработена или получена и съхранявана от държавните органи и която е свързана с държавни или административни функции, с изключение на документите в процес на подготовка” [8].

В препоръката са заложении и гаранциите за сигурността на информацията, сред които са нормативни документи, прокламиращи други права, какъвто е Конвенцията за защита на лицата при автоматичната обработка на лични данни. Предвидени са и ограничения на достъпа до официални документи, които целят да защитят :

„ - националната сигурност, отбраната и международните отношения;

- обществената безопасност;

- предотвратяването, разследването и съдебното преследване на престъпни деяния;

- личният живот и други законни частни интереси;

- търговски и други икономически интереси – както частни, така и държавни;

- равнопоставеността на страните в съдебното производство;

- природата;

- проверките, контрола и надзора от страна на публичните институции;

- икономическата, паричната и валутната политика на държавата;

- поверителността на обсъжданията в рамките на дадена публична институция или между институциите по време на вътрешната подготовка на въпроса [8].

Достъпът до документ може да се откаже, „ако разкриването на информацията, съдържаща се в него, ще навреди или може да навреди на горепосочените интереси, освен ако не съществува надделяващ обществен интерес от нейното разкриване” [8].

След 4 години работа, през 2008 г., е приета Конвенцията за достъп до официални документи на Съвета на Европа (CETS № 205). Сред първите подписали се под нея са 12 държави – Белгия, Естония, Финландия, Грузия, Унгария, Литва, Черна гора, Норвегия, Сърбия, Словения, Швеция, Македония. На 1 септември 2010 г. Босна и Херцеговина също се присъедини към конвенцията, а три държави (Унгария, Норвегия и Швеция), вече я ратифицираха [9].

В контекста на терористичните актове в редица европейски страни сред които Франция, Германия, Белгия и др. може да се търсят причините за това, че все още не са ратифицирали Конвенцията.

Но в международен мащаб е налице и противоположната тенденция. В Румъния през зимата на 2017 г. бяха проведении невиждани протести, свързани точно с темата на изследването- гражданското общество настоява за промяна на закон, който оправдава корумпирани политици. Въпреки, че съседната страна не е ратифицирала Конвенцията, събитията през февруари 2017 г. доказват, че гражданите

реално отстояват ценности като прозрачността, които иначе са прокламирани в нормативната база.

Представлява интерес с какво тази Конвенция е уникална, въпреки че основанията за създаването ѝ, посочени в Преамбюла, са почти идентични с Препоръка (2002)2 на Комитета на министрите към държавите членки относно достъпа до официални документи. Всъщност тя е първият в света правнозадължителен договор, гарантиращ достъпа до информация [9].

Сферата на действието ѝ са държавите – страни по Конвенцията, които са я подписали, или „депозирала своя документ за ратификация, приемане, одобряване или присъединяване, адресиран до Генералния секретар на Съвета на Европа" [5].

Конвенцията предвижда международен механизъм за мониторинг и е насочена към това държавите, които са я приели «да развият и да приложат вътрешни разпоредби, които позволяват по - широко право на достъп, при условие че, въпреки това, минималният набор се прилага" [5].

В нея се представя подробна дефиниция за това кои са „публичните институции", които осигуряват широк достъп до своите официални документи. Това са :

- законодателни органи по отношение на други техни дейности;
- органи на съдебната власт по отношение на други техни дейности;
- физически и юридически лица дотолкова, доколкото те изпълняват публични функции или оперират с обществени фондове, съгласно националното законодателство " [5].

Различните нива на приемане, подписване и ратифициране на Конвенцията задължава държавите да прилагат нейните разпоредби. Предвидена е и процедура за териториално прилагане на Конвенцията, като всяка държава може да присъедини или оттегли чрез нотификация свои територии или региони от полето на действие на този международен документ.

За разлика от Препоръка (2002)2, Конвенцията има задължително действие за държавите и техни региони, които са я приели. В обяснителния доклад към Конвенцията се посочва, че не се забранява на страните да поддържат по-високи стандарти и по-широк достъп до официални документи, отколкото заложените в нея [6].

В Конвенцията подробно са разписани правилата и условията при които се осъществява правото на достъп до официални документи (чл.2); възможните ограничения на достъпа (чл.3); заявленията за достъп и техните форми (чл.4 и чл.6); процедурата по разглеждане на заявленията за достъп (чл.5); таксите за заявленията (чл.7); процедурата за обжалване (чл.8).

Ограниченията за достъп до официалните документи, са идентични в заложените в Препоръка (2002)2, както и мотивите за тях.

Интерес представяват разясненията към някои от случаите, при които се прилагат ограничения в достъпа, подробно описани в Обяснителния доклад към Конвенцията. Един от тях е неразкриване на информация свързана с националната сигурност. Обаче нормотворците са посочили изрично ,че „понятието „национална сигурност" трябва да се прилага стеснително. Не трябва да се злоупотребява с него, за да се защити информация, която би разкрила нарушаване на човешки права, корупция в публични институции, административни грешки или информация, която просто е неудобна за държавните служители или публичните институции" [4].

Като пример за защита на документи, свързани с обществената безопасност е забраната за разкриване на информация за системите за сигурност на сгради и комуникации и др. [6].

Следващият аспект е защита на информация, свързана с дейността на публичните институции - наблюдение, разследване и контрол (проверки или одити на други организации, частни лица или вътре в институцията). Има се предвид не само с различен вид инспекции -текущи данъчни, трудови инспекции, на социалните служби, на институции в областта на здравеопазването и околната среда, а и данни от „училищните и университетски изпити" [6].

Подробно са разяснени ограниченията на достъпа във връзка със защита на търговски и други икономически интереси, частни или обществени. Като такава информация се определят т.нар. „търговски тайни", отнасящи се до конкуренция или производствени процеси, търговски стратегии, списъци на клиенти и други. Такива са и данните, които публичните институции използват при подготовка на колективни сделки, в които те самите участват, или данни за данъчни цели, събрани от частни и юридически лица„ [6].

Обществена чувствителност има и по отношение на защита на личния живот и други законни частни интереси. „Официалните документи могат да съдържат информация от личен или частен характер, която е защитена, например медицински картони и криминални досиета. Не трябва да се забравя, че Член 8 от Европейската конвенция за правата на човека гарантира правото на зачитане на личния и семеен живот" [6].

Защитата на информация във връзка с ефективното правораздаване въобще не се нуждае от коментар.

Внимание предизвиква така наречената подточка „к", която „предвижда възможността за ограничаване на достъпа до официални документи с цел защита на поверителността на процедурите в или между публичните институции във връзка с изследването на някакъв въпрос". Понятието „въпрос" е достатъчно широко, за да обхване всички видове теми, с които публичните институции се занимават, а именно отделни случаи, както и процедури за вземане на политически решения[6].

За съжаление е публична тайна, че у нас съществува практика за отграничение на достъпа до определена информация, неудобна за определени политици, бизнесмени или хора на висши постове, като дори е обявявана за «класифицирана».

Засега България не се присъединила към Конвенцията. Последният доклад за състоянието на достъпа до информация в България е от 2015 г., като към него са посочени препоръки към правната уредба за достъп до информация и нейното прилагане. Те са в три раздела - по отношение на правната уредба и административния капацитет, както и към уредбата, свързана с други задължения за прозрачност. За съжаление осъществяването им изисква определена воля на високо ниво. Явно ни предстои доста работа по отношение на материализиране на прозрачността, което е и възможно обяснение защо Конвенцията все още не е приета у нас, особено ако се акцентира на следващите препоръки:

- възстановяване на обема от информация, подлежаща на публикуване в секция"Профил на купувача",съгласно закона за обществените поръчки (ЗОП);

- създаване на ясно задължение за публикуване на съдържанието на декларациите за конфликт на интереси по ЗПУКИ;

- провеждане докрай на реформата, свързана с обществените обсъждания на проекти за нормативни актове и свързаната с тях необходима прозрачност» [10].

Тъй като целта на настоящата статия е да представи европейската практика в тази насока, няма да бъде правен анализ на българския закон за достъп до обществена информация приет 2000 г., а последно изменен през 2016 г.

В статията ще бъдат посочени само някои акценти в документ, в която са заложени мерки за повече прозрачност в работата на публичните институции у нас, а именно Трети национален план за действие в рамките на инициативата «Партньорство за открито управление»(1 юли 2016 – 30 юни 2018г.). Изборът на този документ е мотивиран от факта, че представлява своеобразна „пътна карта" от конкретни заложени ангажименти.

Заслужават внимание афишираните мотиви за приемането му.На първо място е акцентирано върху променената ситуация поради навлизането на новите технологии в глобален мащаб. В плана се отбелязва, че, „възможностите за търсене и получаване на информация, които Интернет дава на практика са неограничени. Това изгради един напълно нов потребителски модел за ползване и търсене на информация в обществото, който постави държавната администрация в едно изцяло ново положение – от нея изначално и по подразбиране се очаква да осигурява публичност на всяка информация, която съхранява и поддържа.

С появата на уеб 2.0 това очакване се доразви и трансформира в очакване правителството и неговите институции да функционират като платформа за гражданско действие и иновации, която впряга потенциала на всички потребители за подобряване на публичните политики и услуги.

Многобройните софтуерни приложения и инструменти, базирани на наличната публична информация, са силно оръжие, което позволява на отделните граждани и техните организации да контролират, но и да изискват промени в редица обществени сфери, които до скоро оставаха скрити за тях. Новите технологии направиха възможно данните в области като здравеопазване, финанси, транспорт, енергетика, климатични промени, образование, правоохранителна дейност, правораздаване, провеждане на избори и много други да бъдат анализирани и съпоставяни по такъв начин, че бързо да бъдат идентифицирани и визуализирани слабости, свързани с несправедливо или нецелесъобразно разходване на публичен ресурс, лошо управление, корупция или некомпетентност [12].

Глобалните промени и технологичния напредък променят ранжирането на основните ценности, които се приемат за основополагащи в демократичните общества и сред тях прозрачността в работата на институциите е сред водещите. В този смисъл, Третият план прокламира, че „отчетността и прозрачността винаги са били базисна ценност на всяко демократично общество.

Навлизането на новите технологии и разцветът на новите медии обаче придадоха ново качество и значение на тези базисни ценности. Днес вече държавното управление се разглежда като платформа, в която гражданите не са единствено получатели на информация и услуги, те могат да се превърнат в творци и автори на нови и по-добри услуги, ползвайки обществената информация. Откритостта вече е двупосочен процес, който посредством новите медии и технологии дава възможност на гражданите да налагат бързи промени в начина, по който функционират техните демократични институции" [12].

Част от конкретните приноси, в резултат на изпълнение на втория план са следните законодателни промени:

1. Измененията в Закона за нормативните актове, които предвиждат проектите на нормативни актове да могат да бъдат внасяни за обсъждане и гласуване само с оценка на въздействието. Това осигури инструмент, който позволява гражданите, бизнесът, депутатите да бъдат информирани реално за законите, които се приемат. Чрез оценката на въздействието се дава възможност за преценка дали новите нормативни актове са полезни на обществото, дали разходите, които те налагат на гражданите и на бизнеса, са по-големи, или по-малки от ползите.

- Оценките дават отговор на въпроса дали конкретен закон следва да бъде приет, защото има принос за общественото развитие, или не.

- Съгласно направените изменения оценките ще са неизменна част от всички нормативни актове и ще бъдат публикувани достъпно и онлайн.

- Срокът за обществена консултация, който беше 14 дни, бе удължен на 30 дни. Така гражданите и бизнесът ще имат повече информация за предстоящата законова и подзаконова уредба, но и повече време да се запознаят с тях и да изкажат мнение.

1.2. Въвежда се като иновация и последваща оценка, която да определи дали съответният закон е работил добре, дали е изпълнил заложените цели и на база на тази оценка да се направи преценка дали има смисъл да се продължава неговото действие, дали трябва да се промени, и ако е нужна промяна, в каква посока да е тя. Последващата оценка е инструмент, която дава възможност за информирани и фокусирани усилия за намаляване на регулацията за гражданите и бизнеса. Всички закони да подлежат на последваща оценка максимум до 5 г. след приемането им.

2. Измененията в промените в Закона за достъп до обществена информация. През 2007 г. беше уредена повторната употреба на обществена информация, а от началото на 2016 г. са в сила разпоредбите, които задължават институциите да публикуват информацията, която поддържат в отворен машинночетим формат, както и въвеждане на единна електронна точка за публикуване на информация в отговор на постъпили заявления за достъп до обществена информация.

3. За улеснение на процесите по публикуване на данни в отворен формат от края на 2014 г. функционира Порталът за отворени данни (opendata@government.bg). Само за една година на него бяха публикувани повече от 150 набора от данни, което позволи в изследване на European Data Portal България да бъде поставена сред десетте държави, които определят тенденциите в областта на отворените данни, наред с Великобритания, Естония, Австрия и др. [12].

3.1. Публикуването на публичната информация в отворен формат е задължение за организациите от публичния сектор съгласно Директива 2013/37/ЕС на Европейския парламент и на Съвета. С Решение №103 на Министерския съвет от 2015 г. е приет Списък от набори от данни по приоритетни области, които да се публикуват в отворен формат. Списъкът съдържа 119 набори от данни, като отварянето им и публикуването на платформата се извършва съгласно График на списъка с набори от данни по приоритетни области, които да се публикуват в отворен формат. В основата на проекта стои платформата с отворен код CKAN, разработена от Open Knowledge Foundation, Великобритания и използвана широко от държави като

Великобритания, Румъния, Словакия, Холандия, Австрия, Италия, Швеция, Южна Корея, в това число и Европейската комисия [7].

Към 14.01.2017 г. в портала в отметката „Организации" бяха регистрирани 398 такива, сред които са министерства, агенции, общини и др. От падащо меню има възможност да се избират предните отметки „данни", „поискай данни", „визуализации", „новини и информации". Към горепосочената дата свои документи бяха публикували 167 общини в България.

Третият план и раздел «IV. Тематични области и ангажименти", в които са разписани конкретни мерки за изпълнение, сред които са „1. Електронно управление"; „2. Достъп до информация"; „3. Отворени градове (практики на отворено управление на местно равнище); «4. Гражданско участие (диалог с гражданското общество чрез иновативни форми на взаимодействие, позволяващи обратна връзка и съавторство при формулиране на политики, свързани с разширяване на обществените консултации със заинтересованите страни)»; «5. Почтенно управление (подобряване на вътрешния и външен контрол върху дейността на институциите,в контекста на мерки за въвеждане на електронното управление в страната)». Повечето от заложените срокове за изпълнението текат в момента или са предвидени за изпълнение до края на 2018 г., затова няма да бъдат разгледани детайлно [12].

В заключение могат да се формулират някои изводи въз снова на беглия обзор на европейската практика по отношение на достъпа до документи на публичните институции.

1. Европейските институции (респ. и българските) отчитат променената ситуация поради навлизането на новите технологии във всички области на живота, които ранжират сред водещите обществени ценности прозрачността в управлението.

Както беше отбелязано, отделните граждани и техните организации могат вече не само да контролират, но и да изискват промени в редица обществени сфери, които до скоро оставаха скрити за тях.В подкрепа на тезата са и протестите в съседна Румъния.

2. Нормативната база се налага да предвиди гарантиране не само на други човешки права, но и да отчете новата ситуация, в която на преден план са терористичните и киберзаплахите.

3. В разгледаните европейски документи (вкл. и приетите в България) се съчетават с различна интензивност и двете тенденции- на прозрачност и на ограничение на достъпа до официални документи. Разбира се приоритетна във века на глобализма е тенденцията към откритост и свободен достъп до информация.

В заключение, законотворчеството на ЕС трябва да отговори на все по-нарастващите обществени очаквания за прозрачност, откритост, като водещи принципи и ценности в демократичните държави.

В нормативен план е декларирана воля за неговата реализация на практика, независимо от предизвикателствата за сигурността в международен мащаб.

Литература:

1. Всеобщата декларация за правата на човека, www.bg-pravo.com/2013/02/5.html.

2. Европейската конвенция за правата на човека и основните свободи, www.echr.coe.int/Documents/Convention_BUL.pdf.

3. Живановски, Н. Различни гледни точки за езика на омразата и неговото отношение към свободата на словото в американската и европейската теория и практика. Научни трудове на Русенски университет -2010,том. 49, серия 5-2.

4. Закон за противодействие на тероризма, http://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=110439

5.Конвенцията за достъп до официални документи на Съвета на Европа (CETS № 205), http://store.aip-bg.org/legislation/coe/conv_access_bg.pdf

6. Обяснителен доклад към Конвенция за достъп до официални документи на Съвета на Европа, http://store.aip-bg.org/legislation/coe/expl_report_conv_access_bg.pdf.

7. Портал за отворении дани на Република България opendata https://opendata.government.bg/about.

8. Препоръка (2002)2 на Комитета на министрите към държавите-членки относно достъпа до официални документи, http://www.aip-bg.org/documents/rec2_bg.htm.

9. Програма Достъп до информация, http://www.aip-bg.org/legislation.

10. Препоръки относно нормативната уредба, http://store.aip-bg.org//publications/ann_rep_bg/2015/2-proporuki.pdf

11. Регламент № 1049/2001, http://www.aip-bg.org/pdf/1049_2001.pdf.

12. Трети национален план за действие в рамките на инициативата «Партньорство за открито управление»(1 юли 2016 – 30 юни 2018 г.), http://www.strategy.bg/Articles/View.aspx?lang=bg-BG&categoryId=&Id=24&y=&m=&d=

13. http://europa.eu/european-union/eu-law/legal-acts_bg.

АЛГОРИТЪМ ЗА ИЗЧИСЛЯВАНЕ НА НЕЧЕТНАТА ПЕРИОДИЧНА КОРЕЛАЦИОННА ФУНКЦИЯ НА СИГНАЛИ

Борислав Й. Беджев[1], Иван Ог. Николов[2], Пламен Хр. Янакиев[3]

[1] Шуменски университет „Епископ Константин Преславски”, Факултет по технически науки, bedzhev@shu.bg
[2] Шуменски университет „Епископ Константин Преславски”, Факултет по технически науки, i.nikolov@shu.bg
[3] Шуменски университет „Епископ Константин Преславски”, Факултет по технически науки, p.yanakiev@shu.bg

Този доклад е подкрепен по Проект РД-08-78/03.02.2017 г. “Програмиране на микроконтролери в развойна среда Arduino”. Проектът е финансиран със средства, отпуснати целево от държавния бюджет, за присъщата на Шуменския университет научна и художествено-творческа дейност.

ALGORITHM FOR COMPUTING OF THE ODD PERIODIC CORRELATION FUNCTION OF SIGNALS

Borislav Y. Bedzhev, Ivan Og. Nikolov, Plamen Hr. Yanakiev

Abstract: *In the paper a new algorithm for processing of signals is suggested. The algorithm is based on the fast Fourier transformation. The usage of uniform procedures reduces significantly the complexity of the communication devices despite of the great diversity of the signals, exploited by the communication systems in order to preserve proper performance in cases of hostile radio-electronic environment.*

Key words: *algorithm, digital signal processing, radio-electronic resistance*

Увод

Както е известно, шумозащитеността на комуникационната система изразява нейната способност да изпълнява своите задачи в условията на радиоелектронно подавяне (РЕП). В общия случай РЕП включва два последователни етапа - радиотехническо разузнаване (наблюдение) и радиопротиводействие [1, 2]. Целта на радиотехническото разузнаване е установяването на работата (излъчването) на комуникационната система и определяне на нейните параметри, необходими за организация на радиопротиводействието. На тази база при радиопротиводействието се създават такива условия, които биха затруднили работата на системата или дори биха я блокирали напълно.

Основен способ на радиопротиводействие е генерирането на смущения. То е толкова по-ефективно, колкото повече информация за подавяната система е получена на етапа на радиоразузнаването, разкриваща най - уязвимите места на предавателите, приемниците и алгоритмите за обработка на информацията [1, 2, 3, 4, 5].

Способността на системата да изпълнява своите задачи в условията на РЕП се нарича шумоустойчивост.

Радиотехническото разузнаване се състои в последователното изпълнение на три основни задачи: откриване сигналите на разузнаваната система, анализ на структурата на откритите сигнали (определяне на техните параметри) и разкриване на съдържащата се в сигналите информация.

Във връзка със задачите, които решава радиоелектронното разузнаване, скритостта е три вида: енергетическа, структурна и информационна. Енергетическата скритост се характеризира със способността на системата да остане незабелязана от разузнавателните приемни устройства. Структурната скритост се заключава във възможностите на системата да затрудни максимално разкриването на принципите на модулация на сигналите, техните честотни и временни параметри.

Информационната скритост е способността на системата да противостои на мерките, насочени към разкриване на смисъла на предаваната с помощта на сигнали информация. Информационната скритост се нарича още криптоустойчивост и представлява важен самостоятелен научен проблем.

Енергетическата и структурната скритост не са напълно независими параметри тъй като те едновременно зависят от честотно - времевите характеристики на сигналите, както и от възможностите на системата достатъчно бързо да сменя типа на използваните сигнали. В резултат на анализ на практическия опит от последните 50 години е установено, че добро ниво на шумозащитеност се постига само ако обемът на системата от сигнали L е достатъчно голям [1, 2]:

(1) $$L \approx B^m .$$

Тук m, $m \geq 2$ е цяло число, а B е базата на сигнала, която се определя от времевата му продължителност T_s и от ширината на спектъра му F_s:

(2) $$B = T_s.F_s .$$

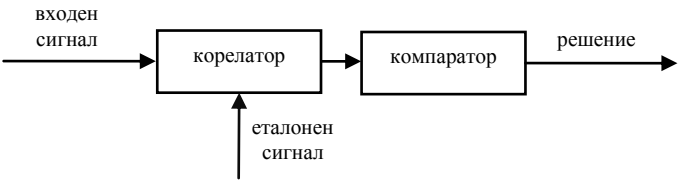
В най-обща ситуация разширяването на обема на системата от сигнали води до значително увеличаване на сложността и стойността на комуникационната апаратура. Предвид на това противоречие по-нататък в доклада е обоснована възможността за оптимална обработка на голямо количество различни сигнали с еднотипни цифрови процедури.

Докладът е структуриран както следва. Първо се припомнят основните операции при оптималното приемане на сигналите. След това се обосновава един нов алгоритъм за изчисляване на нечетната периодична автокорелационна функция на приетите сигнали с помощта на бързо преобразуване на Фурие (БПФ). Накрая се обсъжда практическото приложение на предложения в доклада алгоритъм.

Основни операции при оптималното приемане на сигнали

В теорията на оптималното приемане е доказано, че приемниците на комуникационните системи трябва да имат структурата, показана на фиг. 1 [1, 2, 3, 4, 5].

Както се вижда, оптималният приемник за сигнали следва да съдържа корелатор и компаратор. При това корелаторът пресмята стойността на взаимнокорелационната функция при нулево временно отместване на копието (еталона) на очаквания сигнал $\xi^*(t)$ (представляващ мащабно намалено и комплексно-спрегнато копие на излъчения от предавателя сигнал) с приетия сигнал $\xi(t)$. След това, ако получената стойност е по-голяма от зададения праг, компараторът взема решение, че на входа на приемника е постъпил полезен сигнал.



Фиг. 1: *Структура на оптимален приемник за сигнали*

Следва дебело да се подчертае, че описаните процедури максимизират отношението *сигнал/шум* (с-л/ш) на изхода на приемника при наличие на адитивен бял Гаусов шум, което е най - типичната ситуация при работата на комуникационните приемници.

В зависимост от типа на използваните сигнали работата на цифровите корелатори може да се опише със следните математически модели [6].

Нека

(3) $$\{\xi(i)\}_{i=0}^{N-1} = \{\xi(0), \xi(1),..., \xi(i),..., \xi(N-1)\}$$

е сигналът на входа на приемника на комуникационната система след аналого - цифровото преобразуване. Тук $u(0), u(1),..., u(j),..., u(N-1)$ са комплексни числа

(4) $$\xi(i) = U_{mi} e^{j\frac{2\pi}{N}u(i)}, \quad j = \sqrt{-1}, \quad u(i) \in \{0,1,..., N-1\}, \quad i = 0,1,..., N-1$$

представящи амплитудата U_{mi} и началната фаза $e^{j\frac{2\pi}{N}u(i)}$ на чиповете, формиращи сложния сигнал (3). При това последователността от цели числа

(5) $$\{u(i)\}_{i=0}^{N-1} = \{u(0), u(1),..., u(i),..., u(N-1)\}$$

описва закона на фазова манипулация на сигнала (3).

Ако приетият сигнал (3) е импулсен, тогава корелаторът от фиг. 1 изчислява неговата *автокорелационна функция* (АКФ) по формулата:

(6) $$R_{\xi\xi}(k) = \begin{cases} \sum_{i=0}^{N-1-|k|} \xi(i).\xi^*(i+|k|), & -(n-1) \le k \le 0, \\ \sum_{i=0}^{N-1-k} \xi^*(i).\xi(i+k), & 0 \le k \le (n-1). \end{cases}$$

Тук

(7) $$\{\xi^*(i)\}_{j=0}^{N-1} = \{\xi^*(0), \xi^*(1),...\xi^*(i),...\xi^*(N-1)\}$$

е еталонният сигнал, $k.\tau_{ch}$ е времевото отместване между момента на постъпване на входния сигнал и момента на подаване на еталонния сигнал, τ_{ch} е продължителността на чиповете, а символът „*“ означава „комплексна спрегнатост“.

Ако входният сигнал е периодичен, тогава (3) е един период на входния сигнал и корелаторът изчислява неговата *периодична автокорелационна функция* (ПАКФ) по формулата:

$$Q_{\xi\xi}(k) = \sum_{j=0}^{N-1} \xi(j).\xi^{*}\left\langle j+k \right\rangle_{N} \ . \tag{8}$$

Тук символът „$\left\langle \ \right\rangle_{N}$ “ означава, че сумата в скобите се взема по модул *N*.

От формули (6 и 8) се вижда, че АКФ и ПАКФ са свързани със съотношението:

$$Q_{\xi\xi}(k) = R_{\xi\xi}(k) + R_{\xi\xi}(-N+k), \ 0 < k < N \ . \tag{9}$$

Периодичните сигнали всъщност са дълги повторения на един и същ импулсен сигнал. Така например, ако (3) е импулсен сигнал с продължителност $T_s = N.\tau_{ch}$, тогава при безкрайното му повторение се получава периодичният сигнал

$$\begin{aligned} \{\xi(i)\}_{i=0}^{\infty} &= \{\xi(0),\xi(1),...,\xi(N-1),\xi(0),\xi(1),...,\xi(N-1),...\} = \\ &= \left\{\{\xi(i)\}_{i=0}^{N-1},\{\xi(i)\}_{i=0}^{N-1},\{\xi(i)\}_{i=0}^{N-1},\{\xi(i)\}_{i=0}^{N-1},....\right\} \end{aligned} \tag{10}$$

Важно е да се отбележи, че енергията на периодичните сигнали се излъчва равномерно във времето. В резултат комуникационните системи, използващи периодични сигнали, имат по-висока скритост в сравнение с комуникационните системи, работещи с импулсни сигнали [1], [2]. По тази причина в съвременните сензорни мрежи широко се използват маломощни датчици, излъчващи периодични оптически, радио или акустични сигнали.

От (10) се вижда, че структурната сложност на дадена система от периодични сигнали лесно може да се удвои като през нечетните периоди на работа се излъчва инвертиран сигнал, т.е.

$$\{\zeta(i)\}_{i=0}^{\infty} = \left\{\{\xi(i)\}_{i=0}^{N-1},-\{\xi(i)\}_{i=0}^{N-1},\{\xi(i)\}_{i=0}^{N-1},-\{\xi(i)\}_{i=0}^{N-1},....\right\} \tag{11}$$

В такива ситуации корелаторът на оптималния приемник следва да изчислява така наречената *нечетна ПАКФ* (НПАКФ). Следва да се отбележи, че всъщност ПАКФ и НПАКФ на сигналите имат еднаква важност при анализа на работните характеристики на комуникационните системи [3], [4], [5], но тук няма възможност този проблем да бъде обсъждан в детайли.

От (11) следва, че АКФ и НПАКФ са свързани със съотношението:

$$Q_{odd\,\xi\xi}(k) = R_{\xi\xi}(k) - R_{\xi\xi}(-N+k), \ 0 < k < N \ . \tag{12}$$

Както се вижда, изчисляването на НПАКФ е по - сложно от изчисляването на ПАКФ. По тази причина в следващия раздел от доклада ще бъде обоснован алгоритъм за изчисляване на НПАКФ на сигналите, който ефективен от изчислителна гледна точка, тъй като може да се реализира чрез БПФ.

Алгоритъм за изчисляване на нечетната периодична корелационна функция на сигнали

В теорията на комуникационните системи е доказано, че изчисляването на ПАКФ може да се представи в следната полиномиална форма [3, 6]:

$$\begin{aligned} Q_{\xi\xi}(x) = &\left(\xi(N-1)x^{N-1} + ... + \xi(1)x + \xi(0)\right)\times \\ &\times\left(\xi^{*}(N-1)x^{-(N-1)} + ... + \xi^{*}(1)x^{-1} + \xi^{*}(0)\right) \mod(x^{N}-1) \end{aligned} \tag{13}$$

В (13) $Q_{\xi\xi}(x)$ е така наречената генерираща функция или полином на Хол (Hall's polynomial) [3], [6] на ПАКФ на сигнала $\{\xi(i)\}_{i=0}^{N-1}$:

(14) $$Q_{\xi\xi}(x) = q_{N-1}x^{N-1} + q_{N-2}x^{N-2} + ... + q_0$$

като тук отчетите $q_0 = E_\xi$ и $q_1, q_2, ..., q_{N-1}$ са основният и страничните листа на ПАКФ.

Естествено

(15) $$F_\xi(x) = \xi(N-1)x^{N-1} + ... + \xi(1)x + \xi(0)$$

е генериращата функция (полиномът на Хол) на сигнала $\{\xi(i)\}_{i=0}^{N-1}$, а

(16) $$F_\xi^*(x) = \xi^*(N-1)x^{-(N-1)} + ... + \xi^*(1)x^{-1} + \xi^*(0)$$

е полином, който е комплексно спрегнат и реципрочен на полинома $F_\xi(x)$.

Означението $\mathrm{mod}(x^N - 1)$ показва, че x не е произволна променлива. По-конкретно, тя може да приема само такива стойности, че да е изпълнено

(17) $$x^N = 1, x^{N+1} = x, x^{N+2} = x^2, ...$$

Тъй като корените на уравнението

(18) $$x^N - 1 = 0$$

са само така наречените N-ти корени от единицата

(19) $$e^{j\frac{2\pi}{N}l},\ l = 0,1,..., N-1,$$

то тези числа изчерпват всички допустими стойности на променливата x в (13).

Следва дебело да се подчертае, че ПАКФ може да се изчислява с БПФ. Действително, когато променливата x в (13) последователно приема стойностите (19), тогава полиномите (14) и (15) изразяват отчетите на спектрите на ПАКФ и на сигнала $\{\xi(i)\}_{i=0}^{N-1}$. Следователно полиномиалното равенство (13) е еквивалентно на равенствата

(20) $$C_\xi(l).C_\xi^*(l) = C_Q(l),\ l = 0,1,..., N-1.$$

При това

(21) $$C_\xi(l) = F_\xi\left(e^{j\frac{2\pi}{N}l}\right) = \xi(N-1)\left(e^{j\frac{2\pi}{N}l}\right)^{N-1} + ... + \xi(1)\left(e^{j\frac{2\pi}{N}l}\right) + \xi(0),$$
$$l = 0,1,..., N-1$$

са отчетите на спектъра на използвания от системата сигнал $\{\xi(i)\}_{i=0}^{N-1}$, $C_\xi^*(l)$ са техните комплексно-спрегнати стойности, а $C_Q(l)$ са отчетите на спектъра на ПАКФ.

Следователно корелаторът на оптималния приемник може да изчислява ПАКФ на приетите сигнали по следния алгоритъм.

Алгоритъм за изчисляване на ПАКФ

1. С помощта на БПФ се изчислява спектърът $\{C_\xi(l)\}_{l=0}^{N-1}$ на използвания от системата сигнал $\{\xi(i)\}_{i=0}^{N-1}$. След това се изчислява и се запомня комплексно спрегнатият спектър $\{C_\xi^*(l)\}_{l=0}^{N-1}$.

2. С помощта на БПФ се изчислява спектърът $\{C_\xi(l)\}_{l=0}^{N-1}$ на приетия сигнал.

3. Спектърът $\{C_\xi(l)\}_{l=0}^{N-1}$ се умножава поелементно с комплексно спрегнатия спектър $\{C_\xi^*(l)\}_{l=0}^{N-1}$, при което се получава спектърът $\{C_Q(l)\}_{l=0}^{N-1}$ на ПАКФ.

4. С обратно БПФ, приложено върху $\{C_Q(l)\}_{l=0}^{N-1}$, се изчислява ПАКФ $\{q_i\}_{i=0}^{N-1}$.

Тъй като към момента са разработени и внедрени големи серии от специализирани контролери, които са евтини и извършват БПФ много бързо, се вижда, че горният алгоритъм е ефективен от изчислителна гледна точка и има ниска цена на практическа реализация.

Аналогично на (13), НПАКФ може да се представи в следната полиномиална форма

$$Q_{odd\xi\xi}(x) = \left(\xi(N-1)x^{N-1} + \ldots + \xi(1)x + \xi(0)\right)\times \\ \times\left(\xi^*(N-1)x^{-(N-1)} + \ldots + \xi^*(1)x^{-1} + \xi^*(0)\right) \mod(x^N+1) \tag{22}$$

Тук означението $\mod(x^N+1)$ показва, че допустимите стойности на x са нулите на модулния полином x^N+1. Тъй като

$$x^{2N}-1 = (x^N-1)(x^N+1) \tag{23}$$

в (22) променливата x може да приема само нечетните $2N$-ти корени от единицата

$$e^{j\frac{2\pi}{2N}l},\ l = 1,3,5,\ldots \tag{24}$$

От този анализ се вижда, че в най-обща ситуация изчисляването на НПАКФ е по-сложно от изчисляването ПАКФ, тъй като е невъзможно директното използване на представения по-горе спектрален алгоритъм.

Сега следва да се забележи, че ако дължината на сигнала N е нечетно число, тогава трансформацията

$$x \to -y \tag{25}$$

преобразува (22) до вида

$$Q_{odd\xi\xi}(-y) = \left(\xi(N-1)(-y)^{N-1} + \ldots + \xi(1)(-y) + \xi(0)\right)\times \\ \times\left(\xi^*(N-1)(-y)^{-(N-1)} + \ldots + \xi^*(1)(-y)^{-1} + \xi^*(0)\right) \mod(-y^N+1) \tag{26}$$

В (26) полиномите на Хол съответстват на сигнал, получен от сигнала $\{\xi(i)\}_{i=0}^{N-1}$ чрез поставяне на знак „-“ пред отчетите с нечетни номера $1,3,5,\ldots,N-2$. Тази

процедура е прието да се нарича алтерниране на сигнала [3, 4, 5]. Също така нулите на полинома $-y^N+1$ са *N*-ти корени от единицата (19). Всичко това доказва следното твърдение.

Твърдение: Нека (3) е сигнал, чиято дължина *N* е нечетно число, а НПАКФ е

(27) $\{q_i\}_{i=0}^{N-1} = \{q_0, q_1, q_2, ..., q_{(N-1)/2}, -q^*_{(N-1)/2}, ..., -q_2^*, -q_1^*\}$

Тогава производният от него алтерниран сигнал:

(28) $\{\zeta(i)\}_{i=0}^{N-1} = \{\xi(0), -\xi(1), \xi(2), -\xi(3), \xi(4), -\xi(5), ..., \xi(N-1)\}$

има ПАКФ

(29) $\{q_i\}_{i=0}^{N-1} = \{q_0, q_1, q_2, ..., q_{(N-1)/2}, q^*_{(N-1)/2}, ..., q_2^*, q_1^*\}$

Твърдението позволява да се повиши практически два пъти структурната сложност на множеството от сигнали на всяка комуникационна система, използваща периодични сигнали по следния начин.

Нека (3) е използван от системата периодичен сигнал с нечетна дължина. В случайни моменти от време системата променя сценария на излъчване на сигнала от (10) на (11). При това приемникът не преминава към изчисление на НПАКФ по класическия израз (12), а използва следният алгоритъм.

Алгоритъм за изчисляване на НПАКФ

1. Знакът на нечетните отчети на приетия сигнал се променя на противоположен в съответствие с (28).

2. С помощта на БПФ се изчислява спектърът $\{C_\zeta(l)\}_{l=0}^{N-1}$ на алтернирания сигнал.

3. Спектърът на алтернирания сигнал се умножава поелементно с комплексно спрегнатия му спектър $\{C^*_\zeta(l)\}_{l=0}^{N-1}$, при което се получава спектърът $\{C_Q(l)\}_{l=0}^{N-1}$ на ПАКФ.

4. С обратно БПФ, приложено върху $\{C_Q(l)\}_{l=0}^{N-1}$, се изчислява ПАКФ $\{q_i\}_{i=0}^{N-1}$.

5. Знаците на отчетите на ПАКФ с номера $(N-1)/2+1, (N-1)/2+2, ..., N-1$ се променят на противоположни.

В редица режими на работа на комуникационните системи последната стъпка от алгоритъма може да бъде пропускана. Например при несинхронно предаване/приемане на изхода на приемника листата на корелационните функции на приетите сигнали се смесват хаотично и всъщност има значение само тяхната амплитуда.

Заключение

В доклада е обоснован алгоритъм за изчисляване на НПАКФ на сигнали, чиято дължина е нечетно число. Алгоритъмът позволява да се повиши практически два пъти структурната сложност на множеството от сигнали на всяка комуникационна система, работеща в непрекъснат режим на излъчване. Същевременно сложността на приемника не се увеличава, тъй като оптималната обработка на приетите сигнали се извършва със спектрален алгоритъм, използващ БПФ.

Литература:

1. А. А. Агафонов, С. Н. Артюх и др. под ред. В. Г. Радзиевского, “Современная радиоэлектронная борьба. Вопросы методологии,” Радиотехника, Москва, 2006, 424 с.
2. А. И. Куприянов, А. В. Сахаров, “Теоретические основы радиоэлектронной борьбы,” Вузовская книга, Москва, 2007, 356 с.
3. S. Golomb and G. Gong, “Signal design for good correlation,” Cambridge University Press – 2005
4. H. D. Luke and H. D. Schotten, “Odd- Perfect, Almost Binary Correlation sequences,” *Transactions on Aerospace and electronic systems*, vol. 31, No 1, January 1995, pp. 495-498
5. D. V. Srawate and M. B. Pursley, “Crosscorrelation Properties of Pseudorandom and Related sequences,” *Proceedings of the IEE*, vol. 68, No 5, May 1980, pp. 593-619
6. D. Velikova, V. A. Mutkov, and B. B. Bedzhev, “Analysis of the conditions for synthesis of efficient side-lobes suppression filters for binary phase manipulated signals,” *Journal Scientific and applied research*, ISSN 1314-6289, vol. 6, pp. 106-113, 2014.

АНАЛИЗ НА ПРИЛОЖИМОСТТА НА ТЕОРЕТИКО – ЧИСЛОВИТЕ СПЕКТРАЛНИ МЕТОДИ В ИНТЕЛИГЕНТНИТЕ СИСТЕМИ ЗА НАБЛЮДЕНИЕ И КОНТРОЛ

Борислав Й. Беджев[1], Иван Ог. Николов[2], Пламен Хр. Янакиев[3]

[1] Шуменски университет „Епископ Константин Преславски”, Факултет по технически науки, bedzhev@shu.bg
[2] Шуменски университет „Епископ Константин Преславски”, Факултет по технически науки, i.nikolov@shu.bg
[3] Шуменски университет „Епископ Константин Преславски”, Факултет по технически науки, p.yanakiev@shu.bg

Този доклад е подкрепен по Проект РД-08-78/03.02.2017 г. “Програмиране на микроконтролери в развойна среда Arduino”. Проектът е финансиран със средства, отпуснати целево от държавния бюджет, за присъщата на Шуменския университет научна и художествено-творческа дейност.

ANALYSIS OF THE APPLICABILITY OF THE NUMBER THEORETIC TRANSFORMATIONS IN THE SMART SYSTEMS FOR SURVEILLANCE AND CONTROL

Borislav Y. Bedzhev, Ivan Og. Nikolov, Plamen Hr. Yanakiev

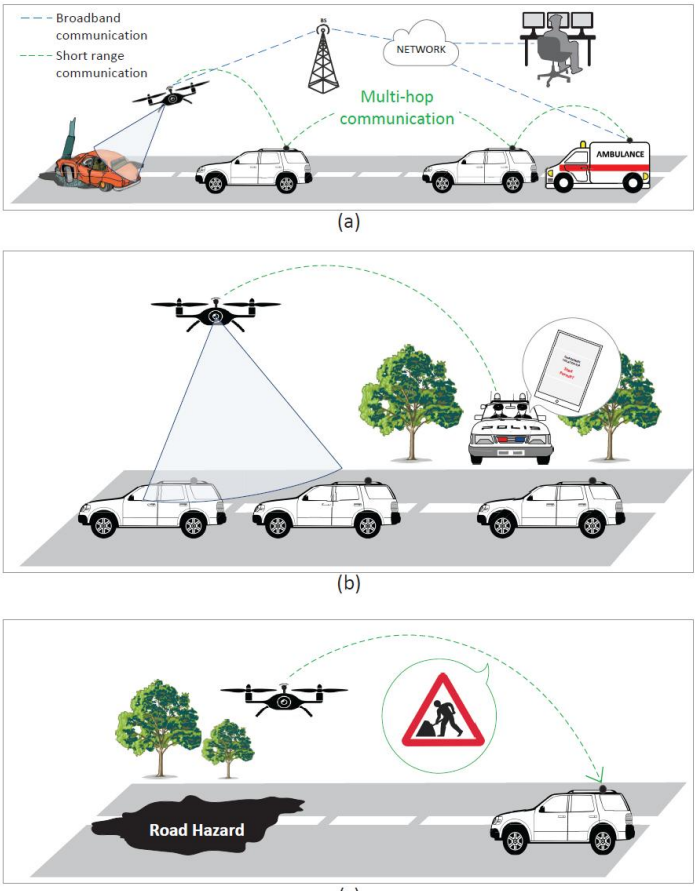
Abstract: *The present smart systems for surveillance and control should process large amount of data in real time. With regard to this fact in the paper the possibility for implementation of the digital signal processing by number theoretic transformations is analyzed. This approach allows the complex communication algorithms to be realized by the means of cost-effective, energy-effective and reliable digital processors.*

Key words: *number theoretic transformation, digital signal processing, reliable communication*

Увод

Постоянното разрастване на автомобилния парк и увеличаването на интензивността на автомобилния трафик са сериозен проблем в съвременните градове. По тази причина във всички развити страни се провеждат активни широко обхватни научно – изследователски разработки, насочени към изграждане на *интелигентни транспортни системи* (ИТС). Основен компонент на ИТС са *сензорните мрежи* (СМ) за наблюдение и контрол на трафика. Те са изградени от стационарни сензори и специално екипирани дронове, на които се възлага решаването на широк кръг задачи. Основните от тях са: документиране на обстоятелствата при пътни инциденти и предаване на доклади за тях, следене за спазването на правилата за движение, измерване на скоростта на автомобилите и генериране на динамични сигнали за пътната обстановка. Тези задачи са илюстрирани на фиг. 1 [4]. За успешното им изпълнение е необходимо дроновете да летят заедно и да действат координирано при изпълнение на всяка специфична мисия. Работата в екип позволява на дроно-

вете да преодоляват успешно ограниченията, породени от малките им размери, ниска товароносимост и малък енергетичен запас [4].



Фиг. 1: *Задачи, решавани от СМ, използваща дронове:* **а)** *документиране на обстоятелствата при пътни инциденти и предаване на доклади за тях;* **в)** *следене за спазването на правилата за движение и измерване на скоростта на автомобилите;* **с)** *генериране на динамични сигнали за пътната обстановка*

От фиг. 1 се вижда, че успешното изпълнение на функциите, възложени на дроновете, съществено зависи от способността им да осъществяват устойчива комуникация, както по между си, така и със стандартните мобилни мрежи дори в тежка радио-електронна обстановка. За решаването на тази задача е необходимо предавателите и приемниците на дроновете да използват сложни алгоритми за

цифрова обработка на сигнали, които обаче най–често се реализират с устройства, характеризиращи се с относително големи размери, цена и потребление на енергия. От друга страна, ограничената товароносимост на дроновете не позволява използването на комуникационна апаратура с големи размери и високо енергопотребление. Предвид на това противоречие по-нататък в доклада е обоснована възможността за реализиране на обработката и филтрацията на комуникационните сигнали на дроновете чрез така наречените теоретико-числови преобразувания, които се осъществяват изцяло с прости целочислени аритметични операции.

Докладът е структуриран както следва. Първо се припомнят основните приложения на спектралните методи за обработка на сигнали. След това се обосновава възможността за реализиране на дискретно преобразуване на Фурие в крайни алгебрични полета посредством аритметика с фиксирана запетая. Накрая се обсъжда практическото приложение на предложения в доклада подход.

Основни приложения на спектралните методи за обработка на сигнали

Нека

(1) $$\{\xi(i)\}_{i=0}^{N-1} = \{\xi(0), \xi(1),..., \xi(i),..., \xi(N-1)\}$$

е сигналът на входа на приемника на комуникационна система след аналого - цифровото преобразуване. Тук $u(0), u(1),..., u(j),..., u(N-1)$ са комплексни числа

(2) $$\xi(i) = U_{mi} e^{j\frac{2\pi}{N}u(i)},\ j = \sqrt{-1},\ u(i) \in \{0,1,..., N-1\},\ i = 0,1,..., N-1$$

представящи амплитудата U_{mi} и началната фаза $e^{j\frac{2\pi}{N}u(i)}$ на чиповете, формиращи сложния сигнал (1). При това последователността от цели числа

(3) $$\{u(i)\}_{i=0}^{N-1} = \{u(0), u(1),..., u(i),..., u(N-1)\}$$

описва закона на фазова манипулация на сигнала (1) [5, 6, 7].

По естествен начин на сигнала $\{\xi(i)\}_{i=0}^{N-1}$ се съпоставя полиномът

(4) $$F_\xi(x) = \xi(N-1)x^{N-1} + ... + \xi(1)x + \xi(0),$$

наречен генерираща функция или полином на Хол [3, 5, 6, 7].

Когато променливата x в (4) последователно приема стойностите

(5) $$e^{j\frac{2\pi}{N}l},\ l = 0,1,..., N-1,$$

наречени *N*-ти корени от единицата, тогава полиномът (4) представя отчетите на спектъра на сигнала $\{\xi(i)\}_{i=0}^{N-1}$, т.е.:

(6) $$C_\xi(l) = F_\xi\left(e^{j\frac{2\pi}{N}l}\right) = \xi(N-1)\left(e^{j\frac{2\pi}{N}l}\right)^{N-1} + ... + \xi(1)\left(e^{j\frac{2\pi}{N}l}\right) + \xi(0),$$

$$l = 0,1,..., N-1$$

В теорията на комуникационните системи е доказано, че е налице еднозначно обратимо съответствие между сигнала (1) и спектъра му (6) [1, 2, 3]. При това

трансформацията (6) се нарича *право дискретно преобразуване на Фурие* (ДПФ), а обратната трансформация от (6) към (1) – *обратно* ДПФ.

Спектралният метод е ефективен аналитичен инструмент (често това е единственият начин) за решаване на някои много важни проблеми при проектирането на комуникационни системи като например: определяне на вида на сигнала след преминаване през честотно–селективен канал за свръзка, оценка на интерференциите между едновременно работещи радио-електронни системи и устройства, компресия на изображения, оптимално приемане на сигнали и др.

Следва специално да се отбележи, че от изчислителна гледна точка преобразуването на Фурие в класическата му форма има следния недостатък. На практика всеки отчет на обработвания сигнал се представя с две цели числа – по едно за реалната и имагинерната компонента на отчета. Аналогично всеки от *N*-тите корени от единицата (5) се представя с две числа, но те са целочислени закръгления на ирационални числа. По тази причина за прилагане на спектралните методи за обработка на сигналите са необходими изчислителни устройства със сложна вътрешна структура, използващи аритметика с плаваща запетая.

Тези недостатъци са съществена пречка за използването на класическо ДПФ при обработката на големи масиви от информация в реално време в интелигентните системи за наблюдение и контрол, изградени от малоразмерни сензори и дронове.

Анализ на приложимостта на теоретико – числовите спектрални методи в интелигентните системи за наблюдение и контрол

Теоретико – числовите спектрални методи за цифрова обработка на сигналите са свободни от недостатъците на класическото ДПФ и могат да се реализират с евтини процесори с малка консумация на енергия, използващи целочислена аритметика. Този факт ще бъде обоснован по следния начин. Първо следва да се забележи, че всеки отчет на сигнала (1) е комплексно число

(7) $$\xi(i) = s(i) + jy(i),\ i = 0,1,...,N\ ,$$

чиито реална $s(i)$ и имагинерна компоненти $y(i)$ са цели числа, тъй като са резултат от работата на някакъв аналого–цифров преобразувател с крайна разрядност. Тъй като аритметичните операции с комплексни числа се извършват покомпонентно, без ограничение на общността по–нататък може да се разгледа само реалната част на сигнала (1), т.е.

(8) $$S = \{s(0), s(1),..., s(N-1)\},\ \forall s(i) \in Z_p$$

Второ, винаги отчетите на сигнала (8) приемат стойности в интервала $[0, p-1]$ като тук p е достатъчно голямо просто число. Освен това може да се приеме, че дължината на сигнала N или съвпада с числото $q = p^n - 1$ или е точен делител на q. Тогава *теоретико-числовият спектър* (ТЧС) на S се изчисляват по следната формула, представляваща аналог на правото ДПФ в крайното алгебрично поле $GF(p^n)$ [1, 2, 3]:

(9) $$A_F(k) = \sum_{i=0}^{N-1} s(i).\beta^{ki},\ k = 0,1,...,N-1$$

В (8) β е елемент на $GF(p^n)$ от ред *N*, което означава, че *N* е минималното положително число със свойството

(10) $$\beta^N = 1.$$

Следва да се отбележи, че съкращението *GF* означава *Galois Field* (*поле на Галоа*) и е въведено в чест на великия френски математик *Еварист Галоа*, който пръв започва системно да изследва крайните алгебрични полета в началото на 19-ти век.

Също както при ДПФ, ако е известен ТЧС

(11) $$A_F = \{A_F(0), A_F(1), ..., A_F(N-1)\},\ \forall A_F(k) \in GF(p^n)$$

на някакъв цифров сигнал, тогава неговите отчети могат да се определят чрез обратното *теоретико-числово преобразование* (ТЧП) [1, 2, 3]:

(12) $$s(i) = \frac{1}{N}\sum_{k=0}^{N-1} A_F(k).\beta^{-ki},\ i = 0,1,..., N-1$$

От (9) и (12) се вижда, че правото и обратното ТЧП напълно съответстват на класическите право и обратно ДПФ. Единствената особеност е в това, че всички аритметични операции в (9) и (12) се изпълняват по законите на крайното алгебрично поле $GF(p^n)$ и могат да се реализират с процесори, използващи аритметика с фиксирана запетая. Това ще бъде пояснено със следния пример.

Пример: Нека *S* е цифров сигнал с дължина $N = 4$, чиито отчети са 4-битови числа

(13) $S = \{s(0) = 0010, s(1) = 1100, s(2) = 0100, s(3) = 0101\}$,

т.е. $S = \{2,12,8,5\}$. Тъй като всички отчети на *S* са по-малки от простото число 17 и освен това дължината на сигнала е точен делител на $17^1 - 1 = 16$, възможно е ТЧС на *S* да бъде изчислен в крайното алгебрично поле $GF(17)$.

Тук следва да се отбележи, че $GF(17)$ е частен случай на така наречените прости крайни алгебрични полета $GF(p)$, чиято аритметика е много проста и се характеризира със следните правила.

1) Елементите на $GF(p)$ са само числата от множеството $P = \{0,1,..., p-1\}$.

2) Събирането и умножението на елементите на $GF(p)$ се изпълнява по модул *p*.

3) Операциите изваждане и деление по модул *p* се изпълняват като се използват така наречените адитивно и мултипликативно обратни елементи. По-конкретно, използва се че

(14) $$a - b = a + (-b);\ a/b = a.b^{-1}.$$

Тук $-b$ е адитивно обратният елемент на b, който се характеризира с равенството $b - b = 0$. Следователно, по модул *p* е изпълнено $-b = p - b \bmod(p)$, тъй като всички числа от вида $\pm p, \pm 2p, \pm 3p, ..., \pm mp, ...$ по модул *p* са 0 (понеже се делят без остатък на *p*).

Аналогично b^{-1} е мултипликативно обратният елемент на b, който се характеризира с равенството $b.b^{-1} = b^{-1}.b = 1 \bmod(p)$.

4) Операциите умножение и деление по модул p се опростяват изключително много от обстоятелството, че във всички крайни алгебрични полета съществуват така наречените примитивни елементи α (само в $GF(2)$ примитивният елемент е точно един $\alpha = 1$). Те се характеризират със свойството, че техните последователни степени

(15) $$\alpha^1, \alpha^2, ..., \alpha^{p-1} \bmod(p)$$

представляват всички ненулеви елементи на крайното алгебрично поле, макар и в някакъв разбъркан ред. Така например в разглеждания случай $GF(17)$ най-малкият по абсолютна стойност примитивен елемент е $\alpha = 3$ и

(16) $$\begin{aligned} &\alpha = 3^1 = 3, 3^2 = 9, 3^3 = 10, 3^4 = 13, 3^5 = 5, 3^6 = 15, 3^7 = 11, 3^8 = 16 \bmod(17) \\ &3^9 = 14, 3^{10} = 8, 3^{11} = 7, 3^{12} = 4, 3^{13} = 12, 3^{14} = 2, 3^{15} = 6, 3^{16} = 1 \bmod(17) \end{aligned}.$$

Освен това, съгласно така наречената *теорема на Ферма-Ойлер* [1, 2, 3], винаги е изпълнено $\beta^{p-1} \equiv 1 \bmod(p)$ за всеки ненулев елемент β на $GF(p)$. Ето защо, ако трябва да се умножат или разделят два елемента на $GF(17)$, например $a = 9$ и $b = 12$, просто трябва да се отчете, че $a = 9 \equiv 3^2 \bmod(17)$, $b = 12 \equiv 3^{13} \bmod(17)$. Следователно

(17) $$\begin{aligned} &a.b = 9.12 \equiv 3^2.3^{13} \equiv 3^{15} \equiv 6 \bmod(17), \\ &a/b = 9.12^{-1} \equiv 3^2.3^{-13} \equiv 1.3^2.3^{-13} \equiv 3^{16}.3^2.3^{-13} \equiv 3^5 \equiv 5 \bmod(17) \end{aligned}$$

След този кратък анализ на аритметиката на крайните прости алгебрични полета вече не е трудно да се изчисли ТЧС на сигнала (6) в $GF(17)$. При това следва да се отчете, че елементът β в (9) и (12) може да бъде някой от елементите $3^4 = 13$, $3^{12} = 4 \bmod(17)$, които са от ред 4 (т.е. $13^4 \equiv 4^4 \equiv 1 \bmod(17)$) и отговарят на условието (10).

Без загуба на общност може да се приеме $\beta = 13$, при което е изпълнено

(18) $\beta \equiv 3^4 \equiv 13, 13^2 \equiv 3^8 \equiv 16, 13^3 \equiv 3^{12} \equiv 4, 13^0 \equiv 13^4 \equiv 3^{16} \equiv 1 \bmod(17)$.

Сега вече не е трудно да се изчисли ТЧС на сигнала (8) чрез (9):

$$A_F(0)=\sum_{i=0}^{3}s(i).\beta^{0.i}=2.13^{0.0}+12.13^{0.1}+8.13^{0.2}+5.13^{0.3}\equiv$$
$$\equiv 2.1+12.1+8.1+5.1=27\equiv 10 \bmod(17),$$
$$A_F(1)=\sum_{i=0}^{3}s(i).\beta^{1.i}=2.13^{1.0}+12.13^{1.1}+8.13^{1.2}+5.13^{1.3}\equiv$$
$$\equiv 2.1+12.13+8.16+5.4=306\equiv 0 \bmod(17),$$
$$A_F(2)=\sum_{i=0}^{3}s(i).\beta^{2.i}=2.13^{2.0}+12.13^{2.1}+8.13^{2.2}+5.13^{2.3}\equiv$$
$$\equiv 2.1+12.16+8.1+5.16=282\equiv 10 \bmod(17),$$
$$A_F(3)=\sum_{i=0}^{3}s(i).\beta^{1.i}=2.13^{3.0}+12.13^{3.1}+8.13^{3.2}+5.13^{3.3}\equiv$$
$$\equiv 2.1+12.4+8.16+5.13=243\equiv 5 \bmod(17).$$
(19)

Следователно, ТЧС на сигнала (8) е

$$A_F=\{10,0,10,5)\}.$$
(20)

Коректността на (20) ще бъде демонстрирана чрез обратното ТЧС, дефинирано с (12). При това $\beta^{-1}=4 \bmod(17)$, тъй като $1\equiv\beta.\beta^{-1}=4.13=52\equiv 1 \bmod(17)$. Следователно

$$s(0)=\frac{1}{N}\sum_{k=0}^{N-1}A_F(k).\beta^{-0i}=\frac{1}{4}\left(10.4^{0.0}+0.4^{0.1}+10.4^{0.2}+5.4^{0.3}\right)\equiv$$
$$\equiv 13\left(10.1+0.1+10.1+5.1\right)=13.25=325\equiv 2 \bmod(17),$$
$$s(1)=\frac{1}{N}\sum_{k=0}^{N-1}A_F(k).\beta^{-1i}=\frac{1}{4}\left(10.4^{1.0}+0.4^{1.1}+10.4^{1.2}+5.4^{1.3}\right)\equiv$$
$$\equiv 13\left(10.1+0.4+10.16+5.13\right)=13.235=3055\equiv 12 \bmod(17),$$
$$s(2)=\frac{1}{N}\sum_{k=0}^{N-1}A_F(k).\beta^{-2i}=\frac{1}{4}\left(10.4^{2.0}+0.4^{2.1}+10.4^{2.2}+5.4^{2.3}\right)\equiv$$
$$\equiv 13\left(10.1+0.16+10.1+5.16\right)=13.100=1300\equiv 8 \bmod(17),$$
$$s(3)=\frac{1}{N}\sum_{k=0}^{N-1}A_F(k).\beta^{-3i}=\frac{1}{4}\left(10.4^{3.0}+0.4^{3.1}+10.4^{3.2}+5.4^{3.3}\right)\equiv$$
$$\equiv 13\left(10.1+0.13+10.16+5.4\right)=13.190=2470\equiv 5 \bmod(17).$$
(21)

Тези резултати съвпадат с (8) и потвърждават факта, че ТЧП имат абсолютно същите свойства, както ДПФ. По тази причина те могат да се използват вместо ДПФ практически във всички случаи на спектрална цифрова обработка на сигнали.

Следва специално да се отбележи, че простите числа на *Мерсен* и *Ферма* позволяват теоретико – числовите спектрални методи да се реализират много просто, тъй като за тях числото $q=p^n-1$ покрива целия динамичен диапазон от стойнос-

ти на отчетите на сигналите, използвани от малоразмерни сензори и дронове. Действително, простите числа на Мерсен имат вида

(22) $$p = 2^{p_1} - 1,$$

като тук p_1 също е просто число. В интервала $[1, 10000]$ простите числа на Мерсен са:

(23) $3 = 2^2 - 1,\ 7 = 2^3 - 1,\ 31 = 2^5 - 1,\ 127 = 2^7 - 1,\ 8191 = 2^{13} - 1$.

Простите числа на Ферма имат вида

(24) $$p = 2^{2^k} + 1.$$

В интервала $[1, 10000]$ простите числа на Ферма са:

(25) $$3 = 2^{2^0} + 1,\ 5 = 2^{2^1} + 1,\ 17 = 2^{2^2} + 1,\ 257 = 2^{2^4} + 1.$$

Заключение

В доклада са анализирани особеностите на теоретико – числовите спектрални методи за цифрова обработка на сигналите. В резултат е обоснована възможността за реализиране на сложни алгоритми за цифрова обработка на сигнали с евтини и надеждни процесори с малка консумация на енергия, използващи целочислена аритметика. Тази възможност има голямо значение за съвременните интелигентни сензорни мрежи, изградени от малоразмерни сензори и дронове.

Литература:

1. Р. Блейхут, Быстрые алгоритмы цифровой обработки сигналов, Мир, Москва, 1989, 448 с.
2. И. В. Вариченко, Г. В. Лабунец и М. А. Раков, Абстрактные алгебраические системы и цифровая обработка сигналов, Наукова думка, Киев, 1986, 248с.
3. S. Golomb and G. Gong, “Signal design for good correlation,” Cambridge University Press – 2005
4. H. Menouar, I. Güvenc, K. Akkaya, A. Selcuk Uluagac, A. Kadri, and A. Tuncer, “UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges,” *IEEE Communications Magazine*, vol. 55, No 3, March 2017, pp. 22-28
5. Ts. S. Tsankov, T. S. Trifonov, and L. A. Staneva, “A survey of phase manipulated signals with high structural complexity and small loses after processing with mismatched filters,” *Journal Scientific and applied research*, ISSN 1314-6289, vol. 4, pp. 88-97, 2013.
6. Ts. S. Tsankov, T. S. Trifonov, and L. A. Staneva, “An algorithm for synthesis of phase manipulated signals with high structural complexity,” *Journal Scientific and applied research*, ISSN 1314-6289, vol. 4, pp. 80-87, 2013.
7. D. Velikova, V. A. Mutkov, and B. B. Bedzhev, “Analysis of the conditions for synthesis of efficient side-lobes suppression filters for binary phase manipulated signals,” *Journal Scientific and applied research*, ISSN 1314-6289, vol. 6, pp. 106-113, 2014.

МНОГОСЛОЕН МОДЕЛ ЗА КИБЕР СИГУРНОСТ НА КРИТИЧНА ИНФОРМАЦИОННА ИНФРАСТРУКТУРА

Лъчезар Т. Петров[1], Николай Т. Стоянов[2]

[1] *Министерство на отбраната на Република България, София 1092, ул. "Дякон Игнатий" № 3, Дирекция КИС, Отдел Политики и планиране развитието на КИС, София, България*
l.t.petrov@mod.bg
[2] *Институт по отбрана, София 1592, бул. „Професор Цветан Лазаров“ № 2*
n.stoianov@di.mod.bg

MULTILAYER CYBERSECURITY CRITICAL INFORMATION INFRASTRUCTURE MODEL

Lachezar T. Petrov[1], Nikolai T. Stoianov[2]

[1] *Ministry of Defence of the Republic of Bulgaria, CIS Directorate, Policy and CIS Development Planning Branch, 3 Dyakon Ignatiy Str., 1092 Sofia, Bulgaria*
l.t.petrov@mod.bg
[2] *Bulgarian Defence Institute, 2 Prof. Tsvetan Lazarov Blvd, 1592, Sofia, Bulgaria*
n.stoianov@di.mod.bg

Abstract: *National and international security, our national well-being are dependent on critical information infrastructures, which could be described as highly interdependent. Keeping them in reliable and secure state and study their dependencies is paramount for every government or organization. Creation and development of multilayer cybersecurity critical information infrastructure model is going to make this world safer. The described here model is a step toward reliable and secure critical information infrastructure.*

Keywords: cybersecurity, critical information infrastructure, multilayer model.

Отношенията в много голяма част от сферите на живота в съвремието се базират на сложна система от взаимно допълващи се, а често и взаимно изключващи се мрежови връзки, които организират контакти към множество системни интерфейси. Така реализацията на всеки продукт или решаването на всяка задача става зависимо от голям, сложен, но относително логичен механизъм, базиран на изградена инфраструктура и обслужван от комуникационни и информационни мрежи и системи от различен клас. Подобен сложен механизъм позволява на организациите (държавни, частни комерсиални и не правителствени) да обслужват своите интереси и да постигат своите цели. Така понятието “Сигурност” и особено възможността за постигането на кибер сигурност налагат намирането на подход, различен от общоприетите до сега.

За да дефинираме обхвата на това, което искаме да постигнем с настоящата публикация, е необходимо да бъдат определени някой от определенията, с които ще боравим. По мое мнение все още няма всеобхватно и общоприето определение на понятието “Критична информационна инфраструктура”. Този факт е само илюс-

трация за значимостта на критичната информационна инфраструктура и интересите, които я съпътстват.

Много изследователи в различни сфери са дефинирали понятието "Критична информационна инфраструктура". За целите на настоящата публикация ще се придържаме към едно, синтезирано от различни източници определение:

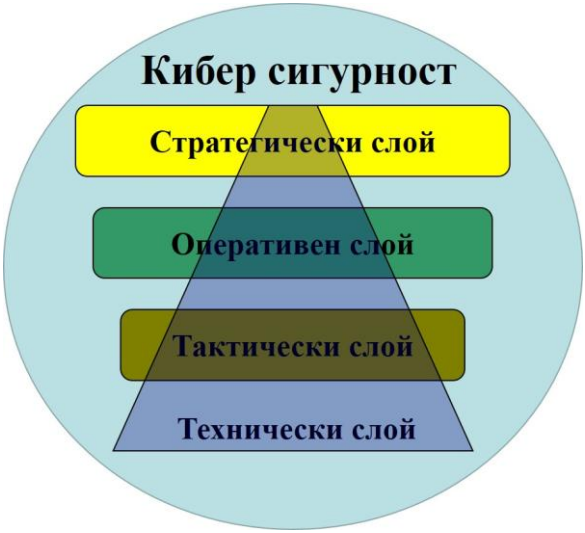
Критична информационна инфраструктура е система от съоръжения, услуги, правила, документи, методики за управление, както и начини обработка и разпространение на информация, чието спиране или неизправно функциониране поради каквато и да е причина, би имало сериозно негативно въздействие върху здравето и безопасността на хората и околната среда. Това би довело също до сериозни финансови и материални загуби и би нарушило ефективното функциониране на държавното и военно управление в даден район или държава.

В съвременния свят е ясна тенденцията за промяна на центъра на тежестта на заплахите от физическо или т.н. кинетично въздействие, към индиректно, неконвенционално въздействие върху критични елементи на информационната инфраструктурата на вероятния „противник". Това довежда и до факта, че подходите за въздействие като тероризъм и кибервойна, често са обединявани под едно общо наименование „хибридна война". Такъв подход няма за основна цел „унищожаване" на противникова критична информационна инфраструктура а цели да наруши нейната работа и да предизвика криза за дебалансирането и. Така, по–късно, излязла от строя критична информационна инфраструктура лесно може да се възстанови и управлява. [1]

За съжаление, в нашето съвремие, заплахата за нарушаване на работата на критична информационна инфраструктура е станала напълно възможна, много достъпна, както във финансово, така и в техническо отношение, а същото време е в състояние да причини значими щети на нормалното функциониране на обществото. Научно и имперично е доказано, че кибер сигурността на такива инфраструктури е възможна само, когато се работи в синергия от всички заинтересовани, следвайки определен модел и спазвайки определена последователност, която ще се опитам да дам по-долу:

- идентификация на заплахата/атаката;
- адекватна реакция на заплахата/атаката;
- управлението на кризи, възникнали следствие на атака върху критична информационна инфраструктура;
- управление на възникналите щети;
- връщане на критичната информационна инфраструктура към нормалната и функция. [2]

Обществото е особено чувствително към заплахи за националната сигурност, а в голяма степен подобни заплахи са насочени към критичната информационна инфраструктура на всяка страна. В областта на сигурността е приета практиката, дискусията за кибер сигурност да се разделя на тактически, оперативни и стратегически нива или слоеве. Към така дефинираните нива/слоеве за кибер сигурност, е необходимо да се добави и един чисто технически слой, като този слой се фокусира върху компютъризирана система на организация и системите за пренос на информация, които най-често съставляват информационната инфраструктура, независимо от степента на нейната важност.



Фигура 1

Многослоен модел за кибер сигурност на критична информационна инфраструктура

Няма никакво съмнение, че всяко от тези нива/слоеве трябва да противопоставят на всяка заплаха/атака. Всеки един от тях обаче има различен фокус върху сигурността, и затова, предложеното разделение ще помогне за идентифицирането на същността на предизвикателствата на кибер защита на критичната информационна инфраструктура.

Технически слой за кибер сигурност

Заплахата в техническия слой произлиза от свойствата на комуникационните и компютърни технологии. Проблемът с кибер заплахата в този слой е технически проблем и поради тази причина трябва да се търси техническо решение.

В техническия слой е необходимо да се изгради гъвкавост на инфраструктурата, което да и позволи, дори и подложена на атака да продължи да изпълнява предназначението си, оставайки в задоволителни параметри. Комуникационната част се изгражда така, че да сме в състояние да реализираме обходи, което намалява значително необходимото време за възстановяване, което в техническия слой следва да е изключително минимално. Критични информационни системи се дублират и работят в паралел отново, за да се намали времето за възстановяване.

Техническия слой преминава през и поддържа всички останали, споменати по-горе слоеве, но той е заема различна част от останалите.

Тактически слой за кибер сигурност

Тактическия слой в най-голяма степен зависи от техническия. Обмена на информация в този слой е до голяма степен интензивна, но обема на съобщенията в доста голяма степен е малък. Друга характерна особеност на тактическия слой, е сравнително краткия живот на съобщението. В голямата си част, това са съобщения

за статус и текущи състояния на системите. Като правило на тактическите нива контролираните системи са динамични и това води до краткия живот на обменяните съобщения. Кибер отбраната в този слой е почти изцяло зависима от кибер отбраната, организирана в техническия слой. Съответно, както и в техническия слой, изискването към необходимото време за възстановяване е то да бъде изключително малко. В противен случай, поради краткия живот на информацията, която слоя обменя и поддържа, риска от загуба на информация и потенциално дисбалансиране на инфраструктурата е значителен.

Оперативен слой за кибер сигурност

Най-натоварен с очаквания по отношение на кибер сигурността е слоя, който сме определили като оперативен. Техническия слой и инженерните решение за сигурност имат доста по-малко влияние тук. В оперативния слой живота на обменяната и обработвана информация е значително по-дълъг. Обикновено в оперативния слой се обменя и обработва информация, свързана с динамиката на процесите в слоя от тази част на критичната информационна инфраструктура. Това в много случаи изисква обработка и обмен на сравнително големи обеми от информация. В перативния слой влиянието на техническия слой е по-малко, като тук са необходими не само технически решения, за да се осигури кибер сигурност. Работата на оперативния слой има необходимост от разработване и прилагане на политики и изисквания при обработката и обмена на информация в процеса на управление. Политиките и изискванията трябва да бъдат съгласувани и приети между всички участници на това ниво. Таблица 1 показва едни обобщени примерни проблеми на кибер отбрана в този слой.

Таблица 1

Потенциални уязвимости	**Възможни реакции**
Паролите за достъп в комуникационните и информационни системи не са променят переодично.	Разработване на политика за управление на паролите
Паролите за достъп в комуникационните и информационни системи са изпратени на други на потребителите в явен вид.	
Недостатъчна физическа сигурност на елементите от критичната информационна инфраструктура	Разработване на процедури за физическа сигурност
Потребители, оператори и администратори, които не работят с и не управляват или администрират критично комуникационно или информационно оборудване имат достъп до него.	
Неудачен мениджмънт на потребителски разрешения за ниво на достъп, дава достъп на служители с нисък ранг до изключително важен	Разработване на процедури за сигурност при достъп до комуникационни и информационни устройства.

Потенциални уязвимости	Възможни реакции
процес.	
Неправилно конфигурирана защитна стена позволява ненужна комуникация.	
Мрежа за управление не е отделена от офис мрежа.	
Оставена е отворена възможност за отдалечен или безжичен достъп до комуникационна или информационна система.	
Процес с възможност за отдалечен достъп, използва отворен протокол или не е защитен с парола.	
Упгрейт по сигурността не е инсталиран на системите	Конфигурационен мениджмънт
Дадени са администраторски права на нормален потребител.	
Достъпът до критични системни компоненти не е бил записан (липса на информационен /log/ запис).	
Информационния /Log/ запис не се проверява редовно.	

Таблица 1 - обобщени примерни проблеми на кибер отбрана в оперативния слой [1]

За осигуряване на кибер сигурност в оперативния слой е необходимо разработването на процедури и документи, както и подготовката на специалисти, запознати с изискванията към слоя. Във връзка с това, че освен чисто технически способи за кибер защита, в слоя има и прилагане на различни политики и процедури, които не са свързани с инженерни решения, необходимото време за възстановяване може да бъде по-дълго.

Стратегически слой за кибер сигурност

В стратегическия слой/ниво заплахата/атаката на критичните информационни инфраструктури се разглежда в рамките на националната сигурност и това излиза извън границите на една организация, бизнес процес или управление на система. В този стратегически слой се гледа на кибер защитата като част от защитата на обществото като цяло.

При организацията на кибер отбраната в стратегическия слой, техническия слой има най-малко влияние. Обменената и обработена информацията на това ниво дава крайни състояние и анализи за развитие на процесите на управление. На това ниво живота на обработваната информация е дълъг и е валиден за вземане на управленчески решения. Както и в армията, стратегическия слой се нуждае от подходящ оперативен, тактически и технически слоеве, но дори това не е достатъчно за постигане на стратегическата цел. В най-сложния слой, е необходима цялостна политика за защита на критичната информационна инфраструктура, която в допълнение към оперативния, тактическия и техническия слой ще вземе предвид поли-

тическите, икономическите и организационните аспекти на кибер отбраната. На такова ниво кибер отбраната изисква взаимнообвързани организационни дейности, подкрепени от ефективен орган за управление и контрол на процесите. Това е сложно предизвикателство за кибер защитата на всяка критична информационна инфраструктура. На такова ниво става ясна необходимостта от отбрана киберпространството като цяло, специфичните характеристики на някой от елементите, което прави задачата още по-трудна.

Заключение

Кибер сигурността на критичната информационна инфраструктура е не само технологичен проблем. Кибер сигурността на критичната информационна инфраструктура влияе върху икономическото благосъстояние и е в пряка връзка с националната и обществена сигурност, от което следва, че кибер сигурността на критичната информационна инфраструктура е политически проблем, бизнес проблем и проблем на индивида. Науката и технология разработват различни модели за осигуряването и.

Работата по многослойния модел за кибер сигурност на критична информационна инфраструктура не е самоцел, а ще даде възможност на съответните мениджъри да определят своите приоритети, както и средствата и механизмите за постигане на целите си. Това е стъпка за създаване на интегрирана система за сигурност и защита на цялата критична информационна инфраструктура.

References

1. Lieutenant Colonel Echevarria II, Antulio: Clausewitz's center of gravity, It's not what we thought. Naval War College Review, Winter 2003, Vol. LVI, No. 1
2. ENISA, Europa: https://resilience.enisa.europa.eu/enisas-ncss- project/CIIPApproaches NCSS.pdf, Critical Information Infrastructures Protection approaches in EU, Final Document, Version 1, TLP: Green, July 2015
3. Lior Tabansky, Critical Infrastructure Protection against Cyber Threats, Military and Strategic Affairs / Volume 3 / No 2 / November 2011

CYBER THREATS IN LOGISTICS - AN OUTLINE OF THE PROBLEM

Monika Szyłkowska, PhD

***Military University of Technology**, Warsaw, Poland*
Faculty of Logistics, Department of Security And Defence
monika.szylkowska@wat.edu.pl

Abstract: *The article presents selected considerations in the area related to cyber threats - general classification and challenges that imply in the logistics. Indicated selected examples, illustrating the scale of the potential risks in this sphere and identified loopholes in this area. In addition, it presents new concepts implied by cyberspace - liability for the software.*

Keywords: *cyberspace, digital threats, liability for the software.*

Today's dynamic, global and digital world is generating new opportunities, challenges, risks and threats in every aspect. Technical and technological revolution has become a determinant of the level of development and growth in countries. Currently, not only all aspects of life and functioning of individuals, businesses, organizations and structures of states, but also international alliances are an inseparable aspect of cyberspace, therefore they are - to a lesser or greater degree - dependent and interrelated to it.

The ICT sector (Information and Communication Technologies) is an integrated system consisting of parts such as hardware, software and IT services. The use of modern systems improves and supports numerous complex tasks and processes in the scope of logistics (e.g. inventory management, supply planning, customer service, etc.). The use and implementation of modern solutions is nowadays a sine qua non condition for the functioning, ensuring a competitiveness of a company. In the age of globalization, the logistics market is also subject to a dynamic development- on the one hand, adapting to occurring changes, on the other, however- aiming at surpassing and then responding to the needs and expectations of customers. Proficient and, most importantly, efficient and optimal cooperation of all chain links in the scope of logistics is possible due to modern systems processing the data and information. The role and importance of information in the modern world does not in fact require any justification as it is the most valuable resource in all areas and fields - in terms of economics, *the information management, its quality and the flow rate are a key factor for competitiveness*.

It seems interesting that - as a principle - **the concept of information** itself is **non-definable**[1], although it "accompanies man and his activity since the dawn of time". However, regardless of the chosen definition, the information has some characteristics among which of the utmost importance are: relevance, accuracy, topicality, completeness, coherence, quality, credibility and security.

[1] Source: www.encyklopedia.pwn.pl. Access: 21.03.2017 r.

General classification and challenges that imply in the logistics

The importance of information and potential risks to it are determined by the place of its functioning, i.e. mainly telecommunications systems - those imply different types of digital threats. The "new generation" crime is the result of civilization development and the IT revolution, therefore being an extremely dynamic subject and thus being subject to constant changes.

Cyberspace is most often defined as the communication space in which digitized information operates. Said information is generated, processed, archived and transmitted in such space. Cyberspace is an area that leads, on one hand, to development, and on the other hand, it generates threats such as cybercrime, **[1]**. These threats are closely related to the economic area, as those are enterprises that often are the victims of digital attacks (especially frauds or ransom demands).

Considering the fact that information and information and communication technology (ICT) are currently crucial in broadly defined terms of logistics, being an important component in the process of achieving a competitive advantage by individual entities, with companies in the field of logistics being one of the most innovative entities in the scope of ICT - potential digital threats may not only be crucial to the basics of their functioning, but also to economic processes. Within existing solutions, one may encounter both typical ones (used in various industries) and solutions that are strictly specialized, dedicated to specific sectors. The main groups of logistics support systems include: ones that support the cooperation between entities, ones supporting functioning of an entity, and solutions that provide with the means to track and monitor consignments and vehicles, iCargo, e-Fraght, etc.

Regardless of the area, domain, or level of advance of the tools and technologies used, the dangers of digitized information remain a common issue. In the Communication from the Commission to the European Parliament, the Council and the Committee of the Regions COM (2007) 267 [2] on the general strategy for combating cybercrime, three basic types of cybercrime have been classified: 1. Traditional forms; 2. Publication of illegal content in electronic media and 3. "typical" crimes within the network. Traditional forms include fraud and counterfeiting - but with the use of electronic computer networks and information systems (an example of which are mass scams, identity theft, and phishing). The second group includes in particular websites containing illegal content (e.g. racial hatred, incitement to terrorist acts, etc.). Crimes "typical" to the network include hacking attacks, cyber-attacks, DDoS attacks.

Cybercrime in its broad scope can be used to define an action resulting in negative effects caused in the space of processing and information exchange, created by ICT systems. Therefore, it would be considered an act in a digital environment that intend to or could potentially disrupt, neutralize or stop the operation of ICT systems, resulting both from the act and the neglect of the human (user).

Given above, the main groups of cyber threats include:

a.) ones resulting from human activities:

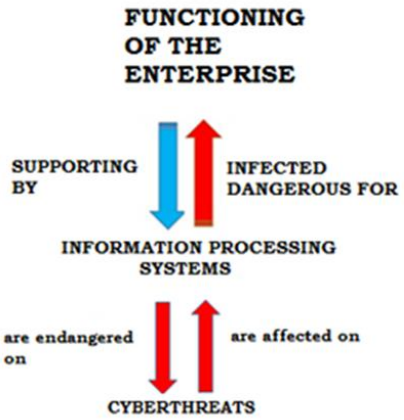
- intentional (virtual and real cybercriminals, an example of which is theft or damage caused to equipment),
- unintentional [untrained, unaware or unconcerned staff],

b.) ones resulting from the natural environment [such as natural disaster resulting in lack of power],

c.) ones not related to intentional human activities [failure of systems, software failures, power supply failures];

d.) mixed/hybrid.

The following illustration presents the potential impact of cyber threats on the functioning of an entity:



The primary threats to information for each entity include in particular:

- lack of information,
- lack of proper information (at the right time, place, to the right recipient).
- wrong, imprecise or false information (overstated costs, underestimated costs, etc.)

but also:

- stealing information (on market competition: particularly new product, new strategy, etc.)
- destroying or modifying information.

It shall be emphasized that unprotected or vulnerable systems might trigger any form of abovementioned examples of threats. Losses due to the lack of possibility of processing of information or the lack of information flow increase total costs, including downtime, necessary repairs and restorations, but also future losses of profits due to e.g. the lack of customer base (and their sales on the black market) as well as they exceed security costs. However, the major and incalculable loss for any entity is the loss of the reputation.

Selected examples, illustrating the scale of the potential risks

Given the variety of types and natures of threats- for objective reasons - only selected ones will be discussed in the article.

According to Kaspersky Lab report in 2016:

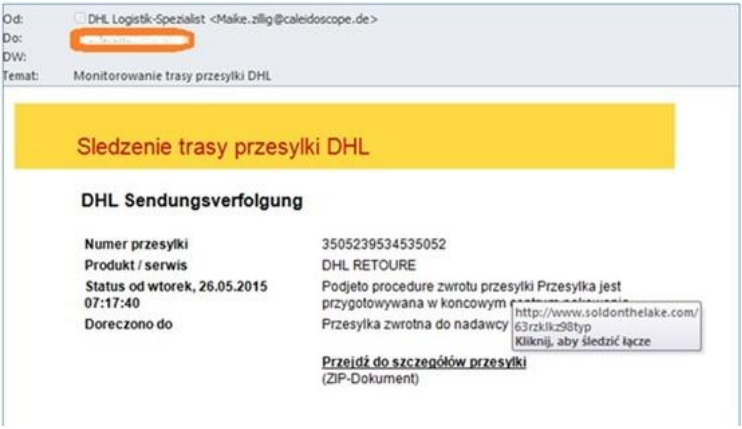
- 49% of the surveyed companies had experienced a targeted attack,
- 50% experienced a ransomware attack (a software that blocks an access to data and demands a ransom), in 20% of cases data were blocked).

- 48% of respondents encountered a security breach incident due to the unconcerned staff. Digital counterfeits are a first example of such, they may be divided into following subcategories [3]:

a. conducted with the use of malicious software,
b. performed with fake messages (e-mails);
c. hybrid (false emails containing malicious software or links to such programs).

The following illustration depicts a fake e-mail containing information about the alleged consignment:

Fig. 1. The content of the fake message containing information about the alleged consignment.



Source: https://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci. Access: 21.03.2017 r.

What is more, the attachment to the message (so called file extension, e.g. .doc, .docx, .pdf) is supposed to suggest a text document that in fact contains a malicious program and is intended to mislead the user to open the file.

Hybrid crime: fraud and deceit that may be classified as a phishing attack (due to its methods of operating: misleading an user and forcing them to perform certain actions) - is a particular type of criminal activity that involves scamming, with money being sent to a fake bank account. The act consists in faking a message that contains information on the change of an existing business' financial account to a new one, which should be used in order to transfer finances. Commonly, the information is contained in a file that presents all personal data of the entity, including the signature of the authorized person (e.g. the chairman). Attention shall also be drawn to the ease with which the entities freely share legal files and documents on their websites, e.g. references without any security measures (for example watermarks), or even without blurring the stamps. Recently, the victims of this type of crime were one of the branches of Province Roads Authority, where a financial department employee transferred 3.7 million pln to a fake bank account. In this case, the malware was not used to commit the crime- the employee believed a false document.

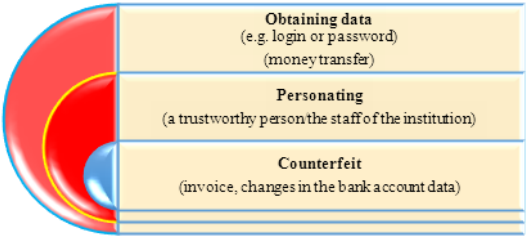
An example of malware counterfeiting is the American Mega Metals Company: criminals have infected a computer of the broker working for the company and sent a message to the entity, concerning the change in the supplier's account number. The credibility of messages received from the real e-mail address relating to real orders has caused the recipient to transfer funds to the designated bank account. The fraud was only discovered when a real supplier sent a notice of unpaid invoices for a total of 100,000$.

Another example are ransomware attacks. Ransomware is a type of malware that encrypts data on an infected computer or blocks an access to it, including the message with instructions that is displayed on the screen- the ransom should be paid in order to recover data or an access to them. According to research conducted by Kaspersky Lab in 2016, the frequency of attacks on entities using this type of software has increased three times, that is one every 40 seconds (1 in 5 companies) [4].

Following illustration presents an example of a result of a ransomware attack:

Source: hongkiat.com.Access: 21.03.2017.

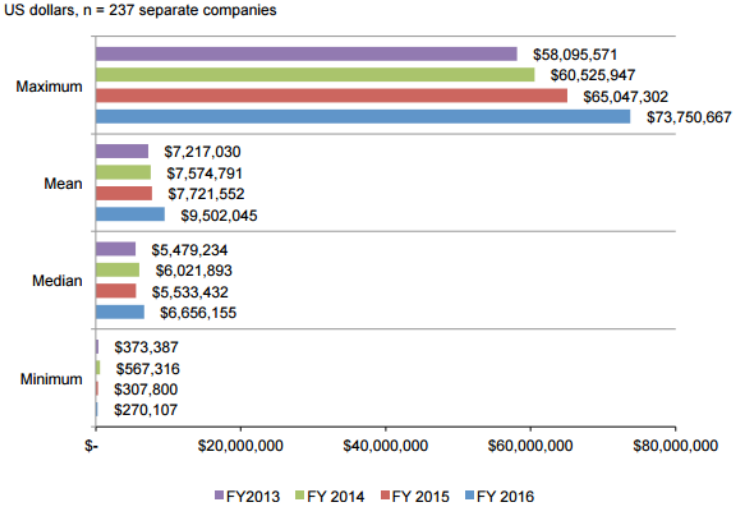
To sum up abovementioned examples, it might be observed that their common denominator is the fact that cybercriminals use both the ignorance and/or the unawareness of IT users. Given that, it is the most common reason of surpassing the protection against all forms of technical attack while searching for the weakest point of the security system, that is the human [5].



Indicated methods:

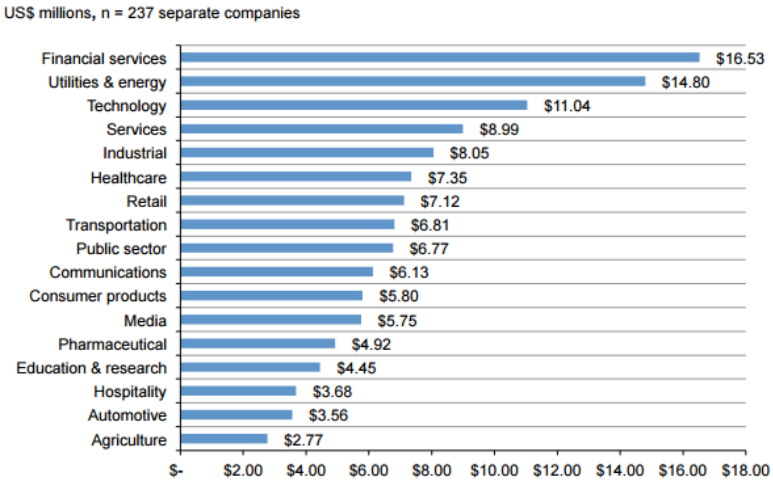
HP Company has presented the results of its annual survey, which indicates that in the course of past three years the frequency of cyberattacks has more than doubled and resulting from them financial losses have increased by nearly 40 percent.

In broadly defined logistics, a primary and fundamental part are business entities that constitute individual links in the chain. This is the cause of the fact that each entity to some extent depends on the other (customer from the supplier, etc.), therefore each materialization of cyber threats will affect the others. As indicated by research conducted by the Ponemon Institute on behalf of Hewlett Packard Enterprise, currently the information theft continues to be the cause of the largest losses (44% of total external costs incurred as a result of cybercrimes); disruptions of the functioning of an entity, or reduced productivity stand for as much as 30 percent of external costs.



Source:http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf. Access:21.03.2017.

It has been indicated that the costs of cybercrime affect all sectors of the economy, as illustrated in the chart below:

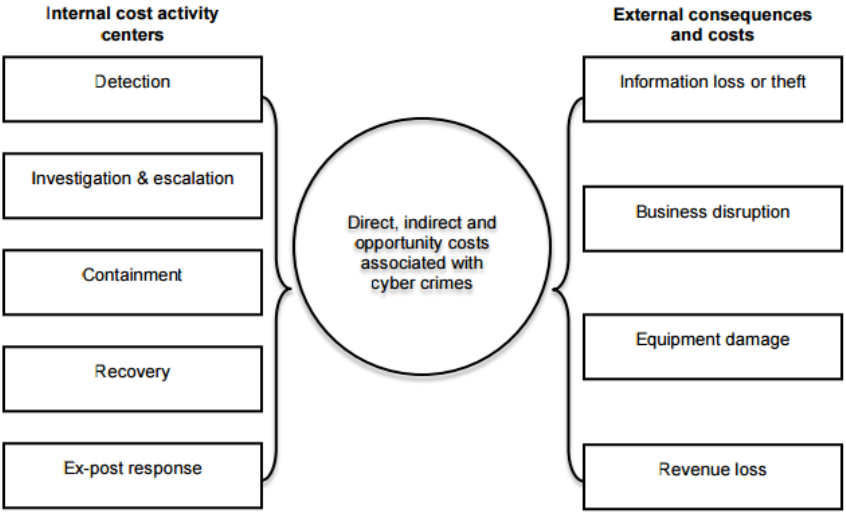


Source:http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf Access:21.03.2017.

Within the same research, the most common types of cyberattacks included:

Source: based on 2016 Cost of Cyber Crime Study & the Risk of Business Innovation, Ponemon Institute© Research Report, Oct.2016. http://www.ponemon.org

It seems profitable to draw the attention to cost frameworks that are a result of a cybercrime for every company:



Source:http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf Access:21.03.2017.

New concepts implied by cyberspace - liability for the software

In the era of supremacy of the widespread use of modern technologies, the crucial challenge is the protection not only of devices and their content alone, but also a software that manages, controls, or supports their functioning. Already existing models for information security management and ICT systems have dedicated, developed solutions in this scope - a classic example is provided by ISO 27001 standard - Information Security Management System. However, an area that continues to be a primary challenge, especially given the legal aspects, is a broadly defined software. Currently, vulnerabilities and lacks within a software indicate the potential for infection and attack conducted on systems, however- apart from software licenses - there is no real responsibility of the manufacturer for its security. It could be assumed that updates constitute a type of performance of the manufacturer's responsibility for the product, but it is well known that the gap-elimination mechanism is based primarily on time-sensitive applications. Given that, it is also the user that is obliged to update (if updates are available), often in a manual manner (non-automatic one), which does not guarantee the prevention of a malware. Another aspect in this respect is illustrated by an example of an attack on Adobe servers that has stolen 40 gigabytes of the source code - including the very popular Adobe Reader code and the ColdFusion framework. A result of such theft may be the identification of errors that attackers might use to conduct an attack on virtually every computer in the world. What is more, there occurs a risk of modifying the source code and appending to it the so called backdoor, which can then be downloaded as an "update". The manufacturer's statement indicated that after having verified the product code, there was no observed violation of its integrity, however, the sole fact of intrusion reveals the scale of the threat, as well as the lack of adequate security provided to the users.

Summary

To sum up discussed matters within the presented subject, it shall be emphasized that regardless of the classification and categorization of digital threats they have a common denominator, that is their mass and unlimited reach. Given that information is of both a strategic value and an essential part of business processes, it seems essential to draw the attention to the fact that new challenges for logistics in the broadly defined digital areas arise in regards with information (its role, importance and meaning in every process) and with the aggregation and use of information resources, as well as with actions undertaken by entities on strategic and operational levels. Selected and presented examples of cyber threats clearly illustrate the scale and variety of potential dangers - from theft of information and databases [of customers, contractors] through forced ransom and false bank accounts, to the possibility of destabilization of functioning. Investing in own - particularly digital - security is not an activity after which one should expect a return on the investment, but it rather should ensure the possibility for stable and uninterrupted functioning, providing with the basis for profitability and competitive advantage. Of a significance is also the fact of combining technology and creating links between information systems- which, as a result, increases the vulnerability to attacks in cyberspace. This stems from both the very essence of the network, and factors such as: compatibility of remote systems, the availability of inexpensive devices and software, the adoption of hardware and software standards, and the access to means for conducting illegal activities. Business entities that operate without any *support* in the form of information superstructures, the use of automatic identification of commodity flows, or electronic data exchange have virtually no chance of surviving in an increasingly dynamic and competitive business environment. In the modern world where information is a fundamental component of functioning, **the lack of awareness or, even worse, decision to ignore threats** may lead to the worst scenario, not included in any strategy of any business enterprise- its bankruptcy.

Bibliography:

1. Sienkiewicz P. *Terroryzm w cybernetycznej przestrzeni*. W (eds.) Jemioła T., Kisielnicki J., Rajchel K.: Cyberterroryzm – nowe wyzwania XXI wieku. Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa 2009.

2. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - *Towards a general policy on the fight against cyber crime* {SEC(2007) 641} {SEC(2007) 642} Brussels, 22 May 2007,
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52007DC0267

3. M.Szyłkowska, *Digital extortion and falsification as the key threat to enterprises - supply chain*,
GOSPODARKA MATERIAŁOWA i LOGISTYKA, 5/2016, PWE 2016, 716-727.

4. Kaspersky Security Bulletin 2016, https://kas.pr/R3tY.Access: 21.03.2017.

5. M.Szyłkowska, *Socio-technical attacks as a threat to the functioning of public entities [in origin: Ataki socjotechniczne jako zagrożenie dla funkcjonowania jednostek publicznych* [In the publishing process]

6. Oleński J. *Ekonomika informacji. Podstawy*. PWE Warszawa, 2001.

7. Hołubowicz W., Samp K., *Informacja i informatyka w logistyce*.
www.logistyka.net.pl/.../Kongres2008-w3-ref-A-1.pdf. Access: 21.03.2017 r.

8. Susłow W., *Od organizacji do systemu informatycznego. Modelowanie i analiza systemów informatycznych*; http://moskit.weii.tu.koszalin.pl/~swalover/MiASI_w1.pdf.
9. Graczyk M. *Projektowanie podsystemu wspomagania decyzji w systemie informacyjnym aglomeracji.*
10. Gozdek J., *Hakerzy bez granic*, CHIP 11/2015.
11. Portal internetowy Encyklopedii Polskich Wydawnictw Naukowych: encyklopedia.pwn.pl.
12. Magazine Niebezpiecznik.pl. http://niebezpiecznik.pl

ТЕХНОЛОГИЧЕН МОДЕЛ ЗА КИБЕР СИГУРНОСТ В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ

Милен Ст. Куцакис

Университет по библиотекознание и информационни технологии,
m.kucakis@abv.bg

Николай Т. Стоянов

Институт по отбрана „Професор Цветан Лазаров“,
n.stoianov@di.mod.bg

TECHNOLOGICAL MODEL FOR CYBERSECURITY IN THE PUBLIC ADMINISTRATION

Milen St. Koutsakis

State University of Library Studies and Information Technologies,
m.kucakis@abv.bg

Nikolai T. Stoianov

Defense Institute "Professor Tsvetan Lazarov",
n.stoianov@di.mod.bg

Abstract: *The state administration is part of the mechanism of public control. State Administration provide citizens with a range of services. These services operate thanks to good planning and infrastructure. The services provided by public administrations are secured and constructed using concrete plans and steps from: "National Strategy for Cybersecurity". Transferring these services to the digital world with improper computer and network structure can lead to many vulnerabilities. Securing connection and any technical means is imperative for proper and safe operation of the services.*

Keywords: *Cybersecurity, Cyber Resistant, Malicious software.*

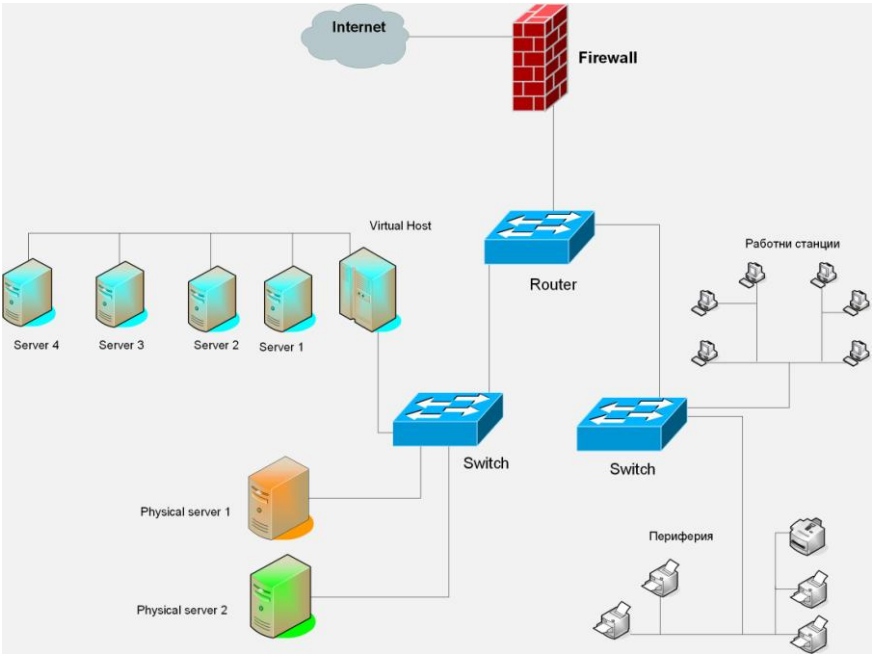
Държавната администрация е част от механизма на общественото управление, извършваща огромния дял от неговата работа. Държавната администрация се представя най-вече като организация, апарат за извършване на определена дейност, предвидена в закона. В тази организация, определяна като държавен административен апарат, влизат всички институции, предвидени по Конституцията на Република България и законите като органи на изпълнителната власт. В апарата на държавната администрация влизат и всички помощни органи и служебни лица, които осигуряват нормалното и непрекъснато функциониране на държавното управление,

а именно: счетоводители, плановици, юрисконсулти, специалисти и експерти от различни направления, включително и специалистите, поддържащи в изправност съоръженията и материално техническата база на административните органи.

Държавната администрация предоставя на гражданите редица услуги. Тези услуги функционират благодарение на добре планирана и изградена инфраструктура. Услугите предоставяне от държавната администрация биват подсигурени и изградени чрез използване на конкретни планове и стъпки от: „Национална стратегия за киберсигурност“, която е част от („Киберустойчива България 2020“). Гражданите и обществото разчитат на достоверна и надеждна информация в интернет пространството. Също така имат нужда от доверие и защита на персоналните данни, на дигиталното „аз“, както и на адекватна защита на човешките права и свободи в кибер пространството. Държавата все повече разчита на интернет като канал за предоставяне на информация и услуги на гражданите и бизнеса, както и за бърз, прозрачен и широк контакт с обществото. Чрез електронното управление тя необратимо пренася дейността си в напълно дигитална среда.

За да предоставя своите услуги нормално държавата се нуждае от подобряване на защитата и устойчивостта на комуникационните и информационни системи. Трябва да се поддържат непрекъснато системите за управление на критичните инфраструктури, за да се гарантира, че основните функции ще бъдат надеждно и безпроблемно осъществявани. С особена важност е нарастването на обвързването на информационните и комуникационните системи със секторите и системите от критичната инфраструктура като: енергетика, транспорт, финанси, здравеопазване, телекомуникации, снабдяване с храни и вода, отбрана и други. Повечето от тези зависещи и основаващи се на специализирани системи услуги, мрежи и инфраструктури, формират жизнено важна част от икономиката и обществото.

Пренасянето в дигиталната среда с неправилно изградена компютърна и мрежова структура може да доведе до много проблеми в различни точки. Подсигуряването на всяка една връзка, всяко едно техническо средство е наложителна за правилно и безопасно функциониране на предоставяните услуги. На фигура 1 е показана примерна схема на вътрешната инфраструктура на звено от държавната администрация:



Фигура: 1.

Фигура 1 визуализира мрежовите устройства, защитните стени, сървърите, работните станции и мрежовата свързаност на системата. Всяко едно устройство има ключово значение за надеждната работа на системата. И също така, всяко едно от тези устройства е потенциална точка на пробив на системата. Това може да се случи както физически (хардуерно), така и софтуерно, чрез злонамерен код или други.

- Физически (хардуерни) атаки

Този тип атаки са по-слабо осъществими, тъй като за тяхното изпълнение злосторникът трябва да има физически достъп до цялостната част от инфраструктурата. При спазване на правилата за контрол на достъп, достъпът на неоторизирани лица е практически невъзможен. Също така за осъществяването на такава атака злосторникът трябва да има познания за необходимите акаунти и парола за достъп до някое от устройствата. Всичко това прави изпълнението на такъв вид атака трудно изпълним. Най-често такъв вид атака се случват от служители със съответното ниво на достъп до системата.

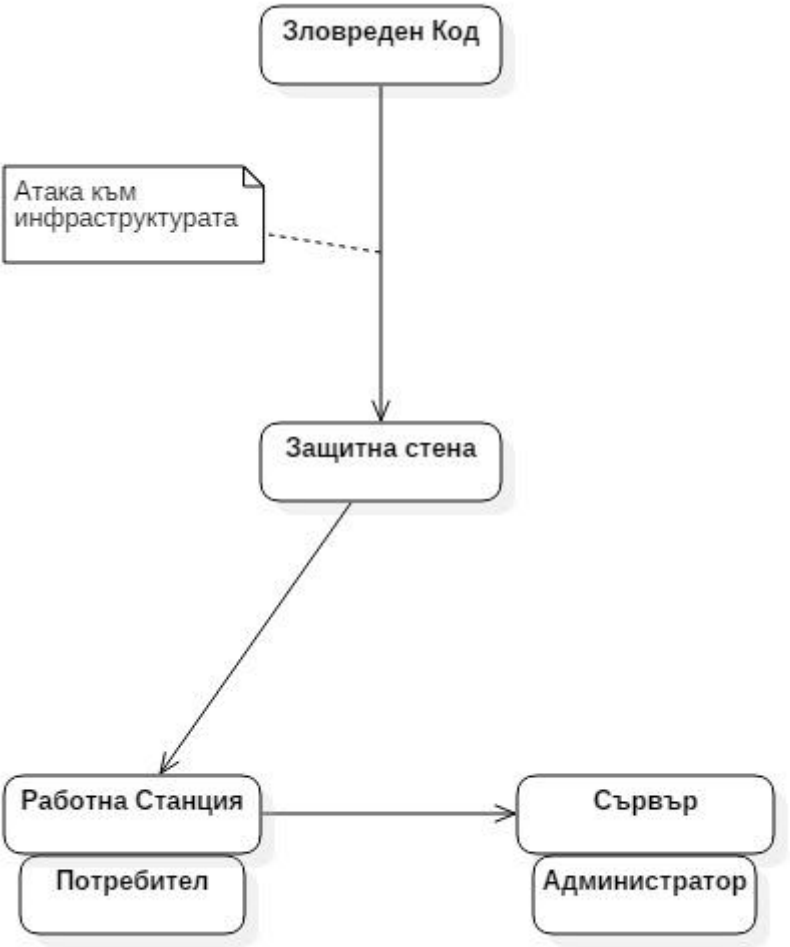
- Софтуерна атака

Софтуерната атака е често срещано явление в днешни дни. Публикуването на зловреден код под формата на вирус, червей, троянски кон е навсякъде в интернет пространството. Прикриването на този код става по най-различни начини. Често използвани са фалшиви сайтове, заразени файлове, заразени имейли или споделяне на линкове с заразено (променено) съдържание. При изпълнение на зловреден код

чрез някои от изброените възможности, злосторникът може да получи достъп до всяка една точка от представената система на фигура 1.
Зловреденият софтуер бива създаден от хора които искат да получат определени облаги чрез измама. След създаване зловреденият софтуер бива разпространен в интернет пространството под формата на заразени файлове, интернет страници и други. След създаване и пускане на зловреден софтуер той търси уязвими пространства в защитни стени и други защитни механизми за да проникне през тях и да получи достъп до защитената среда. Фигура 2 показва опростена методология на атака.

Фигура: 2.

Всяка една атака следва последователност от предефинирани стъпки, които довеждат до нейното правилно изпълнение и предоставяне на неоторизиран достъп или заразяване с вирус. Зловреденият код може да бъде засечен на ниво защитна стена чрез активиране на съответни филтри или създаване на правила които да засекат зловредния код. Правилната и ежедневна поддръжка на защитните механизми затруднява и минимализира шансовете на зловреден код да се изпълни успешно.

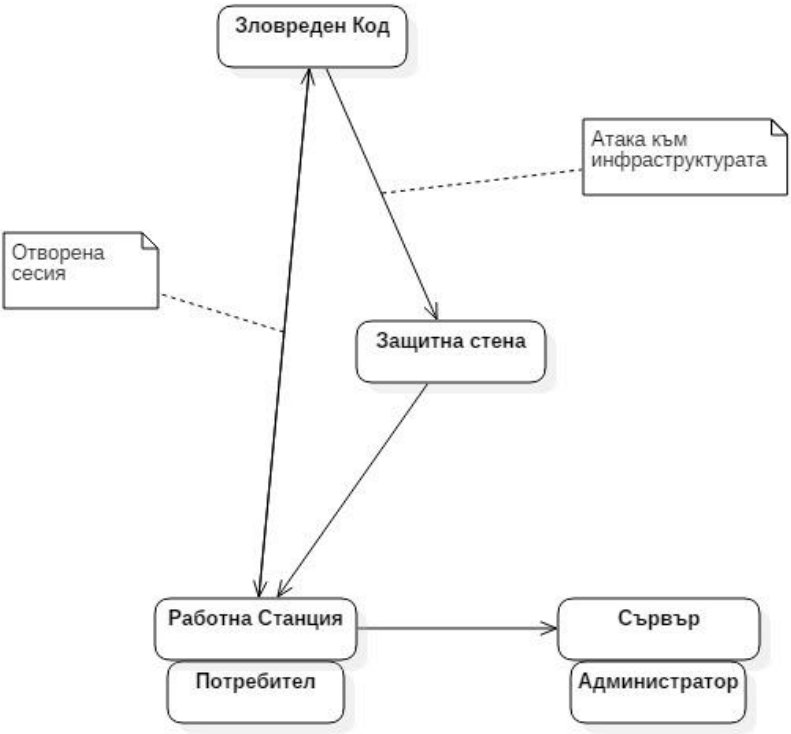


Фигура: 3.

Фигура 3 показва модел, който има за цел да се осигури неоторизиран достъп до сървърната среда на организацията, чрез преодоляване на защитна стена и работна станция. Един от най-разпространените начини за заразяване на работна станция е чрез изпращането на заразен имейл с прикрепен файл. Заразените прикачени файлове не могат да бъдат засечени успешно от защитните стени и биват пропускани. Пропуснатите файлове стигат до имейл кутията на потребителя и

чакат да бъдат изпълнени. Заразените имейли могат да съдържат заразени прикачени файлове или препратки към заразени линкове.

Локалните защитни стени на работните станции не засичат правилно тези заразени файлове и позволяват тяхното изпълнение. При изпълнение на заразен файл най-често се „отваря“ сесия между заразения компютър и компютъра на злосторника (фигура 4).



Фигура: 4.

След получаване на достъп до компютъра, злосторникът може да използва различни методи, за да получи пароли на акаунти. Един от най-разпространените методи е чрез инсталиране на key loggers. След инсталирането на този софтуер, злосторникът може да вижда всичко, което се въвежда от клавиатурата на работната станция. Също така чрез „Brute force“ атаки, може да „разбие“ паролите на администраторските акаунти, което би му дало възможност да достъпва и менажира вътрешните сървърите. С цел да не се допускат тези процеси да бъдат забелязани, те често се замаскират като системни или друг вид обичайни процеси.

Развитието на кибер сигурността и технологите предоставя възможност за разкриване на такива атаки макар и вече да са осъществени. Антивирусният софту-

ер помага за разкриването и блокирането на заразени файлове и съответните отворени сесии. Също така при правилно разпределение на администраторските и потребителски права полученият достъп на злосторника може да се окаже недостатъчен за изпълнение на неговите цели. Селектирането на потребителския достъп до чувствителните сървъри също е метод за защита. Основна защита остава разделянето на мрежите на работните станции, сървърите и останалото оборудване.

Литература

1. http://www.cyberbg.eu/doc/20161024_Cyber_strat_proekt.pdf Национална стратегия за киберсигурност „Киберустойчива България 2020" 24.10.2016г.

2. http://computerworld.bg/46595_startirat_euslugi_za_kibersigurnost_po_proekt_na_mtits Стартират е-услуги за киберсигурност по проект на МТИТС 22.11.2014г.

3. http://www.dnevnik.bg/tehnologii/2013/11/12/2179864_kibersigurnostta_u_nas_postepenno_se_povishava/ Киберсигурността у нас постепенно се повишава 21.11.2014г.

4. Мичев, Стефан. Илюзията за сигурност. София, 2012,

5. Слатински, Николай. Измерения на сигурността, София, 2000,

СЪВРЕМЕННИ КАНАЛИ ЗА ПРЕДАВАНЕ НА КОНФИДЕНЦИАЛНА ИНФОРМАЦИЯ

Веселка Т. Стоянова

Национален военен университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС”
9700 Шумен, ул. „Карел Шкорпил”1

MODERN CHANNELS OF TRANSMISSION OF CONFIDENTIAL INFORMATION

Veselka Todorova Stoyanova

National Military University, Faculty of Artillery, AAD and KIS,
1 Karel Shkorpil Str., 9700 Shumen, Bulgaria
+359896758902, veselka_tr@abv.bg

Abstract: *This report examines some mobile applications for transmitting graphical information by comparing the static characteristics of the transmitted images - SNR, PSNR, MSE, entropy, SSIM. Investigated mobile applications are: WhatsApp, Viber, Snapchat, Instagram, Messenger.*

Key words: *mobile application, confidential information, PSRN, MSE*

Въведение

В наситеното ежедневие и непрекъсната нужда за обмяна на информация чрез мигновени съобщения интерес представляват мобилните приложения, които предоставят тези възможности. В зависимост от държавата, използваните от потребителите приложения биват от разнороден характер и популярност. С тяхна помощ може да се изпращат съобщения, които често имат конфиденциален характер, а също би могло много бързо да се създава акаунт, който да се използва за еднократен трансфер на данни. Скритият канал, който предлага всеки слой на интернет протокола, е чудесна възможност, но доста труден за прилагане от потребители, които не притежават специализирани компютърни познания.

Всяко от тези приложения има особености, които е препоръчително да бъдат съблюдавани, за да се използват за нуждите на една конфиденциална комуникация. Разгледаните в статията приложения са подходящи за трансфер на изображения и видео. Както е известно, компютърната стеганографията е наука, която позволява да се скрива конфиденциална информация в прикриващ, цифров носител [4]. След прилагането на някой стеганогрфски алгоритъм, стои въпросът по какъв комуникационен канал да се предаде стегоизображението. Освен традиционните до момента канали, непрекъснато се търсят други начини, като особен интерес представляват и все по-нашумяващите и развиващи се социални мрежи или приложения за

предаване на мигновени съобщения. Такива например са WhatsApp, Viber, Messenger, Snapchat и Instagram, които са обект на настоящото изследване.

WhatsApp е мобилно приложение за смартфони, което служи за изпращане на незабавни съобщения. Приложението е достъпно за различни платформи: iOS, Android, BlackBerry OS, Symbian, Windows Phone. Чрез него могат да се изпращат съобщения, координати посредством Google карти, да се създават групови чатове и мултимедийни файлове между свързани с интернет абонати. Това приложение е изцяло криптирано.

Viber също е мобилно приложение подобно на WhatsApp, разликата е в това, че разполага с настолни програми за Windows и OS X, така че може да изпращат, получават и следят съобщенията от всеки компютър, както и на мобилното устройство. Viber позволява в допълнение към текстовите съобщения да се обменят видео- и аудиосъобщения. Когато се инсталира, приложението сканира адресната книга на абоната за телефонни номера (от всички потребители на Viber, които са регистрирани с номер) и се синхронизира работата на другите потребители. Viber използва Wi-Fi и мобилни данни, напълно е безплатен и без реклами.

Facebook **Messenger** се поддържа от Android, iOS, Windows Phone и Blackberry, също разполага с мобилна версия на Facebook съобщения в движение. Използва се, за да може потребителите да общуват с приятелите си във Facebook, които също използват приложението, за да се изпращат и получават съобщения на потребители, които не използват Facebook изобщо.

В зависимост от това къде се намира, потребителят може да използва Facebook Messenger само с име и телефонен номер. Приложението поддържа текст, изображения и споделяне на местоположението, както и Wi-Fi гласови повиквания.

Snapchat е мобилно приложение за изпращане на моментни изображения и съобщения. Приложението се използва за споделяне на снимки, писане на съобщения и преправяне на снимки в реално време с многобройни и забавни ефекти. Използвайки приложението потребителя може да записва видео, да прави снимки, да добавя текст или рисунки и да ги изпраща до приятели. Може да се създава лимит от време (от 1 до 10 секунди), за което получателят може да види изпратения му файл, след което той става недостъпен за получателя, но остава на сървъра на Snapchat. Повторно може да се разгледа само последния snap и то само веднъж в рамките на 24 часа. Ако даден потребител реши, че иска да запази дадено изображение, което му е изпратено, той не може да го свали. Единственият начин да го запази е, като му направи скриншот. Когато се направи скриншот, притежателят на изображението бива уведомяван, за тези действия.

Instagram е онлайн мобилна социална мрежа, която служи за споделяне на снимки и кратки видеа. По оригиналната идея снимките са квадратни и основно за фотоапарати на Polaroid или Kodak, но вече с версия 77,5, издадена през 2015 г., приложението позволява на потребителите да споделят снимки и видеа с различни размери. В това приложение могат да се добавят филтри на изображенията, които развалят качеството на оригиналната снимка и не са много удачни, когато става въпрос за скрита комуникация. Максималното времетраене на видеата е 15 секунди.

Освен така разгледаните приложения има и други подобни, които биха могли да послужат за нуждите на тайна комуникация. Общото между всички тях е предаването на изображения и видео информация и то в режим на мигновен трансфер. Съхраняването на тази информация в някои от приложенията е за кратък период,

което е предимство, поради факта че ако иман наблюдател на скритата информация съществува вероятност, той да пропусне трансфера.

Основни характеристики за оценка изображения

Освен възможността за предаване на информация е препоръчително да се оцени и качеството на изображенията предавани през съответното приложение.

За целта е необходимо да се изследват статистическите харктеристики на оригиналното изображение и вече преминалото през алгоритмите на мобилното приложение изображение.

При сравнение на две изображения се пресмятат четири основни статистически характеристики, които описват степента на подобие между изображенията: средна квадратична грешка MSE (Mean Squared Error), отношение на пиковия сигнал към шума PSNR (Peak Signal-to-Noise Ratio), индекс за измерване на структурната прилика в изображение SSIM (Structural Similarity Index for Measuring) и ентропията в изображения.

Изчисляването на средната квадратична грешка е стандартен статистически подход за обективно измерване на степента на различие между две изображения. Малка стойност на MSE означава, че средното ниво на разликата между тях е малко. В случай на две еднакви изображения, MSE има стойност, равна на нула. За разлика от MSE, по-голяма стойност на PSNR означава по-добро качество на изображението. При еднаквост на две изображения, PSNR има стойност клоняща към безкрайност. Основна цел на е минимизиране на стойността на MSE и съответно максимизиране на стойността на PSNR [1].

Изследваните характеристики са представени съответно чрез формули (1) и (2), като PSNR се базира на стойностите, получени за MSE:

$$(1) \qquad MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,\ j) - K(i,\ j)]^2,$$

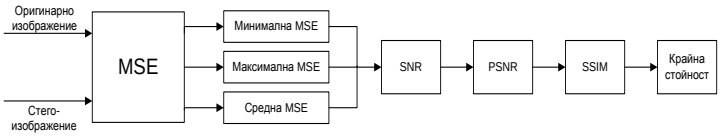
където m и n са ширина и височина на изображението; I(i, j) и K(i, j) са съответни пиксели с координати (i, j) в оригиналното и стего-изображение.

$$(2) \qquad \mathrm{PSNR} = 10.\log_{10}\left(\frac{\mathrm{max}^2}{\mathrm{MSE}}\right) = 10.\log_{10}\left(\frac{\mathrm{max}}{\sqrt{\mathrm{MSE}}}\right),$$

където max = 255 за 8 битови изображения.

Степента на подобие на изображенията преди и след процеса на предаване на изображенията през каналите, измерена чрез средната квадратична грешка MSE и отношението на пиковия сигнал към шума PSNR, определя качеството на изображенията [2].

На фиг. 1 е представена блокова схема визуализираща етапите на изчисляване на основните функции за качество изображенията. От фигура 1 става ясно, че те са взаимосвързани и произтичат един от друг.



Фиг. 1. *Блок схема на преобразуване на основните качествени характеристики в изображение [1]*

Индексът за измерване на структурната прилика в изображение SSIM (Structural Similarity Index for measuring) е подобен на MSE и PSNR, но е създаден с цел да ги подобри. Като показател той измерва промяната в яркостта, контраста и структурата на дадено изображение. За получаването на SSIM се комбинират стойностите, получени за средната интензивност на яркостта, вариациите в контраста и структурата на взаимната корелация между оригиналното и обработеното изображението. Яркостта, контрастът и стойността на структурната прилика са представени съответно чрез уравнения (3, 4 и 5):

$$(3) \quad l(x, y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1}$$

$$(4) \quad c(x, y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2}$$

$$(5) \quad s(x, y) = \frac{2\sigma_{xy} + C_3}{\sigma_{xy} + C_3},$$

където C1, C2 и C3 са константи, получени чрез равенствата

$$(6) \quad C1 = (K1L)2,\ C2 = (K2L)2.$$

В (6) L = 255 за изображение с 8 бита/пиксел, а K1 << 1 и K2 << 1 са много малки константи.

Получените в (3, 4 и 5) стойности се комбинират в крайна осреднена стойност за SSIM индекса

$$(7) \quad SSIM(x, y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma},$$

където $\alpha > 0$, $\beta > 0$ и $\gamma > 0$ са параметри, които определят относителната значимост на трите компонента в стойността на $SSIM(x, y)$ [3]. В статията е приета еднаква значимост на яркостта, контраста и стойността на структурната прилика, т.е. $\alpha = \beta = \gamma = 1$, както и C3 = C2/2.

От гореизложеното уравнение (7) следва в (8), в което е представен крайният вид на SSIM индекса между две изображения x и y:

$$(8) \quad SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

SSIM(x, y) приема стойности в интервала [0; 1], а когато x = y стойността на SSIM (x, y) = 1.

Изследване на статистическите характеристики на сравняваните двойки изображения

За изследването се използва оригинално изображение, което е с размери 3024x4032. Методиката, която ще следва, е:

- предаване на изходното изображение през съответното мобилно приложение;
- извличане на обработеното, изходно изображение;
- реализиране на сравнение на двете изображение с помощта на вградените функции в Matlab;
- анализ на стойностите за статистическите характеристики.

След първоначално реализиране на сравнение се установи, че в различните приложни среди размерът на изображението се трансформира. Така например WhatsApp коригира размера на изображението до 1200 x 1600, Viber до 1024 x 1280, за Instagram до 3024 x 3780, за Messenger-360 x 480.

Така установените размери не позволяват коректно изчисление на статистическите характеристики, в случай че оригиналното изображение не бъде коригирано до тази размерност. Поради тази причина оригиналното изображение се преоразмерява до размер, подходящ за дадения канал.

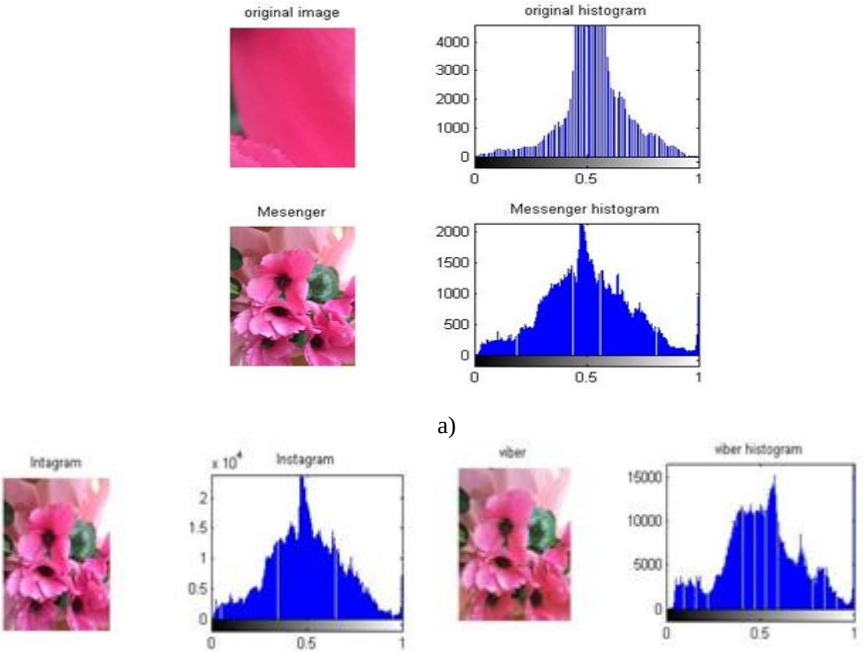
След преоразмеряването се получиха следните резултати, които са представени в табл. 1.

	MSE_{min}	MSE_{max}	MSE_{avr}	SNR	PSNR	Entropy
Viber	36.3148	58.9978	47.6563	4.2092	9.1834	7.8316
WhatsApp	34.2009	51.4985	42.8497	4.8471	9.6159	7.8000
Messenger	20.7087	61.2505	40.9796	7.4871	11.9589	7.8294
Instagram	8.6993	46.9152	27.80725	20.0595	24.1964	7.8245

Табл. 1. *Сравнение на статистическите характеристики при различните канали*

MSE и PSNR са две величини, които са в обратнопропорционално съотношение. С нарастване на MSE, PSNR намалява. От получените резултати, представени в табл. 1, се вижда, че статистическите характеристики на изображението, преминало през Instagram, са с най-добри стойности, а тези на Viber - с най-лоши.

На фиг. 2 са представени оригиналното и обработеното изображения с техните хистограми, получени в средата на Matlab 2012a.



***Фиг. 2**. Хистограми на оригинално и предавано изображения в различните комуникационни канали а)Messenger, б)Instagram и в)Viber*

При визуален анализ на изображенията и на хистограмите може да се забележат различия, които в повечето случаи са незначителни и недоловими от несъвършения зрителен апарат на анализатора. Трябва да се отрази и факта, че при една тайна комуникация анализаторът не разполага с оригиналното изображение, за да направи анализ. В повечето случаи, той може само да промени предаваното изображение, за да наруши целостта на скритата информация, макар че полезно би било за него да извлече предаваните данните.

В табл. 2 е реализирано сравнение между комуникационните канали по определени критерии, според които WhatsApp е най-разпространеното сред потребителите мобилно приложение, като общото е, че всички от разгледаните приложения позволяват споделяне на видео, изображения и разговори.

Показател за сравнение					
Приложение	***WhatsApp***	***Viber***	***Messenger***	***Snapchat***	***Instagram***
Брой на потребители към 2016г.	1.2 bilion регистрирани потребители	858 milion регистрира-ни потреби-тели	1 bilion регистрирани потребители	158 milion дневно активни	600 milion
Безплатно приложение	ДА	ДА	ДА	ДА	ДА
Поддържани платформи	IOS, Android, Windows, Black Berry, Symbian	IOS, Android, Window, Linux	IOS, Android, Windows IPhone,BB	IOS, Android	IOS, Android,
Споделяне на мултиме-дия	ДА	ДА	ДА	ДА	ДА

Табл. 2. *Сравнение на мобилни приложения за предаване на съобщения*

Заключение

Настоящото изследване позволява да се установи по какъв начин се променят изображенията, когато биват предавани чрез WhatsApp, Viber, Instagram, Messenger и Snapchat. Чрез сравнение на статистическите характеристики на двойките изображения се установи, че Instagram запазва най-добри показатели на статистическите характеристики, а тези на Viber водят до най-големи промени. Това би могло да подкрепи тезата, че Instagram би бил полезен за предаване на тайни съобщения чрез общодостъпни канали. Чрез изследването се установи, че всяко от приложенията променя размера на оригиналното изображение и ако то трябва да се използва за други нужди (напр. за предаване на тайни съобщения), трябва да се преоразмери.

Литература:

1. Stoyanova, V., Zh. Tasheva, Research of the characteristics of a steganography algorithm based on LSB method of embedding information in images, *Publication: Trans MotAuto15*. Available from: https://www.researchgate.net/publication/304579312_Trans_MotAuto15 [accessed March 30, 2017].
2. Rao K. R., and P. C. Yip. „The Transform and Data Compression Handbook“, 1st ed.: CRC Press, 2001
3. Wang Z., A .C .Bovik, H. R. Sheikh, and E. P. Simoncelli. “Image quality assessment: From error measurement to structural similarity,” IEEE Trans.ImageProcessing,vol.13, Jan.2004
4. Станев, Ст. Стеганологична защита на информацията. УИ „Еп. К. Преславски“, Шумен, 2013, стр. 119

СТУДЕНТСКО-ДОКТОРАНТСКА СЕКЦИЯ

CERT БЪЛГАРИЯ

Геновева Р. Парашкеванова, Цветослав С. Цанков

Геновева Радославова Парашкеванова, e-mail: g.parashkevanova@abv.bg
Цветослав Станиславов Цанков, e-mail: c.cankov@shu.bg

CERT BULGARIA

Genoveva R. Parashkevanova, Tsvetoslav S. Tsankov

***Abstract**: The mission of CERT Bulgaria is to assist the users of its services in carrying out proactive actions to reduce the risks of accidents in computer security. Assist in the resolution of such incidents in the event that already occurred.*

***Keywords:** Cyber-attack, Cyber incident, Information security, Ransomware*

Националният център за действие при инциденти в Информационната Сигурност – CERT Bulgaria предоставя централизирана база данни с информация, свързана с осигуряване на сигурна и защитена информационна среда.

CERT Bulgaria се ръководи от Васил Грънчаров.

Целите, които се поставят, включват:

- защита на информацията и технологичните активи;
- ограничаване директното влияние на инцидентите в сигурността върху информационното общество;
- помощ при възстановяване от инциденти;
- оценяване на въздействието от инциденти в сигурността;
- събиране и разпространение на техническа информация, свързана с инциденти в компютърната сигурност, както и с уязвимости в сигурността на системите и начините за предотвратяването им;
- провеждане на изследвания, свързани с нови технологии в мрежовата и информационна сигурност;
- провеждане на обучения, свързани с информационна сигурност и управлението на инциденти.

CERT България отчете 2949 сигнала за кибератаки през 2014. CERT България регистрира през декември 319 атаки, 37 от които са определени като заплахи с много висок риск, съобщи изпълнителен директорът на ИА „Електронни съобщителни мрежи и информационни системи" (ИА ЕСМИС) при откриването на конференция по ИТ сигурност.

Най-често срещаните кибератаки са зловредният код – 67%. Разпределените атаки за отказ от услуги (DDoS) са 18%, 8% са опитите за проникване, а 4% са определени като спам. Киберпрестъпленията навлизат във все повече аспекти от нашия

живот. Във фокуса им е не само икономиката, на дневен ред е и политиката. Навлизат все повече и нови играчи и вече говорим за организирана престъпност.

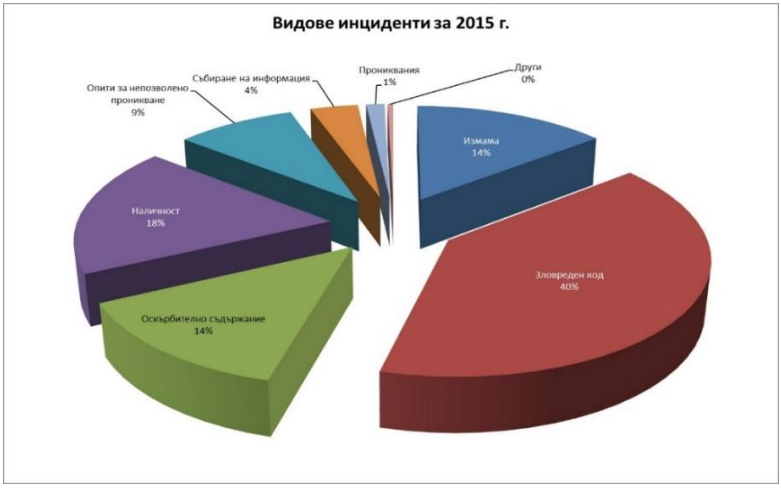
Той сподели, че в ИА ЕСМИС е внедрен специализиран софтуер, като част от защита на мрежата на агенцията, който визуализира трафика.

В Националния център за реакции при инциденти в областта на информационната сигурност (CERT България) към ЕСМИС са постъпили и обработени 2949 сигнала за нарушения в и от българското Интернет пространство през 2014 г.

Автоматизираните системи са подали 1832 сигнала, а 1117 са дошли от външни CERT и други организации, включително банки. Общият брой на засегнатите IP адреси е над 46 хиляди, но броят на компютрите е много по-голям тъй като зад редица IP адреси стоят компютърни мрежи с много компютри, допълни той. Важно е да се знае, че не всеки получен сигнал означава непременно инцидент.

От видовете инциденти най-голям е делът на DDoS атаките (41%), следват зловредните кодове (35,6%), опити за проникване (4,7%) и бот мрежи (3,32%).

„Най-слабото звено в информационната сигурност е човекът, именно към хората, а не към системите са насочени повечето атаки, коментира Васил Грънчаров. ИТ системите в някои държавни структури са сертифицирани за информационна сигурност, както се изисква от приетата наредба. Сертификацията обаче не е достатъчна, тъй като в законодателството не е предвидена отговорност за нарушаване на информационната сигурност“, добави Грънчаров. Според него ситуацията с информационната сигурност е такава, че не може и не трябва да се разчита само на помощта на държавата.



Фиг. 1: Модел на връзките между същностите в киберпространството

Над 700 киберинциденти регистрира CERT България за 2015 г. 737 са регистрираните у нас киберинциденти през 2015 г., според данни на Националния Център за действие при инциденти в информационната сигурност (CERT България) в Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи“ (ЕСМИС). Най-голям е броят на тези със зловреден код – 294, следвани от

измами – 105, такива с оскърбително съдържание – 100, опит за непозволено проникване – 65, събиране на информация – 26, проникванията – 10. За изминалата година 41 държавни институции са били участници в различни видове инциденти.

За януари 2016 г. от получените в националния център 59 сигнала за нарушения във и от българското интернет пространство, са установени 845 засегнати IP адреса.

Кибератаки срещу държавната администрация

Общо 5 са били кибератаките, регистрирани срещу интернет сайтове на държавни, общински администрации и други институции, според данни на Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи“ (ЕСМИС).

Петте атаки са били от типа “Ransomware”, който представлява зловреден софтуер. Той работи, като криптира файловете в системата, блокира или затруднява работата ѝ или блокира съответния браузър. След като се инсталира върху компютъра на жертвата, Ransomware криптира голяма част от работните файлове, като компютърът остава работоспособен, но файловете са недостъпни.

BULGARIA STANDARD CERTIFICATION

Повишаването на конкурентоспособността на българските компании не на последно място зависи и от въвеждането на все повече системи, както за управление, така и за сигурност.

BS CERT предлага на българските компании провеждане на сертификационни и контролни одити по международните стандарти от компетентни одитори, с продължителност и спазвайки процедура, съгласно изискванията на БДС EN ISO/IEC 17021:2006, което гарантира:

- въвеждането на ефикасно работеща система
- 100% успех, при решение на компанията да представи внедрената система пред чуждестранен акредитиран сертификационен орган;

BS CERT извършва сертификация на системи за управление съгласно международните стандарти:

- БДС EN ISO 9001:2008 Системи за управление на качеството. Изисквания;
- БДС EN ISO 14001:2005 Системи за управление на околната среда. Изисквания и указания за прилагане;
- BS OHSAS 18001:2007 Системи за управление на здравето и безопасността при работа. Изисквания;
- БДС EN ISO 22000:2006 Системи за управление на безопасността на хранителни продукти. Изисквания за всяка организация принадлежаща към хранителната верига;
- БДС ISO/IEC 27001:2006 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания.
- HACCP – Анализ на опасностите, контрол на критичните точки.

Литература:

1. **Каракънева**, Ю. Информационни системи в сигурността. Нов български университет, Платформа за електронно обучение.
2. **URL**: https://govcert.bg/

ЗАПЛАХИ В ИНТЕРНЕТ. ФИШИНГ И ФИНАНСОВО МУЛЕ

Геновева Р. Парашкеванова, Айлин И. Махмуд, Цветелина И. Методиева

Геновева Радославова Парашкеванова, e-mail: g.parashkevanova@abv.bg
Айлин Илияз Махмуд, e-mail: nurten_70@abv.bg
Цветелина Илиева Методиева, e-mail: tsvetelina. metodieva@abv.bg

INTERNET THREATS. PHISHING AND FINANCIAL MULE

Genoveva R. Parashkevanova, Aylin I. Mahmud, Tsvetelina I. Metodieva

***Abstract**: More than 90% of transactions to bank accounts of "financial mules" are associated with cybercrime. Illegally acquired funds often come from committed cyber-attacks such as phishing, online fraud when shopping / ecommerce fraud in card payment, compromising business e-mail.*

***Keywords**: Cyber-attack, Phising, Spoofing*

1. ФИШИНГ

Явлението се нарича „фишинг“ („phishing“ – „зарибяване“, произлиза от fishing – риболов), защото електронните съобщения, които се разпращат, са като „въдици“. Измамниците се надяват някои от получателите да се „хванат“ поради своята неопитност и неосведоменост, като им отговорят.

При фишинга измамници разпращат електронна поща, която претендира, че идва от почтена компания, и се опитва да убеди получателя да даде важна лична или финансова информация. Електронното съобщение обикновено моли да я изпратите в отговор или да я въведете на уебсайт, към който има връзка. Тези данни, например потребителски имена, пароли и номера на кредитни карти, после се използват от измамниците, за да се получат пари или услуги от името на пострадалия. Какво представлява фишингът или онлайн измамата?

Фишингът представлява способ за онлайн измама, използван от престъпниците, за да ви подмамят да разкриете свои лични данни, която след това им позволява да:

- кандидатстват и получат кредит от ваше име,
- изпразнят банковата ви сметка и направят разходи до лимита на кредитните ви карти,
- изтеглят пари от сметките ви,
- използват копие на дебитната ви карта, за да теглят парите ви от всяка точка по света.

1.1. Тревожни симптоми

Вероятно се осъществява опит за измама, ако ви бъде поискано да:

- предоставите лични данни на непознат източник,
- удостоверите данните за акаунта си под заплахата от блокирането му,
- продадете даден артикул с обещание, че ще ви се плати много повече от стойността му,

- направите преки парични дарения.

За да се предпазите, е необходимо да следвате няколко прости принципа:

- Използвайте съвременни операционни системи и антивирусни решения.
- Регулярно променяйте своите пароли за достъп.
- Не отваряйте съобщения от непознат източник.
- Изберете няколко независими канала за комуникация с Вашите контрагенти.
- Редовно следете банковите си наличности.
- Запознайте се подробно с разделите ни „Как да се защитя“ в секцията „Заплахи в интернет“!
- Сигнализирайте своевременно органите на МВР.

1.2. Компютърен жаргон

Фишингът и спуфингът едно и също нещо ли са?

СПУУФИНГЪТ /от английската дума spoof – пародия, измама/ е имитация на електронно съобщение или на уебсайт, направена от измамници, за да се създаде впечатление, че съобщението или сайтът принадлежат на някой друг. Фишинг атаките обикновено започват с разпращането на непоискани „спууф“ съобщения, които изглеждат като изпратени от законна компания. **Така че спууфингът е основна част от фишинга**, тъй като измамниците Ви карат да вярвате, че електронните съобщения и уебсайтовете всъщност произхождат от компании и организации, на които имате доверие.

Защо сте получили „спууфинг“ електронно съобщение?

Малко е вероятно съобщението да е адресирано лично до Вас. По-скоро много хора са получили едно и също съобщение, а ако Вие сте клиент на компанията, от която съобщението претендира, че идва, това е чисто съвпадение.

Какво е фарминг?

Измамниците завладяват домейн името на уебсайта на законна компания и прехвърлят потребителите към собствената си „спууфинг“ версия на същата Интернет страница. Така те събират личните данни, които вие въвеждате на лъжливия сайт. За съжаление, адресът на страницата изглежда нормално във Вашия уеб браузър и обикновените потребители могат да направят твърде малко срещу фарминга. За да се спре завладяването на домейн имена, е нужно техническо решение. Потребителите трябва да бъдат нащрек и да спазват съветите в рубриката ни за издайнически знаци.

2. ФИНАНСОВО МУЛЕ

Т. нар. съвременен феномен „финансови мулета“ е необходим на кибепрестъпниците, за да останат анонимни при прехвърляне на откраднатите финансови средства.

Какво означава „финансово муле“?

Физическо или юридическо лице, което, в поръчение на трети лица, прехвърля незаконно придобити финансови средства между различни финансови акаунти, в различни държави.

„Финансовите мулета“ са предварително набрани от киберпрестъпниците с цел превеждане на откраднати пари. За участието им се обещават комисионни, дават им се пари в брой, с които да регистрират банкови сметки в различни валути.

Дори „финансовите мулета“ да не са замесени пряко в престъпленията, с които нелегално се генерират парични средства (киберпрестъпност, при разплащане и

онлайн измами, наркотици, трафика на хора и т.н.), техните действия са незаконни: с прехвърлянето на финансовите средства финансовите мулета извършват „изпиране на пари“ /чл. 253 от Наказателния кодекс на Република България/, които са нелегално придобити.

Ако бъде установено, че извършвате дейност като „финансово муле“, дори да е било в следствие на заблуда, може да бъдете осъден на лишаване от свобода, глоба или обществено полезен труд. Създавате си също лоша банкова репутация, което ще се отрази при кандидатстване за кредит и други взаимоотношения с банковите институции.

Как се набират „финансови мулета“?

Набират става по два основни начина:

1. чрез директен контакт – случайно или целенасочено запознанство, последвано от предложение за печалба на лесни пари;
2. чрез публикуване фалшиви обяви за работа в Интернет.

С развитието на новите технологии и тенденции, организираните престъпни групи разработват нови системи за извършване на престъпления:

- чрез обяви за работа, които на пръв поглед изглеждат законни (напр. „парични преводи“);
- чрез онлайн публикации;
- чрез директен подход – личен контакт или чрез имейл;
- чрез социални мрежи (публикации в затворени групи);
- чрез съобщения, изпратени чрез незабавни приложения за съобщения (напр. Whatsapp, Viber)

Кои лица най-често стават „финансови мулета“?

Търсещи допълнителна работа, безработни, студенти, хора в затруднено финансово положение, туристи. Предимно мъже на възраст 18-45 години.

За какво да внимаваме?

Може да познаете, че се опитват да ви привлекат за „финансово муле“ по следните особености:

- Ако комуникацията между вас и лицето, което отправя предложението, протича по електронна поща, писането често включва лоша структура на изреченията с граматически и правописни грешки. Имейл адресът, свързан с офертата, използва уеб-базирани услуги (Gmail, Yahoo и т.н.), вместо да е с домейн, собственост на компанията, която отправя предложението.
- Обяви и реклами от името на чуждестранната компания, която търси да наеме на работа „местни / национални представители“ или „агенти“, с които да работи за определен период от време, с цел избягване на такси и др.
- Работните задължения включват основно прехвърляне на финансови средства или стоки;
- Конкретните задължения за работно място не са описани;
- Работната позиция не изисква притежаване на специално образование или предишен опит;
- Всички взаимодействия и транзакции ще се извършват онлайн. Офертата обещава високи приходи с малко ангажименти и усилия;
- Основното правило за започване на работата е да се използва вашата банкова сметка, за да се прехвърлят паричните средства.

Как да се предпазим?

Бъдете много внимателни при получаване на нежелани имейли или при случайни контакти в социалните мрежи с лица, обещаващи печалба на лесни пари.

Уверете се, че всяка компания, която ви отправя предложение за работа е реално съществуваща.

Бъдете особено предпазливи при предложения за работа от хора или дружества от чужбина, тъй като ще бъде по-трудно за вас да разберете дали те са реални.

Никога не предоставяйте банковата си сметка или други лични данни на непознати лица.

Какво да правя?

Ако сте получили имейли от този тип, не реагирайте на тях и не кликвайте върху линковете в съобщенията.

Ако след като прочетете тази брошура се съмнявате, че сте станали финансово муле, веднага спрете прехвърлянето на парите, като уведомите банката си и след това се свържете с полицията.

Литература:

1. **URL**: https://www.tad.bg/bg/
2. **URL**: http://www.cybercrime.bg/bg

ИНФОРМАЦИОННО ПРОСТРАНСТВО И ТЕХНОЛОГИИ

Глория И. Стоянова, Радослав М. Русев, Албена Б. Александрова

Глория Илиянова Стоянова, e-mail: stoqnova.4@abv.bg
Радослав Милков Русев, e-mail: rado199477@abv.bg
Албена Бойкова Александрова, e-mail: alb.alexandrova@abv.bg

INFORMATION SPACE AND TECHNOLOGY

Gloria I. Stoyanova, Radoslav M. Rusev, Albena B. Aleksandrova

***Abstract**: Information space is a hot topic nowadays, because it is related with the information society, in which we already are, and with the information technology, that are developing rapidly, affecting the individual person and the world around him.*

***Keywords**: information space, information technology, information warfare, society, Internet.*

Информационното пространство е една актуална тема в днешно време, защото е свързано с информационното общество, в което вече се намираме, и с информационните технологии, които се развиват с бързи темпове, оказвайки влияние на отделния човек и обкръжаващия го свят.

Информационно общество

Бурното развитие на компютърната техника и информационните технологии служи за тласък към развитието на обществото, построено на базата на използването на различна информация. Поради тази причина то получава названието информационно общество (ИО). То е степен в развитието на съвременното общество. Характеризира се с увеличаване на ролята на информацията и знанията в живота, нарастване на информационните комуникации, информационните продукти и услуги. Достъпът на хората до световните информационни ресурси и удовлетворяването на социалните и личностните им потребности от информационни продукти и услуги нарастват. В информационното общество се изменя не само производството, но и целият начин на живот, ценностната система. Нараства значимостта на материалните ценности.

Днес съществуват някои възгледи за информационното общество:

- ❖ това е общество на строг държавен контрол и цензура, потоп от културни полуфабрикати, тривиалности, сензации, пропаганда, информационна война;
- ❖ това е общество на свободата на личността, демокрация, висок професионализъм, творчество, международни корпоративни бази знания и технологично базирано развитие.

Информационно пространство

Информационното пространство е мрежа от субекти (информационни системи), обекти (информационни носители), състояния на обработка, събития и процеси, подчинени на пространствено-времеви и количествено-качествени причинно - следствени връзки. Също така се разбира като сървър, който може да бъде използван от различни лица, организации или администрации, за получаване на информация. В зависимост от областта, понятието си има своите различни принципи.

Информационното пространство е голяма и сложна система, която обединява:

- ❖ циркулираща и постоянно преобразуваща се информация;
- ❖ обекти на единна интегрирана информационна инфраструктура;
- ❖ субекти, които създават, събират, обработват, съхраняват, разпространяват и ползват информация.

Могат да се забележат и редица общи особености на моделите на информационното пространство, а именно:

- ❖ нарастване на скоростта, производителността и качеството на обработката на информацията, която възпроизвеждат всички рутинни човешки функции в рамките на общ унифициран модел;
- ❖ глобален обхват, достъпност и непрекъсната работа (т.н. нулиране на дистанциите и времето), превръщащи информационното пространство в най-мощния инструмент за градивно или деструктивно въздействие върху хората;
- ❖ генериране на многообразие от потребителски интереси, намерения, цели и задачи, водещо до поява на противоречия, конкуренция, конфликти и желания (намерения) за използване на организирано насилие (информационна война) с цел постигане на информационно превъзходство или господство и други.

Сигурност в информационното пространство

Характерна черта на днешната епоха стана развитието на отрасли, занимаващи се със създаването и предаването на информация в съвременния свят. Мнозинството от хората днес живеят не само в материално-природния свят, но и във виртуалния - това е информационно пространство, диктуващо свои закони и фактически превърнало се във втора реалност на човечеството. През последните десетилетия, с развитието на компютърните технологии, се увеличиха и средствата за информационно-психологическо въздействие върху хората. Във връзка с това, под заплаха се оказаха някои основни международни принципи: държавният суверенитет, ненамеса във вътрешните дела, мирното разрешаване на конфликтите и др. Възниква потребността от изясняването на някои понятия:

- ❖ информационно противоборство - това е форма на междудържавно съперничество, реализираща се чрез информационно въздействие над информационната инфраструктура и над обществото като цяло, за постигане на собствени цели.
- ❖ информационна безопасност - това е състояние на защита на информационното пространство в интерес на гражданите, организациите и държавата като цяло.
- ❖ информационно оръжие - това е комплекс от технически и други методи, средства и технологии, насочени, преди всичко, към установяване контрол над чуждите информационните ресурси. Те могат да са насочени и към вмешателство в дейността на чуждите системи за управление (държавни) с цел понижаване

работоспособността им, изземване на съдържащата се в тях информация или целенасочена дезинформация. Актът на използване на информационно оръжие се нарича информационно въздействие.

❖ информационно въздействие - това е влиянието на информационната среда върху живота, мислите и чувствата на хората. То може да протича, както на микро ниво, отнасящо се единствено да личното пространство на отделни граждани, така и на макро ниво, засягащо интересите на цялата държава.

В днешно време информационната безопасност има водеща роля в изследването на световната мрежа Интернет. Овладяването на тази проблематика позволява съсредоточаване върху ключови информационни заплахи и мерки по тяхното предотвратяване. Регулирайки отношенията на субектите и обектите на виртуалната среда Интернет на държавно ниво, е изключително важно да се спазва балансът между масовото възпроизвеждане на информация и ограничаване предаването на информация, накърняваща честта и достойнството на човека. Свободата съвсем не означава всепозволеност. Трябва да се отчита и балансът между свободата на достъп до информация и информационната безопасност на държавата, обществото и личността.

Да се защитят информационните ресурси (и по-точно - сървърите, на които те се съхраняват) в мрежата е много по-трудно, отколкото в други системи. Това произтича от някои свойства на Интернет като оперативност, незатвореност, трансграничност. Затова и една от първоначалните задачи на всеки потенциален ползвател, който се включва към „мрежата", е да обезпечи, посредством различни програми, безопасността на съхраняващите се на неговия компютър данни - нещо, което много хора пренебрегват, без да си дават сметка, че самата „мрежа" по своята структура не е способна, а и не е длъжна, да осигурява защита на отделните сървъри.

В САЩ с подобна дейност се занимава правителствената организация CERT (the Computer Emergency Response Team), представляваща група за реагиране на заплахи срещу компютърната безопасност. Организацията изучава проблеми по защита на информацията, като си сътрудничи с производителите на програмно и кадрово обезпечаване, а също така се занимава и с оповестяване на способите за регулиране на проблемите и изготвя инструкции по премахване на пробивите в защитните механизми. В рамките на тази организация функционират и специализирани служби за поддръжка на сървърите.

Бъдещите технологии за обработка на информацията ще се развиват на базата на цялата физическа същност, т.е. цялото информационно пространство, ще засегнат концептуалната рамка на информационното пространство и ще променят нейната същност, връзки и характеристики. От тази гледна точка, това е най-размитата абстрактна парадигма, която някога е разглеждана.

Информационни технологии

Това е съвкупност от дейности, специализирано оборудване и техники за управление, които се използват при създаването, преработката, съхраняването и разпространението на информацията. Информационните технологии включват в себе си два аспекта: социален и технически. От социална гледна точка информационните технологии направиха и продължават да правят качествена промяна в масовите комуникационни системи. От техническа гледна точка технологиите

водят до качествена промяна на средствата и методите за третиране на информацията. Развитието на технологиите за обработка на информацията осигурява повисоки скорости на трансфер на информацията от сигнали към знания.

Много хора, дори и специалисти в областта на информатиката, използват термина „информационни технологии“ като синоним на технологии, базирани на използването на компютри. На сегашния етап от своето развитие, информационните технологии представляват солидна база за представителна мотивация от една страна на социалния аспект на процесите за управление на достъпа до информация, а от друга – на комерсиалното, пазарно развитие на електрониката и свързаните с нея съпътстващи производства.

С тяхното развитие на практика се постига повишена скорост на информационните потоци, по-голяма пропускателна способност на каналите, повишена достъпност на услугите, разширяване на функционалните възможности и видовете услуги на системите и повишено търсене на този вид услуги като ефект от повишената зависимост от тях.

Интернет

Една от централните разлики между хибридната и традиционната война днес откриваме в използването на интернет. С негова помощ, а най-вече използвайки социалните мрежи, един агресор може да предизвика непознато досега объркване. Мнозина специалисти все по-настойчиво твърдят, че военният компонент вече не е най-важното при тази форма на война. Нещо повече - че той дори е най-маловажното.

Интернет, сателитните телевизионни системи, оптичните кабелно-разпределителни мрежи и мултимедийните технологии са монопол на малка част от човечеството, която предопределя тяхното развитие и начин на използване. Публичността на информационните канали и носители дава възможност за достъп до тях на всеки. Но този достъп днес е поставен под контрол и е собственост на малка група държави, корпорации и частни лица, които получават едно ново стратегическо превъзходство. Засилващата се интеграция на световното информационно пространство дава възможност това превъзходство да се реализира, където информационните операции са взрив на насилие върху човешкия разум и психика.

С огромната си тиражност, глобален обхват и неограничена памет, съвременните глобални информационни системи превръщат медийните психологически операции в стратегическо оръжие за въздействие върху човешката цивилизация. „Експлозията” на знанията, разпространението на глобалните информационни инфраструктури и внедряването на висшите информационни технологии във военното дело, радикално промениха съотношението между огневата мощ и информационното осигуряване, което продължава да се променя с високи темпове, в полза на последното . Тази тенденция наложи да се преразгледат приоритетите в структурата на въоръжените сили, тяхната екипировка, въпросите на командването и управлението, бойната подготовка и персоналният тренинг.

На практика, превръщайки се в основен способ за радикално решаване на възникналите кризи и конфликти, информационните операции се превърнаха в една от основните стратегически заплахи за националната сигурност.

Светът усвоява нови форми, способи и средства за въоръжена борба. Развитието на информационните технологии все повече отдалечава хората от бойните

полета и превръща сраженията в „Звездни войни“. Нахлуващата през телевизионните екрани и интернет информация, непрекъснато променя установените възгледи и нищо не е в състояние да спре този процес.

Информационни войни

Информационната война е:

- ❖ технологична война за осигуряване на технологично господство над световното информационно пространство.
- ❖ война за информационно превъзходство.
- ❖ война, чрез която се цели постигането на право и възможност за провеждане на информационно базирани нападателни или отбранителни операции с употреба на информационни оръжия срещу информационната инфраструктура на противника.

В края на XX век технологичното развитие на човешката цивилизация внесе необратими промени в хода на бъдещата война, която ще бъде:

- ❖ машинно, а не човеко-ориентирана;
- ❖ във форми, произтичащи от технологии, а не от организации;
- ❖ с приоритет на възпиращите бойни действия, вместо въвличане в унищожителни сражения;
- ❖ поставена на индустриално- технологична, а не на командно-административна основа.

Бъдещето на информационните войни

Бъдещите бойни действия ще се развиват в три макросфери: физическа, информационна и морална. Въоръжената борба се очаква да се води като динамични, високотемпови, високоинтензивни въздушно-космически операции, обхващащи огромни територии. Високоточните оръжия, които се доближават по унищожаващата си сила до тактическите атомни оръжия, но не предизвикват вторични разрушения, ще бъдат използвани от самото началото на войната. Те ще унищожават вражеските такива, командването и управлението на противника, противовъздушната му отбрана и оперативно-тактическите групировки. Тактическият бой във физическата сфера ще е краткотраен, с увеличаваща се смъртоносност и експлозивно нарастваща интензивност. Тази война ще се води с внезапни и бързи маневри, сложно структурирана отбрана, силна информационна интеграция и висок професионализъм .

В бъдещите сражения ще се използват множество нови оръжия, изградени на базата на авангардни технологии и нови физически принципи - геофизически, електромагнитни, радиочестотни, инфразвукови, генетични, психотронни, лазерни и др. Пробивите в природните науки предлагат множество нови възможности за създаване, както на уникални оръжия за масово поразяване, така и на несмъртоносни такива. Като краен резултат развитието на средствата за въоръжена борба ще продължи да захранва протичането на два глобални процеса:

- ❖ трансформационен, при който рутинните интелектуални функции на човека се прехвърлят върху новите интелигентни оръжия и
- ❖ интеграционен, при който всички подсистеми за командване и управление на въоръжените сили се обединяват в една обща “Система от системи”.

Тези два процеса променят характера и структурата на бъдещата война, изместващи центъра на тежестта на атаките от унищожаване на хората към деактивиране или разрушаване на средствата за въоръжена борба.

В тази разработка бяха разгледани определенията за информационно общество, информационно пространство, информационни технологии, информационна война и връзката между тях. Основните изводи, до които успяхме да стигнем, са:

- ние вече се намираме в едно информационно общество.
- на пазара навлизат все по-нови и по-нови технологии.
- с тях могат да бъдат засегнати както отделни граждани, така и държавни организации.
- под заплаха се оказват държавните интереси, мирното разрешаване на конфликти и други. В следствие от това възниква потребността от информационна безопасност и сигурност на информацията и информационното пространство.
- светът усвоява нови способи и средства за въоръжена борба чрез новите технологии.
- в бъдещите сражения ще се използват множество нови оръжия, изградени на базата на нови технологии и нови принципи.

Тъй като сме в информационната ера и информационното общество, информационното пространство е сферата, където в днешно време се водят информационните войни. През 21-ви век границата между мира и войната постепенно се размива. По съответен начин се променят логиката и практиката на войната, която изведнъж се оказва явление без начало и без край. Насилието е само част от това явление, което използва политически, икономически, информационно-технически и други средства. Това може да е заплаха за всички.

ЛИТЕРАТУРА:

1. **Семерджиев, Ц.** Информационна война. „Софттрейд“, С., 2005.
2. **URL**: http://iniod.unibit.bg

SWOT АНАЛИЗ НА ВЪВЕЖДАНЕ НА „ОБЛАЧНИ” ТЕХНОЛОГИИ В АВТОМАТИЗИРАНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ

Петър С. Генов

Висше военноморско училище „Никола Й. Вапцаров“,
Варна 9026 ул. „ Васил Друмев“ 73 GSM:0883551019

SWOT ANALYSIS OF THE INTRODUCTION OF „CLOUD“ TECHNOLOGIES IN AUTOMATED INFORMATION SYSTEMS

Petar S. Genov

Abstract: *The term "cloud" is used as a metaphor based on the image of the Internet in computer network diagrams. Users of cloud computing can significantly reduce costs for infrastructure (in the short and medium term) and to respond flexibly to changes in computer and network needs, using computer elastic properties (elastic computing) cloud services.*

Keywords: *monitoring as a service – MaaS, resource pooling, backup as a service, self service on demand*

I. ВЪВЕДЕНИЕ

Облачните услуги могат да осигурят на бизнеса най-ефективните средства за подобряване на обслужването на клиенти, разширяване на продуктовите предложения и развитие на иновациите. По оценка на IDC , пазара на публични облачни изчисления през 2009 г. е $17 млрд — или около 5 % от целия пазар на информационни технологии. От националния институт по стандарти и технологии на САЩ са определени следните задължителни характеристики на облачните изчисления:

Самообслужване по заявка (self service on demand). Потребителят самостоятелно определя и изменя изчислителните потребности, такива като сървърно време, скорост на достъпа и обработка на данни, обем на съхраняваните данни, без взаимодействие с представител на доставчика на услугата;

Универсален достъп по мрежата. Услугите са достъпни за потребителя по комуникационната мрежа, независимо от използвания терминал.

Обединяване на ресурите (resource pooling). Доставчика на услуги обединява ресурси за обслужване на голямо число потребители в един пул/басейн, като динамично преразпределя мощностите между потребителите в условия на постоянна промяна на заявки. При това потребителите контролират само основните параметри на услугата (например, обем данни, скорост на достъп), но фактическото разпределение на ресурсите, предоставяни на потребителите се осъществява от доставчика.

Еластичност на услугата. Услугите могат да бъдат предоставени, разширени, свити във всеки момент от времето без необходимост от взаимодействие с доставчика, като правило в автоматичен режим.

Отчет на употребата. Доставчикът на услугата автоматично изчислява потреблението на ресурса на определено ниво на абстракция и на база тези данни оценява обема на предоставените на потребителя ИТ услуги.

II. ОСНОВЕН ТЕКСТ

1. SWOT анализ. Целта за създаването на SWOT анализ относно въвеждането на „облачните“ технологии е да видим нагледно дали си заслужават разходите за една такава иновация. Кои са предимствата и недостатъците, как да изберем най-добрият сервиз за нас от многобройните доставчици и др.

SWOT

Таблица 1. Swot таблица за критерии

Силни страни	Слаби страни
Функционалност	Данните са на локалният диск
Мобилен достъп	Има различни политики за сигурност
Самообслужване при необходимост	Различна предлагана функционалност
Лесна употреба	Липса на компетентни кадри
Помощ и поддръжка	Остаряла материална база
Намаляване на разходите	
Гъвкавост	
Постигане на позитивни промени	

Таблица 2. Swot таблица за критерии

Възможности	Заплахи
Ниски търговски бариери	Мобилният достъп
Инфраструктура IaaS	Голям брой доставчици
Платформа PaaS	Протоколите за криптиране
Софтуер Saas	Промяна на потребностите на потребителите
Мониторинг MaaS	

2. Силни страни

а. Функционалност. Облачните услуги позволяват да се съхранява и обработва всякакъв вид съдържание точно така, както се извършва на твърдия си диск – от текстови документи до музикални и видео файлове. Някои услуги позволяват да се съхранява електронна поща, контакти и електронен календар. Услугите позволяват да се достъпва, редактира и споделя съдържание, без значение от каква платформа –настолен или преносим компютър, смартфон или таблет. Други важни функции са синхронизиране на файловете от всичките устройства, а споделянето е защитено с парола и криптиране на файловете.

б. Мобилен достъп. Едно от най-големите предимства на облачните услуги е, че може да се достъпват от различни устройства. Независимо от устройството и мястото - служебен (на работа) или личен компютър (у дома), смартфон или таблет (в движение), облачните услуги позволяват да се използва определено съдържание навсякъде от голям брой приложения и браузъри за мобилни устройства.

в. Самообслужване при необходимост: всеки клиент може да получи различни изчислителни услуги, включително сървъри, дискови масиви и приложения. Те работят автоматично, елиминирайки нуждата от човешки контакт с доставчиците на услуги. Според потребностите на клиента осигурените компютърни ресурси и услуги могат да се увеличават или намаляват, в зависимост от специфичните нужди на бизнеса или организацията.

г. Лесна употреба. Мобилните приложения и браузърите, с които се достъпват „облачните" услуги са с интуитивен и лесен за използване потребителски интерфейс. Мобилните приложения са лесни за потребителска настройка и конфигурация, като остава да се направи само локална настройки по предварително дефинирани шаблони (темплейти).

д. Помощ и поддръжка. Получаването на помощ при проблем, когато се използват „облачните" услуги става чрез връзка с доставчика по телефон, през имейл или чат.

е. Намаляване на разходите. Използването на „облачни" услуги води до намаляване на разходите, свързани със закупуване на хардуер, софтуер, наемане на помещения и квалифициран персонал, който да се грижи за тяхната поддръжка. Заплащат се само заявените и използвани услуги, т.е. Клиентите плащат месечна такса и не са налага закупуването на скъпи лицензи.

ж. Гъвкаво ценообразуване. Тъй като клиентите могат сами да определят типа и обема на облачните услуги, които ползват, те имат възможността правилно да планират своите разходи.

з. Гъвкавост. Доставчикът на „облачните" услуги предлага възможност за промяна по всяко време на необходимите ИТ ресурси, за да се реагира на промяна (растеж или спад) в бизнес средата;

3. Слаби страни

а. Потребителските данни не са на локалния диск. Обикновено съхраняването на потребителските данни на отдалечено място (сървър за данни) не е проблем, а предимство тъй като са централизирани за достъп отвсякъде и лесни за архивиране. Ако обаче използвате като услуга система за планиране ресурсите на предприятието (erp система), данните от които се изтеглят всяка вечер в система за бизнес анализ (bi система), за да се подготвят за анализ от бизнес мениджърите – очевидно липсата на данните на достатъчно бързо и лесно за достъп място е сериозен проблем.

б. Прилагане на различни политики за сигурност. Обикновено прилаганите политики за сигурност на локалната система са различни от политиките за сигурност на доставчика на „облачните" услуги. Това означава, че създаваните потребители в локалната активна директория не се създават автоматично в „облачното" приложение, отделно се управляват паролите, липсва централизирано наблюдение върху дневниците (логовете) за сигурност и др.

в. Разлика в предлаганата функционалност. „облачните" приложения могат да имат различна, по-голяма или по-малка функционалност от предлаганата от локалните приложения. Това може да доведе до наличието на „излишни" функции или до определени ограничения в работата и степента на използване на приложението.

4. Възможности

а. Инфраструктура като услуга (iaas). Използва се вече изградена ит инфраструктура, при която клиентът заплаща само за ресурсите, които са му необходими. По този начин потребителят може да „създаде“ сървър във виртуална среда, без да има проблемите и ограниченията, съществуващи при физическото инсталиране на хардуер. Това означава, че може практически по всяко време да се създаде, стартира, спре и премахне даден сървър. Към инфраструктурата като услуга се включват - складове за данни като услуга (data wherehouse aas) - доставчикът предоставя информация за ползване при провеждане на маркетингови кампания и бизнес анализи; резервни копия на данните (backup as a service) – доставчикът създава и съхранява резервни копия на данните и при необходимост възстановя състоянието от тях; комуникация като услуга(communication as a service – caas) - доставчикът предоставя комуникационни канали за бърз и сигурен (защитен) достъп.

б. Платформа като услуга (paas). Набор от средства за разработване на софтуер и софтуерни приложения, които са разположени на сървър на доставчика и са достъпни по интернет, без значение от използваната операционна система, ресурси и др. Пример за наемане на цялостна платформа за разработване на софтуер е windows azure, включваща c# + windows azure compute + wcf + asp.net mvc + azure tables + sql azure + azure blobs + azure cdn.

в. Софтуер като услуга (saas). Използване на софтуерни ресурси чрез интерфейс портал (front-end), което практически гарантира тяхната достъпност от всяка точка на планетата. Подобни услуги могат да включват както уеб-базирана електронна поща, така и пълноценното използване на интегрирана система за управление на бизнеса или отделни компоненти;

г. Мониторинг като услуга (monitoring as a service – maas). Доставчикът предоставя услуги за мониторинг и анализ на прилаганите ит политики – например политики за сигурност и т.н.;

5. Заплахи

а. при много от „облачните” услуги разработчици не спазват протоколите за криптиране, които защитават информацията от неразрешен достъп. Различните мобилни приложения имат различно ниво на защита – както като ниво на сигурност, така и като отговор на нови атаки.

б.Доставчиците разработват нови актуализации за мобилните приложения, както и нови мобилни приложения за да се намалят рисковете и направят услугите по-защитени, но това е свързано със изтегляне (сваляне) и инсталиране на тези приложения, което носи рискове от вируси. Очаква се бъдещите „облачните” услуги да предлагат унифицирано решение, което ще увеличи защитата срещу атаки.

6. Проучване на Gartner

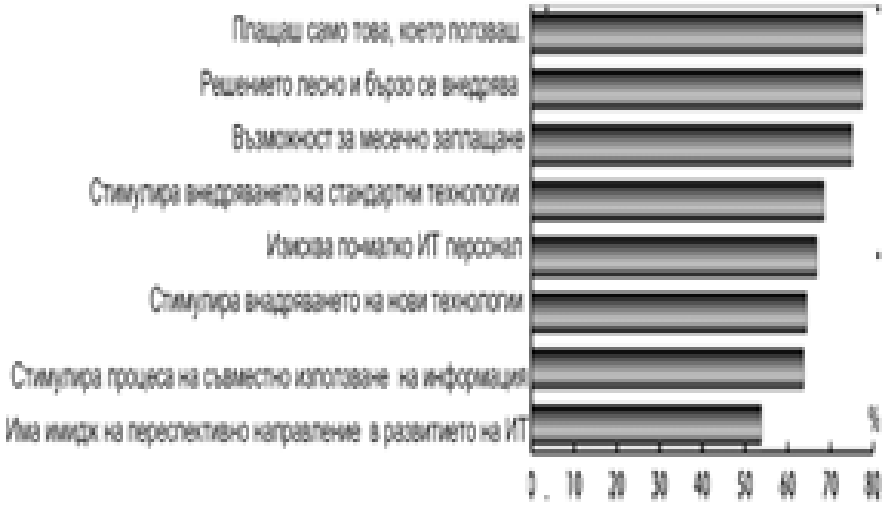
Проучване на Gartner за търсенето на облачни услуги през 2014 г. за 2016 г. показва, че компаниите приемат радушно облачния компютинг и все по-мащабно се възползват от предимствата му.

Търсене на облачни услуги

Източник: Gartner

Както се вижда от фигурата:

SaaS (69% през 2014г. и 66% през 2016 г.) - най-голям интерес;
компютърните услуги – 14% (22% през 2016 г.);
интегрираните услуги – 12% (6% през 2016 г.)
PaaS услугите – 3% (3% през 2016 г.),
услугите за съхранение - 1% (2% през 2016 г.);



Фигура 1. Проучване на Gartner

Фигура 1 едно показва най-големите и основни предимства на облачния компютинг. Нагледно може да видим, че на челно място седи именно финансовото облекчение следвано от бързото внедряване. За ефективно сравнение на предлаганите на ИТ пазара сервизи на облачен компютинг могат да бъдат използвани следните критерии.

Ориентация към бизнеса - Сервизът трябва да бъде ориентиран към създаване на услуга, с възможност за измерване с метриките на бизнеса.

Техническите детайли трябва да бъдат скрити, като са изяснени преимуществата, които дава сервиза на бизнеса.

Еластична мащабируемост - Системата е задължително да има гъвкави възможности за мащабируемост, както в страна на увеличение, така и в страна на намаление на използваните ресурси.

Пакетна доставка на услуги - Всяка услуга трябва да съответства на задачите на бизнеса и да се предоставя само при възникване на необходимост.

Автоматизация, интероперабелност и интеграция на компонентите на системата - Системата трябва да се изгражда чрез интеграция на компонентите в единно цяло. Основна цел - повишаване качеството на сервиза и снижаване стойността на услугите.

III. ЗАКЛЮЧЕНИЕ

Изводите от SWOT анализа и от фирмената гледна точка ясно показват, че „облачните“ нововъведения могат да бъдат полезни, но в никой случай не трябва това да се приема като панацея, тъй като може да се срещнат доста спънки, които са ясно изразени в „Заплахи“. Като цяло „блачният“ компютинг има своето място в малките предприятия. Развитието на технологиите в тази сфера ще се наблюдава преминаване на системи от традиционния към този по-нов модел на работа. В същото време обаче фирмите, трябва да извършват този преход внимателно и добре обмислено, а решенията им трябва да бъдат добре мотивирани и смислени от бизнес гледна точка.

ЛИТЕРАТУРА:

1. Списание, .Net, Брой 43, София, 2011
2. Тодоров Л., Съвременни модели за оценка на бизнеса, София, 2014
3. Антонов Г., Swot-анализ. СУ, София, 2010.

ЗАЩИТА И КОНФИДЕНЦИАЛНОСТ НА ИНФОРМАЦИЯТА И ДОСТЪПА В TETRA

Михаела Й. Йотова
Васил В. Иванов **Николай Пл. Маринов**

Адрес за кореспонденция:
Михаела Йотова - гр.София кв.Младост 4 бул."Александър Малинов" №1;
тел: 0876886665; email: mi6etuu@abv.bg
Николай Маринов – гр.София кв.Младост 4 бул."Александър Малинов" №1;
тел: 0889868198;email: niki94_1993@abv.bg
Васил Иванов – гр.София кв.Младост 4 бул."Александър Малинов" №1;
тел: 0899688415;email: unknown_alfa@abv.bg

SECURITY AND PRIVACY OF INFORMATION AND ACCESSIN TETRA

MihaelaYotova
Nikolay Marinov **Vasil Ivanov**

Abstract:*In report are described the processes of encoding the speech, noise resistant encoding of the data and cryptographic protection of the information and the accessin Tetra standart. The algorithms for authentication of the subscribers and the access in Tetra are visibly presented here. The standart and the high level of confidential protection of the information in Tetra are described by the radio interface and cryptographic encoding of the data from one spot to another. In a table is shown the dependence of the information sharing speed from the cryptographic protection level.*

Keywords:*communication system, Tetra, security, information, protection, encoding*

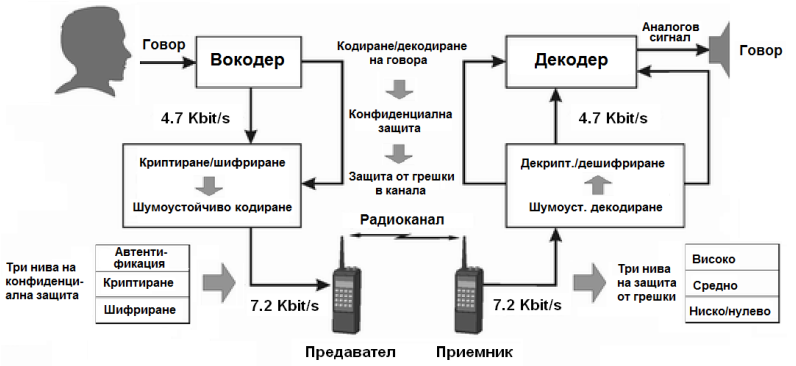
I. Въведение

TETPAce явява цифрова комуникационна системаза нуждите на правоохранителните органи, сигурността и отбраната, поради което конфиденциалността на информацията и достъпа в нея са от изключително важно значение[3].В тази връзка стандартът осигурява повишена степен на защита и конфиденциалност в сравнение със стандартите за публични мобилни комуникации, каквито в момента са:GSM, UMTS, WiMax – IEEE 802 и др. [1,2]. Конфиденциалността на връзката се постига чрез шифриране на говорния трафики данните в канала, но освен тях, съществен принос за повишаване на конфиденциалността имат и процесите по цифровото кодиране и компресиране на говора, както и многостепенното шумоустойчиво канално кодиране на данните.

II. Изложение

КОДИРАНЕ НА ГОВОРА В TETRA

TETRAсе явява цифровакомуникационна система и трансфера на информацията в нея, включително и говора, се осъществява по цифров път.Прилагането на цифрови методи за предаване дава възможност за съществено повишаване ефективността, шумозащитеността и конфиденциалността на информацията и системата като цяло. За целта информацията се подлага на обработка, чрез различни видове кодиране (Фиг.1), като: кодиране на говора, шумоустойчиво кодиране, криптографско кодиране.



Фиг. 1. Процеси по кодиране и декодиране на говора и информацията в TETPA

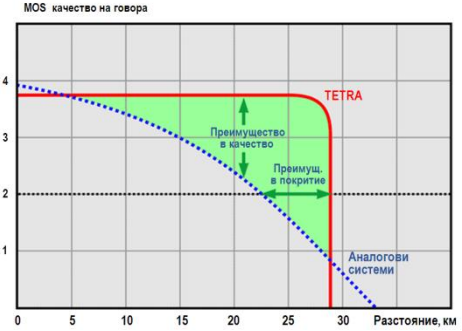
Кодирането и декодирането на говора в стандарт TETRA се осъществява с вокодери и съответно декодери,обединени функционално във вид на кодеци, използващи алгебрични алгоритмис линейно предсказване и многоимпулсно възбуждане– ACELP (AlgebraicCodeExcitedLinearPredictions) [1,7].ВокодеритеACELP преобразуватаналоговия говорен сигнал от микрофона в цифров поток със скорост 4700bit/s. След съответно шумоустойчиво канално кодиране, чрез добавяне на допълнителни битове, сумарната скорост на инф. поток нараства на 7200 bit/s.Тъй като вTETRA на една носеща честота саразположени 4 абонатни канала (тайм слота), сумарната скорост нараства на (4x7200) 28.8 Kbit/s. В последствие се добавя и допълнителна служебна информация за синхронизация иуправление, в резултат на скоросттанарастване на 36 Kbit/s.В приемната страна се осъществява декодиране на сигнала, чрез аналогично преобразуване в обратен, ред (фиг.1).

Обработката на говора въввокодера и декодера се осъществява по блокове. Продължителността на тези блокове е 30 ms, от които, чрез дискретизация по време с честота 8 kHzce вземат по 240 отчета, които се кодират цифрово с АЦП чрез 8 битов двоичен код. За всеки такъв блок след съответно компресиране с вокодерсъгласно алгоритъма ACELPce формира цифров блокс обем от 137 bit, което съответства на скорост на предаване на информацията 4,567 Kbit/s. одекът ACELPизползван в TETPA, осигурява качество на възпроизвеждане на говора по скалата MOS - MeanOpinionScore(осреднена оценка на разбираемост на говора)

равна на 3,7, с което незначително отстъпва по качество от вокодерите в GSM мрежите (MOS=3.9) [6]. За сравнение: оценка MOS 4 означава «превъзходно качество с незабележимо влошаване»; MOS 3 «добро качество с забележимо, но не дразнещо влошаване». За сметка на това стандарт TETRA осигурява двукратно по-голяма компресия на сигнала (TETRA - 4,7 Kbit/s, GSM – 9,4Kbit/s) и четири пъти по-висока спектрална ефективност.

Във втората версия на системата – TETRA се използват два допълнителни кодека – AMR (AdaptiveMultipleRate) и MELPe (MixedExcitationLinerPredictive, enhanced) за съвместимост с GSM и комуникационните системите на НАТО.

Цифровото предаване на говора в TETRA в сравнение с аналоговите системи позволява запазване неизменно качество на говора в зоната на покритие, независимо от разстоянието (фиг. 2).



Фиг. 2. Преимущество на цифровото предаване в качество и покритие пред аналоговото

ШУМОУСТОЙЧИВО КОДИРАНЕ В TETRA

За повишаване на защитеността и достоверността на предаванатаинформация в ТЕТРАсе прилагашумоустойчиво кодиране на информацията в канала за връзка, чрез въвеждане в състава на предавания цифров сигнал допълнителна („излишна“) информация (фиг. 1). С помощта на тази „излишна“ информация в приемната страна грешките, възникващи в процеса на предаване се откривати отстраняват [4].

Стандарт ТЕТРАосъществява шумоустойчиво кодиране чрез последователно преобразуване на информацията на 4 нива чрез: блоково кодиране, конволюционно кодиране, умножение,скремблиране. Структурната схема на процесите по каналното кодиране в TETPA е представена на фиг. 3 и е обща за всички видове логически канали, използвани в стандарт TETPA.

Фиг. 3. Схема на процесите по каналното кодиране в TETRA

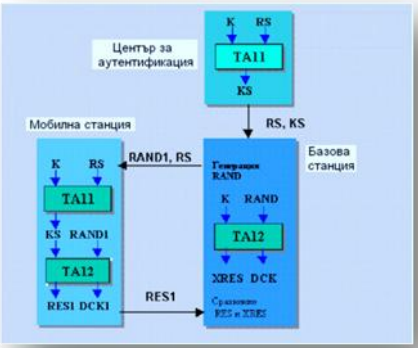
Блоковото кодиране е предназначено за откриване на единични и групови грешки в канала и в определени случаи за тяхното коригиране и изправяне.Конволюционното кодиране основно се използва за изправяне на единични грешки, макар и да не осъществява тяхното откриване. Кодирането чрез умножениесе осъществява чрез пренареждане на битовете без внасяне на излишни битове в информационния блок. Основно е предназначено за преобразуване на груповите грешки, възникващи в канала за връзка вследствие на многолъчевото разпространение на сигнала, в единични грешки, които лесно се отстраняват с помощта на блоковото и конволюционно кодиране. Скремблирането се осъществява чрез 32-битов изместващ регистър с логически обратни връзки и служиза нормализиране на статистическите свойства на информационния цифров поток в канала за връзка и повишаване конфиденциалността на предаваната информация [5].

КРИПТОГРАФСКА ЗАЩИТА НА ИНФОРМАЦИЯТА В TETRA

За осигуряване на безопасност на свръзката и достъпа до мрежата стандартът TETRA използва следните механизми за защита: автентификация на абонатите, шифриране и криптиране на информацията.

Автентификацията на абоната – това е метод за доказване на неговата самоличност с цел за защита на ресурсите на мрежата от несанкциониран достъп до нея. Процедурата по автентификацията наабонатите се осъществява чрез уникалния ключ – К на абоната и алгоритмите за автентификация -TA11 и TA12, записани в електронен модул за автентичност на абонатните терминали [7].

При влизане на абоната в мрежата базовата станция анализира информацията в този модул и взема решение дали да допусне абоната до ресурсите на мрежата, или не. За целта центърът за автентификация генерира случаен код RS и го изпраща на мобилната станция. От своя страна тя, чрез случайния кодRS, индивидуалния ключ К и криптографския алгоритъм TA 11 формира сеансовия ключ KS.



Фиг. 4. Алгоритъм за автентификация на мобилните абонати
RS-случаен код; К – индивидуален ключ; ТА 11 – криптографски алгоритъм;
KS– сеансов ключ; RAND 1 – случайно число; DCK1 – ключ за шифъра;
RES1 - стойност на отклика

След това сеансовият ключ KS и кодът RS се предават на базовата станция. Чрез тях базовата станция генерира случайното число RAND1 и го предава на мобилната станция съвместно със случайното число RS. Мобилната станция на основа на случайното число RAND1, сенасовия ключ KS и ключа за шифъра DCK1 изчислява числото RES1 съгласно алгоритма ТА12. След това кодът RES1 се предава на базовата станция и се сравнява с очакваното число XRES1, което се изчислява в базовата станция. Завършването на автентификацията произтича при условие, че е налице съвпадение на RES1 = XRES1. В противен случай абонатът получава отказ за обслужване.

По аналогичен начин протича процедурата по автентификацията и на група абонати. Различното в случая е, че вместо алгоритмите ТА11 и ТА12 се използват сертифицираните алгоритми ТА21 и ТА22.

За обмен на данни станциите използват единна парола, която може да бъде както фиксирана, така и да се променя и задава в зависимост от вида на данните. Тази парола се включва от предаващия абонат в тялото на съобщението, след което на приемната страна се извлича от приетото съобщение и се сравнява с оригиналната парола, в резултат на което се взема решение за достоверността на съобщението.

Криптиране на информацията в TETRA

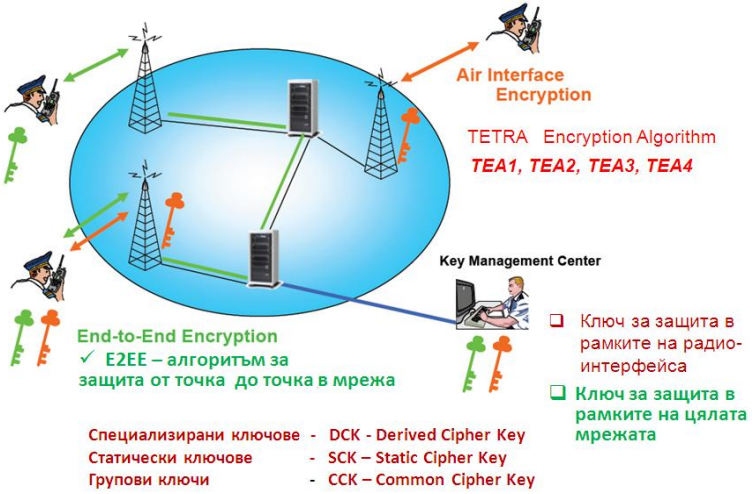
Стандартът осигурява две нива на безопасност на свръзката чрез криптиране/шифриране на информацията в канала за връзка:

1. Стандартно ниво, използващо криптиране с помощта на радиоинтерфейса на системата- AIE (Air Interface Encryption) - аналогично в системите за клетъчна връзка GSM.

2. Високо ниво на шифриране - E2EE (End to End Encryption - от източника до получателя), осъществявано чрез специални видовеалгоритми.

Криптирането чрез радиоинтерфейса - AIE се осъществява в системата на промеждутъка между абонатния терминал и базовата станция, като вътре в радиосистемата информацията се предава в «открит» вид.

При високото ниво на криптиране от «точка до точка» информацията в цялата мрежа се предава в криптиран вид (фиг. 5).



Фиг. 5. Илюстрация на методите за криптографска защита в TETPA

Криптирането чрез радиоинтерфейса се осъществява с алгоритъм за шифриране TEA (TETRA Encryption Algorithm). Освен него, допълнителна защита на данните в случая се получава и за сметка на непрекъснатото превключване на информационните канали и каналите за управление по време на сеанса за свръзка.

Стандартът TETRA предвижда 4 нива на шифриране с алгоритъма TEA:

- TEA1 –за комерсиално приложение вътре в Европейския саюз (ЕС);
- TEA2 – за служби на обществената безопасност на ЕС;
- TEA3 – за служби за обществената безопасностизвън пределите на ЕС;
- TEA4 –за комерсиално използване извън пределите на ЕС.

Тъй като при стандартното ниво информацията в мрежата се предава в открит вид, бързодействието на мрежата е високо, но защитеността на трафика на информацията е сравнително ниска.

При работа с ниското ниво на защита в TETRA се използва поточно шифриране, при което се генерира псевдослучайна кодова последователност (зависеща от ключа DCK) и се сумира побитово с потока от данни. Знаейки ключа DCK и инициализиращия вектор IV (Initial Vector), приемащата страна може да генерира същата псевдослучайна кодова последователност и чрез сумирането ѝ по модул 2 с приетото съобщение се осъществява декриптирането.

За осигуряване на висока степен на защита и конфиденциалност на информацията, в TETPAсе използва високото ниво на шифриране - от точка до точка E2EE

(End to End Encryption), осъществявано програмно, както със стандартни, така и със собствени алгоритми за криптиране. Освен софтуерно, в TETRA се прилага и канално апаратно шифриране, както и комбинация от канално шифриране + софтуерно криптиране.

Повишаването на степента на защитеност и конфиденциалност на свръзката съществено се отразява на скоростта на предаване на информацията в радиоканала [8]. В случаите на шифриране само на говора, поради ниската скорост на информационния поток е възможно прилагане на сложни алгоритми за кодиране и криптиране. Такава криптозащита осигурява почти пълна защита на разговорите от несанкционирано подслушване. При предаването на данни степента на безопасност се избира от абоната в зависимост от изискването за бързодействие на предаване на данните в канала, табл. 1.

Таблица 1:

Ниво на защита	Брой на използваните тайм-слотове			
	1	2	3	4
Без защита	7,2 Kbit/s	14,4 Kbit/s	21,6 Kbit/s	28,8 Kbit/s
Ниско	4,8 Kbit/s	9,6 Kbit/s	14,4 Kbit/s	19,2 Kbit/s
Високо	2,4 Kbit/s	4,8 Kbit/s	7,2 Kbit/s	9,6 Kbit/s

За защита на информацията и данните в TETRAсе използват следните видове ключове:

- Специализирани ключове (DCK - Derived Cipher Key), служещи за организация на point-to-point защита
- Статични ключове (SCK – StaticCipherKey), които се прилагат за ограничена защита на сигналите за сигнализация в системите, които функционират без явна автентификация.
- Групови ключове (CCK –CommonCipherKey) използвани за шифриране на информацията при груповоповикване.

III. Заключение

В заключение може да се каже, че стандарт TETRA отговаря на всички изисквания, предявявани от службите за обществена безопасност по отношение на конфиденциалността на информацията и достъпа в мрежата. Той предлага както стандартни алгоритми за криптографска защита, така и възможност за създаване на индивидулни такива за предаване на секретна информация и данни от особено важно значение.

Литература:

1. Стандарт на Европейския институт за стандартизациия в областта на комуникациите (ETSI) EN 300 392-1 V1.3.1 (2005-06). Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design.

2. Технически отчет на Европейския институт за стандартизация в областа на комуникациите (ETSI) ETR 300-1 «Terrestrial Trunked Radio (TETRA);Voice plus Data (V+D);Designers' guide;Part 1: Overview, technical description and radio aspects».

3. Концепция на ДКИС за развитие на комуникационните и информационни системи в МВР до 2020 г. Утвърдена от министъра на МВР на 08.07.2014 г.

4. Тренов, Й., Комуникации – принципи, системи и мрежи, С.,“Техника“, 2011.

5. Ненов, Г., Бичев, Г. Въведение и основи на телекомуникациите, /електронен учебник/, С. „Нови знания“, 2013.

6. Пасарелски, Р., Универсални мобилни телекомуникационни системи, Ун. изд. „НБУ“, 2012.

7. Чивилев, С., Стандарт профессиональной радиосвязи TETRA. Преимущества и возможности, (http://citforum.ru/nets/articles/tetra/)

8. Молдовян, АА. Криптография. Скоростные шифры. Санкт-Петербург, „БХВ-Петрбург“, 2009 г.

КОМПЮТЪРНА СИГУРНОСТ И ИНФОРМАЦИОННА ЗАЩИТА НА КОМПЮТЪРНИ СИСТЕМИ И МРЕЖИ

Михаела Й. Йотова
Васил В. Иванов **Николай Пл. Маринов**

Михаела Йотова - гр.София кв.Младост 4 бул."Александър Малинов" №1; тел: 0876886665; email: mi6etuu@abv.bg
Николай Маринов – гр.София кв.Младост 4 бул."Александър Малинов" №1; тел: 0889868198;email: niki94_1993@abv.bg
Васил Иванов – гр.София кв.Младост 4 бул."Александър Малинов" №1; тел: 0899688415;email: unknown_alfa@abv.bg

THE PROTECTION OF INFORMATION IN COMPUTER SYSTEMS AND NETWORKS

Mihaela Yotova
Nikolay Marinov **Vasil Ivanov**

Abstract: *Inthe report are presented terms connected with the informational security and its models. Described are actions for protecting the information from main dangers and their effectiveness, also the standarts for managing the security. We also consider the obligations of the Directorate "Communication and Information systems" and their contribution to the security of networks used by Ministry of Interior.*

Keywords:*computer, information, protection, threats, security policy*

I. Въведение

Информационна сигурност е защитата на информацията и информационните системи от неоторизиран достъп, използване, разкриване, промяна, прочитане, запис и унищожаване. В доклада са описани основните заплахи за информационната сигурност, мерките за защита и принципите за изграждане на система за защита.

II. Изложение

Термините информационна сигурност, компютърна сигурност и защита на информацията често и неправилно се използват, като синоними. Тези термини са свързани и имат общи цели, като конфиденциалност, интегритет и достъпност на информацията, но има разлика между тях.

• Информационната сигурност е защитата на информацията, независимо от нейната форма – електронна, отпечатана или други.

• Компютърната сигурност се фокусира върху коректната работа на компютърните системи и мрежи и обработваната от тях информация.

• Информационна защита са практиките по управление на рисковете, свързани с използването, работата, съхранението и предаването на информацията, както системите и процесите използвани за тези цели.

В днешни дни огромна част от информацията се събира, обработва и съхранява в електронна форма в даден етап от жизнения си цикъл. Това е причината компютърната сигурност и информационната защита на компютърните системи и мрежи и използваната в тях информация да е един от основните елементи на информационната сигурност.

Модел на информационната сигурност

Най-използваният модел на информационна сигурност включва три основни компонента – конфиденциалност, интегритет и достъпност, като съществуват и други модели, които разширяват посочения.

• Конфиденциалност

Представлява предотвратяване разкриването на информация на неоторизирани лица или системи. Нарушаването на конфиденциалността може да има много форми:

- надничане в компютърен екран при наличие на чувствителна информация
- кражба или загуба на мобилен компютър или флаш памет
- предаване на некриптирани данни през компютърна или телефонна мрежа, когато няма физически контрол върху преносната среда, това включва публични телефонни мрежи, интернет, некриптирани виртуални частни мрежи.

• Интегритет

Това е невъзможността за промяна на информацията без разрешение. Интегритета е нарушен, когато служител несъзнателно или съзнателно изтрие или унищожи важна информация (файл), когато вреден софтуер зарази компютър, когато служител или външно лице има възможността неоторизирано да промени чувствителна информация.

• Достъпност

Представлява възможността информацията да бъде достъпна, когато е необходима. Компютърните системи, които обработват и съхраняват информацията, техническите мерки за защита и комуникационните канали, използвани за предаването и да работят коректно. Т.е. прекъсването на ток, техническите проблеми, свързани със софтуер и хардуер, както и подновяването или смяната на техника или софтуер да не прекъсват работните процеси, свързани с обработка и съхранение на информацията.

Управление на риска

Управлението на риска е процес по установяване на уязвимостите и заплахите, свързани с дадена организация и бизнес процесите, както и мерки за редуцирането на този риск до приемливи нива. Той е важна част от защитата на информацията.

Управлението на риска и сигурността са непрекъснати процеси, а не еднократен акт. Инсталирането на нов софтуер, хардуер или друга система ще повиши нивото на сигурност, но няма да ви предпази ако не се извършва постоянен контрол, мониторинг и адаптиране на тези системи към новите уязвимости и заплахи.

Мерки за налагане на информационна сигурност

• Административни (организационни, процедурни) мерки

Тези мерки включват одобрени политики, процедури, стандарти и указания. Те информират персонала, какво трябва и какво не трябва да прави при всекидневната си работа. Нормативната база и регулации също са тип административни мерки. Пример за такива мерки са политиките за сигурност. Тези мерки формират базата за техническите и физическите мерки.

• Логически (технически) мерки

Тези мерки включват използването на софтуер, мониторинг и контрол на достъп до информацията и компютърните системи. Примери за това са пароли, антивирусен софтуер, защитни стени, контроли за достъп, криптиране и други.

Важен логически контрол са ограничените права при използване на компютърна система. Чрез ограничаване на правата на всеки потребител, програма или системен процес се предоставят само необходимите права за изпълнение на определените задачи. Пример за нарушаването на този принцип е използването на компютър за всекидневни задачи с администраторски права.

• Физически мерки

Тези мерки включват мониторинга и контрола над работната среда. Контрол на достъп, видео наблюдение, алармена инсталация, системи за противопожарна охрана, заграждания и жива охрана са пример за такива мерки. Важен аспект от защитата на информацията при обработката и съхранението и в компютърни системи и предаването и в локални мрежи е физическата защита на кабелната система, комуникационното оборудване, сървърите и работните станции от неоторизиран достъп.

Класификация на информацията

Елемент от информационната сигурност и управлението на риска е оценката на информацията и дефинирането на процедури за защитата в зависимост от тази оценка. Информацията е различна от гледна точка на стойността и за дадена организация, като различната информация предполага различни мерки за защита. Това предполага класифициране на информацията и създаването на организационни документи, които да описват съответните грифове и критерии за класификация, както и необходимите мерки за защита за всяка класификация.[1]

Примерна класификация за частни организации и организационни мерки за защита в компютърни системи и мрежи:

– публична информация – може да се обработва, съхранява и предава свободно;

– служебна информация – може да обработва, съхранява и предава само върху компютърни системи и мрежи и електронни носители (твърди дискове, флаш памети) собственост на организацията; не се разрешава публикуване и предаване (електронна поща, чат клиенти) в Интернет или други публични мрежи без разрешение;

– конфиденциална информация – може да се обработва, съхранява и предава само върху компютърни системи и мрежи собственост на организацията, които не са свързани с Интернет или други публични мрежи; забранява се записа или съхранението върху преносими електронни носители без одобрено за организацията криптиране; забранява се публикуване и предаване в Интернет или други публични мрежи без разрешение и без одобрено за организацията криптиране;

Добра практика е освен грифове в съдържанието на самите документи да има и политика за имената на файловете и/или съхранението на тези файлове да се извършва в отделни папки според класификацията.

Защита в дълбочина

Информационната сигурност трябва да предвижда защитата на информацията през целия и жизнен цикъл от първоначалното и създаване, до унищожаването и. Тя трябва да е защитена когато е в движение и когато се съхранява. За да бъде

защитена във всяка фаза от жизнения си цикъл трябва да съществуват различни механизми за защитата. Всяка система е сигурна, колкото е сигурно най-слабото й звено. Чрез използването на защита в дълбочина, при пропуск в дадени елемент, другите предприети мерки биха предоставили необходимата защита на информацията.

Пример на защита в дълбочина:

- Защити на ниво мрежа
- Защити на ниво хост (сървър, работна станция)
- Защити на ниво приложение
- Защити на ниво данни

Управление на сигурността

Защитата на информацията е екипно усилие и неделима част от всеки бизнес. Тя изисква участието и поддръжката на всички служители на дадена организация, както и одобрението и подкрепата на мениджърския екип. Трябва да бъдат въведени и наложени съответните организационни мерки, като всички служители съвестно да се запознаят с тях и да ги изпълняват, а мениджърския екип на всички нива трябва да следи за това изпълнение. Всички трябва да разберат изискванията и да се придържат към тях.

Служителите, чиито служебни задължения включват информационната защита и техническото осигуряване на компютърните системи и мрежи трябва да имат план за реакция при настъпване на аварии, в това число и план за възстановяване след срив.

Стандарти

ISO 27001 – Системи за управление на сигурността на информацията

Този международен стандарт се отнася за всички видове организации (например търговски предприятия, правителствени агенции и организации с идеална цел). Този международен стандарт определя изискванията за създаване, внедряване, функциониране, наблюдение, преглед, поддържане и подобряване на документирана информация с оглед на общия риск, свързан с дейността на организацията. Той определя изискванията за внедряване на механизми за контрол по сигурността, пригодени към потребностите на всяка организация или части от нея.

ISO 27002 – Кодекс за добра практика за управление на сигурността на информацията

Този международен стандарт дава указания и общи принципи за внедряване, поддържане и подобряване на управлението на сигурността на информацията в дадена организация. Целта му е да се предоставят указания за общоприетите насоки при управление на сигурността на информацията. [4]

Целите по контрола и механизмите за контрол в този международен стандарт се предвижда да бъдат внедрени така, че да отговарят на изискванията, определени чрез преценяването на риска. Този международен стандарт може да служи като практическо указание за разработване на стандарти за сигурност на информацията в организацията, ефикасни практики за управление на сигурността и да подпомогне създаването на защита на служебната информация за вътрешноорганизационните дейности.

Основни заплахи за сигурността на информацията

• Вреден софтуер - софтуер, който работи без знанието и информираното съгласие на потребителите на дадена компютърна система. Това включва компютър-

ни вируси, червеи, троянски коне, софтуер за шпиониране и други. Легитимен софтуер, като системи за архив, системи за отдалечена техническа поддръжка и системи за мониторинг на персонала, също могат да се използват като вреден софтуер, ако бъдат скрити от потребителите. Компютърна система може да бъде заразена с вреден софтуер нецеленасочено при посещаване на интернет страници, отваряне на писма и прикачени файлове от електронна поща и чат клиенти, използване на преносими електронни носители, използване на споделени ресурси в компютърна мрежа, инсталиране на заразен легитимен софтуер и т.н. Само с използването на антивирусен софтуер не може да се гарантира защита поради факта, че антивирусните софтуери работят основно с бази данни (дефиниции) на вече разпространен вреден софтуер.

За приемливо ниво на защита от вреден софтуер трябва:

- използваният софтуер за всеки отделен компютър да е предварително определен и свързан само със служебните задължения на потребителите;
- да се използват ограничени права при работа с компютрите, като само определени лица трябва да имат достъп до администраторските акаунти, така че единствено те да могат да инсталират системен софтуер и да променят системни настройки;
- да има правила (заложени в политиката за сигурност), кой, кога и с чия санкция може да инсталира нов софтуер;
- да са инсталирани всички кръпки (пачове), свързани със сигурността на използвания системен и приложен софтуер;
- да се използва антивирусен софтуер с актуални дефиниции;
- да се извършва централизиран и непрекъснат мониторинг на антивирусния софтуер и другите използвани софтуери за сигурност.

Могат да се прилагат и допълнителни мерки :

- един път в месеца ръчно да се извършва проверка на всички или на случайно избрани компютри, по предварително подготвена процедура, на инсталирания софтуер, стартираните процеси и други;
- технически да се забрани стартирането на различен от предварително одобрения и инсталиран вече софтуер;
- да се извършва мониторинг на трафика в локалните мрежи.

• Нелоялни служители - съзнателно се стремят да навредят на конкретния бизнес или работодател. Такъв служител може да отпечата или запише и изнесе чувствителна информация, до която има достъп; да даде на външни технически грамотни лица, физически или отдалечен достъп с помощта на софтуер и/или хардуер, до компютърните системи и мрежи на организацията.

Най-голяма е опасността от нелоялни служители, чиито служебни задължения включват информационна защита и техническо осигуряване на компютърните системи. Те или имат или лесно могат да получат неоторизиран достъп до цялата информация.

За приемливо ниво на защита от нелоялни служители е нужно:

- чувствителната информация да се съхранява на сървърите на организацията и/или на отделни компютри, за които са въведени по-строги мерки за защита;
- да се ограничи физическият достъп до помещенията със сървърите/компютрите;

- да се създаде структура от папки със съответните контроли за достъп (кой, до коя папка/файл има достъп), като се вземе под внимание принципа „необходимост да се знае“;
- да се въведе задължително използване на пароли за достъп до компютърните системи и услуги със съответните правила (заложени в политиката за сигурност);
- за системите и услугите, които обработват чувствителна информация да се извършва непрекъснат запис на всички събития, свързани с достъпа до тези системи, услуги и информацията, която обработват;
- да има правила (заложени в политиката за сигурност) – кой, кога и с чия санкция може да извършва, технически действия свързани с кабелната система, комуникационното оборудване, сървърите и компютрите;
- да се въведе адекватна защита от вреден софтуер.

Могат да се прилагат и допълнителни мерки:
- да се въведе софтуер за мониторинг на персонала;
- да се използва криптиране на трафика в локалните мрежи;
- да се използват смарт карти, вместо пароли за достъп до компютърните системи и услуги;
- компютрите, определени за работа с чувствителна информация да нямат връзка с интернет или други публични мрежи;

• Човешка грешка - несъзнателно действие или бездействие на служител, което вреди на организацията. Това действие или бездействие може да е в следствие подвеждане, немарливост или незнание. Тези грешки могат да доведат до заразяване с вреден софтуер, да спомогнат действията на нелоялни или външни лица, целящи да навредят на организацията, да предизвика техническа неизправност или да унищожи информация, да разкрият чувствителна информация, както се даде достъп до нея през интернет или изгуби електронен носител.

За да се постигне приемливо ниво на защита от човешка грешка, е нужно:
- да се въведе адекватна защита от вреден софтуер;
- да се въведе адекватна защита от нелоялни служители;
- да се въведе система за автоматизиран архив;
- да има правила за работа със системите (заложени в политиката за сигурност) и да се следи дали тези правила се спазват.

Могат да се използват и следните допълнителни мерки:
- да се ограничи използването или да се въведе одобрено от организацията криптиране на електронни носители (флаш памети, мобилни компютри);

• Техническа неизправност - може да се получи в следствие на софтуерна грешка, отказ на хардуера, природно бедствие, човешка грешка, злоумишлени действия на служител или външно лице. Техническите неизправности обикновено водят до спирането на услуги и прекъсват дадени процеси в организацията. Неизправност може да доведе и до загуба на информация.

За приемливо ниво на защита от техническа неизправност, трябва:
- да се въведе адекватна защита от вреден софтуер;
- да се въведе автоматизирана система за архив;
- да се резервират и дублират всички важни компоненти на компютърните системи;
- да се изготви план за реакция при настъпване на инциденти/план за възстановяване след срив.

• Външни атаки - действията на софтуер или трети лица, които целят да навредят на дадена организация. Тези действия могат да доведат до изтичане или унищожаване на информация или до спиране на определени услуги.Това може да стане отдалечено – с използване уязвимости в операционната система, в системния и приложния софтуер, с прихващане на некриптиран трафик, с използване на вреден софтуер, с помощта на социален инженеринг.

Ето пример как принципно трябва да изглежда една мрежа:

- Собствен рутер/защитна стена.
- Подредена и документирана кабелна система и комуникационни устройства.
- Устройствата за безжична връзка трябва да имат сложни пароли (които се сменят регулярно) и да не използват остарели алгоритми за криптиране.
- Ограничен физически достъп до сървърите, ако е възможно до комуникационното оборудване и кабелната система.
- Централизирани система за идентификация/автентикация, конфигуриране;
- Всички услуги и документи, които са свързани с важна информация да се намират на сървъри със съответното резервиране и дублиране.
- Структура от папки със съответните контроли за достъп (кой до коя папка/файл има достъп), като се вземе под внимание принципа „необходимост да се знае“.
- Компютрите са с ограничени права, само софтуер, свързан със служебните задължения на потребителите.
- Необходимо е да се извършва контрол на външни лица фирми – които физически или отдалечено извършват дейност за фирмата.
- Необходимо е да има точно определено/определени лица за техническа поддръжка и ако е възможно, да има лице, което се занимава със сигурността на информацията в компютърните системи и контролира тяхната работа.
- Да има въведени разписани правила, процедури, политики, които се спазват.

III. Нормативна уредба

Задълженията на дирекция „Комуникационни и информационни системи“ са описани в чл.150ж от Правилник за прилагане на Закона на Министерство на вътрешните работи :

Чл. 150ж. Специализирана административна дирекция "Комуникационни и информационни системи":

1. изгражда и поддържа телекомуникации за управлението на МВР;

2. изгражда и поддържа в технологично отношение автоматизирани информационни системи в МВР;

3. изгражда и поддържа в технологично отношение автоматизирани информационни фондове в МВР;

4. проектира, изгражда и развива общия информационен модел за съхранение на информацията в МВР и общата система от класификатори за автоматизираните информационни системи на МВР;

5. организира взаимодействието с комуникационните и информационните системи на други държавни органи или държави, администрира връзките с националната и международните електронни комуникации, осигурява специални съобщителни средства за държавни органи;

6. изготвя проекти, планове и програми за развитие на комуникационните и

информационните технологии на МВР, в т.ч. за сътрудничество с други структури;

7. планира, организира и осъществява дейностите по защита на комуникационните и информационните системи на МВР;

8. поддържа в техническо отношение електронния портал на МВР, осигурява интернет и електронна поща;

9. планира и разпределя радиочестотния ресурс на МВР и участва в актуализирането на националния радиочестотен план; създава и поддържа номерационен план в МВР и участва в създаването и разпределението на националния номерационен план;

10. изгражда и поддържа комуникационно-информационната система на МВР за управление при кризи;

11. осъществява методическо ръководство и контрол на съответните звена в структурите на МВР по предмета на дейността си. [2]

Всеки държавен служител може да има достъп до класифицирана информация и неговата отговорност е описана в чл. 25 от Закон за държавния служител:

Защита на класифицираната информация, представляваща държавна или служебна тайна

Чл. 25. (Изм. - ДВ, бр. 45 от 2002 г.)

(1) Държавният служител е длъжен да защитава класифицираната информация, представляваща държавна или служебна тайна, станала му известна при или по повод изпълнение на служебните му задължения.

(2) Класифицираната информация, представляваща държавна или служебна тайна, както и редът за работа с нея се определят със закон (Закон за класифицирана информация). [3]

IV. Заключение

Информационната сигурност е наука и не може да се разгледа в няколко страници. Използвайки информация от интернет, много специалисти и неспециалисти биха могли да извършат първоначална оценка на състоянието на информационната сигурност в средата, в която работят. Естествено, за изграждане на професионална система за информационна сигурност е необходима помощ от професионалист.

Литература:

1. Списание Professional – Чобанов Д., брой 8

2. ПРАВИЛНИК за прилагане на Закона за Министерство на вътрешните работи - Обн. - ДВ, бр. 47 от 09.06.2006 г.; изм., бр. 24 от 20.03.2007 г.; изм., бр. 44 от 09.05.2008 г.; изм. и доп., бр. 91 от 21.10.2008 г.; изм. и доп., бр. 1 от 06.01.2009 г.; приет с ПМС № 126 от 2.06.2006 г.

3. ЗАКОН за държавния служител - Раздел II - Задължения на държавния служител - бр. 24 от 31.03.2015 г., доп., бр. 54 от 17.07.2015 г., в сила от 17.07.2015 г.

4. Евростандарти: *ISO 27001, ISO 27002;* ЕВРО СТАНДАРТ СЕРТИФИКАЦИЯ ЕООД (Copyright © Euro Standard Certification Ltd. ' 2012)

УЯЗВИМОСТИ В IPV6

Севгин Мехмед Юмер **Лидия Лефтерова**

IPV6 VULNERABILITIES

Sevgin Mehmed Umer **Lidia Lefterova**

***Abstract**: When designing Ipv6 the main issue was to solve the problem with the insufficient number of IP addresses, whereas security was left behind, which led to the same serious problems as with IPv4, and even more. The main objective of this paper is to examine the vulnerabilities of IPv6.*

***Keywords**: IPv6, vulnerabilities, security, manipulation*

УВОД

Популяризацията на интернета и нарастването на устройствата, свързани към него, след 1990та година породило един основен проблем - изчерпването на IP адресите.

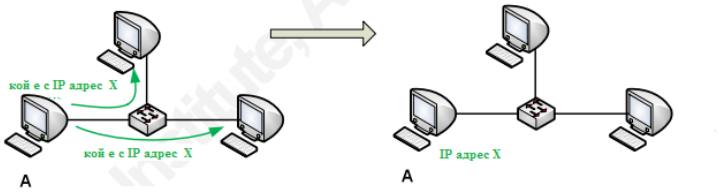
За тази цел е създаден Ipv6.

IPv6 е протокол, предназначен за идентификация на устройства в мрежово ниво.

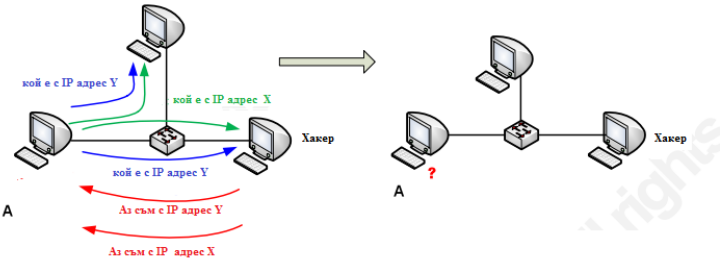
Основният проблем, е че при създаването на IPv6 е мислено главно, за да се реши проблемът с недостига на IP адресите, а сигурността е оставена на заден план, което води до наличие на същите проблеми, каквито има IPv4, че и повече.

Дублиране на адреси

За да получи компютър A IPv6 адрес и се свърже към мрежата, използва ICMPv6 протокола, което се изразява в изпращане на пакети Neighbor solicitation, към другите устройства, със запитване “кой е с IP адрес X“, ако компютър A не получи пакет отговор , компютър A приема IP адрес X за свой, а при условие, че устройството получи пакет “Neighbor advertisement“ от някое друго устройство, това означава че IP адрес X е вече зает и компютър A трябва да изпрати нов Neighbor solicitation, с друг IP адрес и така докато компютър A получи IP адрес, който не се дублира.

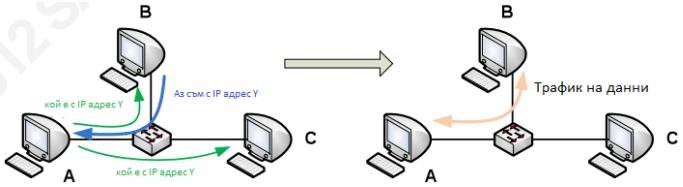


Този алгоритъм позволява неговото манипулиране. Евентуален хакер да отговоря с Neighbor advertisement, че предлаганият IP адрес се използва от него, при което жертвата не може да получи IP адрес и да се свърже към мрежата.

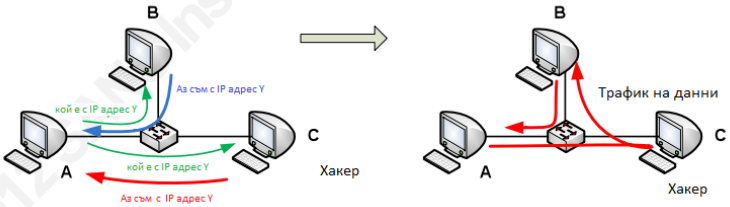


Фалшиви ICMPv6 Neighbor Advertisement

Когато компютър A иска да започне работна сесия с компютър с IP адрес Y, изпраща запитване Neighbor solicitation до всички устройства "кой е с IP адрес Y", като това съобщение се получава от всички и само въпросният компютър с IP адрес Y отговаря с Neighbor advertisement и се установява сесия между двете устройства.

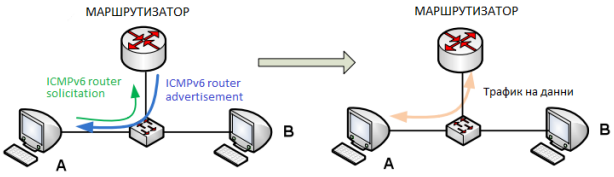


Уязвимостта се изразява в това, че и друг компютър може да се представи, че притежава същия IP адрес IPv6, като по този начин да реализира атака от вид Man in the middle и наблюдава сесията между двете страни.

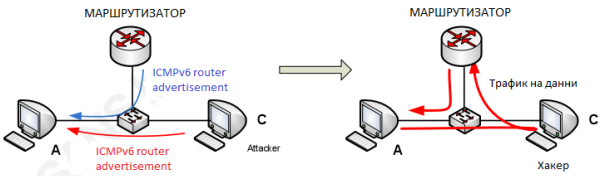


Фалшиви ICMPv6 Router Advertisement

За да получи Default Gateway и други мрежови данни, компютър А изпраща запитване ICMPv6 router solicitation до всички маршрутизатори, този който е най-близо отговаря с ICMPv6 router advertisement, предоставяйки желаните данни на компютър А.



Уязвимостта тук е, че и друго устройство (хакерски компютър) може да се представи за маршрутизатор и да предостави съвсем друг Default Gateway на компютър А, при което да накара трафика на компютър А да преминава през него.



Заключение

В следващите години се очаква пълно навлизане на IPv6. В доклада са посочени само няколко проблема, няма гаранция, че няма да бъдат открити и други. За да се избегнат неприятните последици, е необходимо изследване на уязвимостите и предприемане на мерки за смекчаване тези уязвимости.

Източници:

http://searchsecurity.techtarget.com/
https://www.ietf.org/rfc
A complete guide to IPv6

ЗАПЛАХИ ЗА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ В НОСИМИ СИСТЕМИ ЗА ПРОСЛЕДЯВАНЕ НАЧИНА НА ЖИВОТ

Георги Н. Мазаджиев **Щилияна Р. Стоянова**

Национален военен университет „В. Левски", Факултет „Артилерия, противовъздушна отбрана и комуникационно и информационни системи"

SECURITY THREATS OF PERSONAL DATA IN LIFESTYLE SELF-TRACKING WEARABLE SYSTEMS

Georgi N. Mazadzhiev **Sthiliana R. Stoianova**

Abstract. *The security of personal data, obtained by using wearable systems of lifestyle self-tracking, is studied. The necessity to protect this category of personal data is grounded. The information security threats are analyzed connected with to the data lifecycle, the architecture of the self-tracking system, some abuses and their prevention.*

Keywords: *Quantified Self, Self-Tracking, models, personal data, risks*

Въведение

Концепцията за фитнес/**лайф тракинг**, **обхваща носими сензорни технологии за проследяване на начина на живот,** физическата активност и физиологичния статус. Авто-мониторингът се осъществява чрез постоянно носим аксесоар, оборудван със система за събиране, съхранение и обработка на информацията. Текущите резултати се наблюдават върху собствен дисплей или се изпращат към смартфон, откъдето често се преминава и към **облачна услуга**. Крайната количествена самооценка в зададена форма и в желано от нас направление може да разкрие аномалии и да създаде предпоставки за здравословна корекция на поведението.

Във философски смисъл самонаблюдението е условие за себепознание и оттам за целенасочен самоконтрол, който може да подобри жизнения статус, самоуважението и в крайна сметка усета за благополучие и щастие. Технологично подпомогнатата количествена самооценка има съществени преимущества в направленията – обективност, рационалност и мотивираност [5,7].

Фитнес-тракърите се обособиха като много успешен отделен клас носими компютризирани системи с ясна функционалност и приложения, издръжливи батерии и привлекателен дизайн. Форм факторът е клипс, лента, компактен блок или маншет/гривна (фиг. 1). Традиционната им функционалност за пасивно наблюдение се усъвършенства до интерактивна функционалност на фитнес-асистент [1].

Според маркетингово проучване на Transperancy Market Research, пазарът за носими технологии (Wearable Technologies) расте средно с 40.8% годишно с прогнозен обем $5.8 млрд. за 2018 г. и съответно 485 млн носими аксесоари за самооценка [4].

Потребителите са свикнали да споделят компромисно с доставчиците на онлайн-услуги традиционна информация за идентификация (Personally identifiable

information, PII), като: име, дата на раждане, телефонен номер, адрес, имейл адрес, парола, номера на социални осигуровки (SSNs), данни за разплащане с карти и др.

Фиг. 1. Носими системи за проследяване начина на живот

Рискът за поверителността обаче се увеличава значително с увеличаване на обема и обхвата на данните за нас. Персоналната информация, генерирана чрез услуги за самопроследяване, е със значителен обем и детайлност. Тя издава това, което правим, къде сме били и потенциално защо правим нещо. Когато допълнителната информация от проследяващите устройства се комбинира с традиционната PII, потенциалът за злоупотреба става много по-голям. Колкото повече данни се обобщават, те се трансформират в прогнозна информация за личния профил и поведение на потребителите. Това е златна мина за маркетинг, но и за киберпрестъпници.

С масовото навлизане на носими системи за самопроследяване става наложително да се анализират възникващите рискове за личните данни на потребителите. Цел на изследването в доклада е да се анализират заплахи за информационната сигурност, свързани със жизнения цикъл на данните, архитектурата на системата за само-проследяване, някои злоупотреби и предотвратяването им. На тази основа може да се обосноват подходи за тяхното ограничаване или преодоляване.

2. Анализ на заплахи за сигурността на данните при самопроследяване

2.1 Области на заплахи

Жизненият цикъл на данните, в носимите системи за само-проследяване включва три етапа: локално събиране, съхранение и обработка на данни, предаване на данни, съхранение и обработка в облачно пространство с потенциал за обратна връзка [1]. Така се очертават три основни области на риск: в устройството (локално събиране, съхранение и обработка); при комуникация; в облака (съхранение, обработка и връщане на резултатите).

1. Заплахи в носимата система за проследяване

Данните, съхранени на персонални носими системи за проследяване се отнасят за един потребител. Те са изложени на риск от зловреден софтуер, който може да открадне данни на местно ниво. За да се смекчи този риск, трябва подходящ контрол и разрешения за достъп до данните. В Android и IOS е изграден ограничителен режим, за да се предотврати интерференция на данните между приложенията. Това е възможно в случаите когато даденото устройство не е преинсталирано и не

са открити никакви уязвимости, които могат да преодолеят тези контроли. Ако локално съхранените данни са твърде важни, те трябва да се криптират.

Друг очевиден риск за локално съхранени данни е заплахата от кражбата на устройството. Много устройства за само-проследяване не предлагат начини на защита в случай на физическа кражба. Потребителите на смартфони могат поне да се възползват от заключващата функция на телефона, за да се предотврати неоторизиран достъп до данни, ако устройството бъде откраднато.

2. Заплахи при предаване на информация

Данните за един потребител или ограничен брой потребители, събрани от приложения и устройства за само-проследяване често се налага да бъдат изпращани в облака в реално време или на партиди след края на сесията на дейността. Предаването може да се осъществи директно от устройството към облака или от устройството към компютър, а след това към облака. Непряко синхронизиране може да включва използването на ниско-честотни технологии като Wi-Fi, Bluetooth, или NFC, или кабелно синхронизиране. Всички тези методи имат за разрешаване свои собствени проблеми със сигурността. По време на предаване, данните са изложени на риск от различни заплахи[2]:

- при атака „traffic sniffing“ (подслушване на трафика), атакуващите събират всички предавани данни;
- при атака „man-in-the-middle“ нарушителят се намира между приемащия и предаващия, прихваща трафика, който минава транзитно. Той може да пренапише трафика или да променя пакетите преди те да достигнат до получателя без той да разбере за това;
- при „redirection“ атаки данните биха могли да се пренасочат до грешен сървър.

Подход за смекчаване на някои от тези рискове е да се използва криптиране и автентикация на данните, които се предават. Например, при безжичната комуникация Wi-Fi, връзката може да бъде шифрована със WPAv2. За комуникация „local-to-cloud“, решения за сигурност на мрежово ниво като например TLS и VPN, трябва да се използва при ненадеждни мрежи. Според чувствителността на данните, които се изпращат, данните могат да бъдат криптирани в приложния слой.

3. Заплахи при използване на облачни услуги

Обхватът на риска за данните може да се отнася до един или до всички потребители. Един хакер може да пробие един потребителски акаунт или може да компрометира цялата система и всеки потребителски акаунт, съхраняван в нея, целейки се в системите на доставчика на услуги или в неговия персонал.

Когато данните пристигнат в облака, те се обработват и съхраняват в централната база от данни в някакъв формат. Тъй като базата от данни може да получава данни от отдалечени клиентски приложения, тя е изложена на рискове за компрометиране в по-малка или по-голяма степен от външния свят. В зависимост от конфигурацията на системата, може да има различни заплахи като[3]:

- атаки SQL injection (атака на сървърна база от данни чрез техника за инжектиране на зловредно съдържание);
- атаки account Bruteforce login (логическа атака на „грубата сила“);
- разпределена атака за отказ на услуга (distributed denial-of-service, DDoS) към даден сървър);

- атаки remote software vulnerability (дистанционна атака на уязвими точки в софтуера);
- атаки default password (атаки в системи с парола по подразбиране);
- атаки back door (атака тип „задна врата“).

Киберпрестъпниците определено са заинтересувани от лична информация, генерирана чрез услуги за само-проследяване, особено ако тя е съчетана с традиционна лична информация (PII). Може да се търси изход в използването на подобрен контрол за достъп, силни пароли, както и решения като двуфакторна автентикация (2FA) за предотвратяване компрометирането на профила. Тъй като доставчиците на облачни услуги трябва да излагат своите интерфейсни услуги към света като цяло, те са уязвими за probing (сондиране, изследване) и targeted (целенасочени) атаки от киберпрестъпниците, които желаят да получат неоторизиран достъп до данните.

Доставчиците на услуги трябва да гарантират, че техните системи са изградени и са защитени по подходящ начин. Как данните за само-нанаблюдение се управляват в облака е обикновено извън контрола или видимостта на потребителите, но те може да следят как доставчиците на услуги защитават техните данни. Потребителите трябва да търсят инициативи за защита на личните данни и сигурността (например iCloud, Fitbit, и Jawbone) и спазването на подходящи стандарти, като например PCI-DSS, HIPAA, или ISO 27001.

Доставчиците на услуги могат да криптират всички данни, независимо дали са в процес на предаване или са в съхранение, и следва да съблюдават подходящ контрол за достъп до данните – DLP(data-loss-prevention) решения могат да помогнат за предотвратяване на неоторизиран достъп и копиране на данни. Данните трябва да бъдат подходящо разделени; един потребител никога не трябва да бъде в състояние да получи достъп до данни на други потребители. Доставчиците на услуги трябва да обмислят също анонимни потребителски данни като допълнителен защитен слой. Например, ако набор от GPS координати не може да бъде свързан с определен човек или момент от време, тези данни са по-малко полезни за нападателите.

2.2. Сигурност на данните и архитектура на носимата система за само-проследяване

Колкото повече функционални възможности се добавят към една система, толкова по-сложна става тя, следователно несигурността се увеличава. Архитектурата и оттам функционалността на една система за самопроследяване може да се усложнява на три нива: самостоятелно физическо устройство, смартфон със сателитен сензорен аксесоар и накрая добавка на облачна услуга [1, 6].

1. Самостоятелно физическо устройство за сензорно проследяване на активността, локално съхранение на данните и дисплей за визуализацията им не представлява голям риск за личната неприкосновеност. Единственият риск е някой друг да разбере какво е правил собственика, ако получи физически достъп до устройството.

2. Практически значима полезност при съвременното ниво на технологиите възниква, ако фитнес/лайф тракера е интелигентен периферен модул към смартфон(фиг. 2). В този случай стандартно се поддържа функция за безжичното синхронизиране на носимата система с приложение на смартфон с по-добър дисплей и

повече място за съхранение на данни – табл. 1 [1]. За целта се използва най-често Bluetooth Low Energy - нискочестотен енергоикономичен безжичен комуникационен протокол. С добавянето на тази функция се подобрява използваемостта и функционалността, но и се въвежда риск нападателят отдалечено да придобие излъчените безжично данни. Алтернативно, атакуващите могат да съсипят механизма за безжично синхронизиране на устройството, като се опитат да проникнат в него чрез слабости в сигурността или чрез принуждаване или измама устройството да се свърже с компютър, контролиран от нападателите. Ако данните се синхронизират по кабел, съхраняването на данните за самопроследяване на друго устройство увеличава рисковия профил, тъй като данните се съхраняват на две места. В смартфона се съхранява голям обем допълнителни лични и общи данни. Така потенциалният риск, ако атакуващият компрометира данните, съществено нараства.

Фиг. 2. Архитектура „фитнес-тракер + смарфон“ и панели с резултати (Jawbone)

Таблица №1 Фитнес-тракери - синхронизация

Устройство	Polar Loop	BodyMedia FIT Core	FuelBand SE	Jawbone Up24	Basis 1	Fitbit Force
Мобилно устройство	не	не	да	да	да	да
Компютър	да	да	да	не	да	да
Лесен за синхронизация	1.5 от 5	1.5 от 5	4 от 5	3 от 5	3.75 от 5	5 от 5
Bluetooth 4.0	да	не	да	да	не	да
Bluetooth 3.0	не	-	-	-	не	не
Bluetooth 2.0	не	-	-	-	да	не
Touchscreen	не	-	-	-	не	не
Headphone Jack	не	-	-	да	-	-
Автоматична синхронизация	да	не	да	да	да	да
Авт USB синхр.	не	-	-	не	не	да
Ръчна USB синхронизация	да	да	да	-	да	не

3. Функционалността се разширява още с облачна онлайн услуга. Потребителят е синхронизирал своите данни към смартфон-приложение (което е все още в рамките на физическия му домейн), но тези данни чрез облачна онлайн-услуга могат да се предадат за съхранение, анализ и социално споделяне. Като се добави интеграция на социални медии и на API, за да се позволи на third party-разработчици(програмисти на софтуер за свободна употреба – трета страна) да изграждат приложения, базирани на данни за само-проследяване рисковете още се увеличават. За разлика от данните в домейна на потребителя, домейнът на облачната услуга е извън контрола на потребителите. Те имат ограничен контрол върху автентичността, разрешенията, достъпа и споделянето. Почти всичко останало, включително отговорността за контрол и сигурност, е предадено на доставчика на услуги, който избира как да се защитят, използват и с кого ще се споделят данните. Става ясно, че добавянето на облачна услуга в системата, става по-трудно тя да се защити като възможността за атака съществено нараства. Рисковете от нападения вече могат да идват от отдалечени места и нападателите могат да се опитат да пресекат трафика в мрежата, за да откраднат данните от отделните потребители или да се целят в доставчика на облачни услуги директно. Един компромис от доставчик на облачна услуга, който да позволи достъп до базата данни на един потребител, може да компрометира всички потребители на услугата.

2.3. Възможнни злоупотреби с лични данни от носими системи за самопроследяване

1. Кражба на самоличност

Съществува престъпна индустрия, която процъфтява чрез събиране и продажба на толкова персонални данни PII, колкото могат да придобият. Комплекти на данни за дадено лице могат да бъдат продадени на други престъпници в пакети, известни като "fullz"(жаргон за пълен пакет с лични и финансови данни). Колкото по-пълен и актуален е набора от данни, толкова по-ценен е той. Например, детайли могат да бъдат използвани за създаване на фалшиви банкови сметки за пране на пари, опити за откуп, или IRS измами чрез фалшиви данъчни декларации (*Internal Revenue Service – Данъчната служба на САЩ*).

Заплахата от кражба на данни или злоупотреба, не трябва да се възниква в една легална организация. Например нелоялни служители които за лична изгода продават информация за клиенти на трети лица. Такива инциденти могат да варират от малка кражба на данни до мащабни случаи, включващи милиони потребители.

2. Профилиране

Детайлите предоставени от потребителите на услугите за само-проследяване биха могли да позволят на маркетингови и правителствени агенции да организират и насочат действия към определени видове потребители. Профилирането е в ущърб на защитата на личните данни и човешките права, защото така лесно може да злоупотреби с определени групи или малцинства.

Застраховките вероятно са един от основните бенефициенти на данни от самопроследяване. В някои застрахователни компании работодателите въвеждат политика за увеличаване на печалбите чрез намаление на здравните вноски при позитивно поведение - водене на здравословен начин на живот.

В застрахователната практика (usage-based, telematics застраховки) проследяващите устройства са монтирани на автомобилите и натрупват данни за навиците и поведението при шофиране с оглед обоснована корекция в застрахователните вноски.

Повече време на пътя в съчетание с лоши навици за шофиране - високо ускорение, късно спиране и бързо завиване - са поведения, които отговарят на профила на агресивно шофиране. Това може да доведе не само до увеличаване на сметката на гориво и бързо износване на колата, но и значително увеличение на застрахователната вноска.

3. Локализация на потребителя

Личната информация PII, съдържаща текущи данни от проследяване местоположението на потребителя, също може да се злоупотреби за престъпни цели.

Например, достъпът до база от данни, съдържаща информация от спортно приложение за проследяване, позволява да се определи къде живее човек и кога той ще бъде най-вероятно далеч от дома си, както и дали планира почивка. Много хора намират своите домове, разбити и ограбени , защото публикуват в социалните мрежи данни за своята отдаленост от дома. С тази информация може да злоупотребят натрапници, частни следователи и правителства, според техните цели.

Полицията използва системи за засичане на скоростта на движение, за да се ограничи шофирането с превишена скорост. Ако във всички автомобили са монтирани задължителни проследяващи устройства и полицията има достъп за наблюдение местоположението и движението на превозните средства в реално време, то е възможен тотален контрол на скоростта на МПС. Последиците за неприкосновеността над личния живот при подобно масово наблюдение са твърде тежки, за да се осъществи засега то на практика. Разбира се, има много други ситуации, в които да не желаем достъп до данни за нашето местоположение.

4. Изнудване с чувствителна лична информация

Има редица приложения, които проследяват медицински или здравни дейности, свързани с телесни и психични функции. Може да се проследяват настроение, сексуална активност и дори ходене по нужда на потребителите. Едва ли някой би се чувствал комфортно да разкрие този вид информация за себе си пред света. Подобна чувствителна информация попаднала в неподходящи ръце често се използва, за да се изнудят жертвите за пари. Тъй като все повече и по-чувствителна информация се събира и предава по целия свят, рискът високо чувствителни данни да попаднат в неподходящи ръце се увеличава.

5. Корпоративна употреба и злоупотреба

Някои от продавачите в технологията за активно проследяване насърчават използването на своите устройства с корпоративни wellness програми. Ползите , които са изтъквани може да са по-евтино здравно осигуряване, намаляване отпуската по болест, намаляване разходите за здравеопазване, и дори увеличаване на производителността заради позитивното настроение на служителите, водещи по-активен начин на живот, насърчаван със системи за само-проследяване.

Въпреки добрите намерения на много от предприятията да запазят информацията за клиентите си, техните бази от данни често стават цел на киберпрестъпници, които извършват кражба на чувствителна информация. Заплахата може да произтича и от вътрешни хора с привилегирован достъп до данните, който им дава възможност да ги копират, манипулират и продават.

3. Заключение

Индустрията за технологично само-проследяване начина на живот, в това число физическата активност и физиологическия статус е във фаза на разцвет. Това обуславя от една страна позитивни очаквания за здравословна корекция на поведението за много потребители. От друга страна възниква широк спектър от сериозни заплахи за злоупотреба с личните данни, получени чрез носими системи за само-проследяване.

Основните резултати в настоящата работа са в направленията:

- Изведена е специална категория лични данни получени чрез самопроследяване - големи обеми широко-обхватна лична информация, с която може да се профилират потребители, да се прогнозира тяхното поведение и да се манипулират техните визии и решения;
- Анализирани са области на възможни заплахи според жизнеият цикъл на данните в носимите системи за самопроследяване;
- Анализирана е зависимостта на риска за сигурността на личните данни от архитектурата на носимата система за само-проследяване;
- Систематизирани са някои възможности за злоупотреба с лични данни от само-проследяване.

В редица случаи се предлагат решения за минимизация на риска за нарушаване на поверителността на личните данни от самопроследяване и недопускане на възможни злоупотреби с тях.

Литература:

1. Мазаджиев Г., Специализирани компютърни системи, Шумен, 2014.
2. Мазаджиев Г., Г. Томов, Мрежова сигурност, Издателски комплекс при НВУ „Васил Левски”, В. Търново, 2013.
3. Мазаджиев Г., Д. Дойчинов, Администриране на компютърни мрежи, Издателски комплекс при НВУ „Васил Левски”, В. Търново, 2013.
4. ABIResearch. (2013). Wearable computing devices, like Apple's iWatch, will exceed 485 million annual shipments by 2018. ABIResearch. Retrieved from https://www.abiresearch.com/press/wearable-computing-devices-like-apples-iwatch-will.
5. Deborah Lupton, Self-Tracking Modes: Reflexive Self-Monitoring and Data Practices, University of Canberra, 2014, HTML.URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2483549.
6. Mario Ballano Barcena, Candid Wueest, Hon Lau, How safe is your quantified self?, 2013, HTML.URL: http://www.thesis.xlibx.info/th-other/4687184-1-how-safe-your-quantified-self-mario-ballano-barcena-candid-wuees.php.
7. Melanie Swan, The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery, MS Futures Group, Palo Alto, California, 2013,HTML.URL:http://online.liebertpub.com/doi/pdf/10.1089/big.2012.0002.

УЯЗВИМОСТИ В МОБИЛНИТЕ КЛЕТЪЧНИ КОМУНИКАЦИИ

Трифон Р. Терзиев **Камен И. Иванов**

Висше военноморско училище „Никола Й. Вапцаров“, Варна 9026
ул. „ Васил Друмев“ 73 GSM: 0886491738 e-mail: t.terziev@abv.bg

VULNERABILITIES IN THE MOBILE CELLULAR COMMUNICATIONS

Trifon R. Terziev **Kamen I. Ivanov**

***Abstract**: GSM technology is very popular, but vulnerability of this technology was kind of taboo for last years. This report is focused mainly on security threats for the end user, which are presented by this service.*

***Keywords** : cellular , mobile , messages , communications , hacking.*

В съвременния свят почти всеки притежава мобилен телефон. От просто устройство, осигуряващо мобилност в нуждата ни да разговаряме с други хора на далечно разстояние, съвременните телефони са се превърнали в персонални компютри, побиращи се в джоба ни. Те предлагат възможности, като да побират огромни количества информация, лесни са за употреба, на достъпна цена, а малките им размери ги правят подходящи да бъдат носени навсякъде.

В срок от 15 години от 1993 до 2011 броят на мобилните устройства(GSM апарати) е нарастнал от 34 милиона на 5.5 милиарда, а броят на консуматорите на тези услуги към момента е 4.77 милиарда. На практика повече от половината население на планетата използва мобилни телефони. Логично, разкриването на слабости в технологията би имало зрелищен мащаб.

И все пак основната функция на мобилните телефони си остават разговорите и изпращането на кратки съобщения (SMS-и). Но до колко те са защитени и представлява ли предизвикателство бързото развитие на технологиите и достъпността им, GSM-устройствата да бъдат лесно компрометирани, следени и подслушвани ? - Отговорът е ДА!

По същество GSM (Global System for Mobile Communications) е стандарт, започнал развитието си в 80-те години на миналия век и придобил популярност в началото на 90-те години. Съществуват няколко поколения на технологията:

-1G – първата версия на GSM която била аналогова. Позволява единствено използване на услугата за гласова комуникация между устройствата;

-2G – използва се широко и до днес. Заместител на 1G. Първоначално се използва единствено за пренос на глас, но в последствие е доразвита до 2.5G, която позволява и пренос на данни;

- 3G – аналогична на 2G, но с доста по-големи възможности за пренос на данни, осигуряваща по-високи скорости;

- 4G(LTE) – най-съвременната версия на технологията, придобила широка употреба, осигуряваща в пъти по-бърз пренос на данни от предшественика си.

Технологията използва мобилни устройства в които се поставят СИМ карти, позволяващи им да се свържат с наличните наземни (стационарни) клетки, които изграждат телекомуникационна мрежа.

Фокусът на настоящия доклад е насочен към услугата гласова комуникация, предоставяна от технологията и възможностите за изпращане на кратки съобщения чрез тях (SMS).

Без да се разглежда в подробности архитектурата на този тип комуникации се вижда, че предвид същността на технологията, факта че е безжична, сигурността на потребителите й е пряко зависима от начина, по който се предава информацията от мобилните устройства към клетките.

Съществуват различни методи за подслушване на тази комуникация, които са широко известни, като хардуерни устройства, които се прикачат допълнително към устройството или зловреден софтуер. И двете изброени могат да бъдат използвани за откриване на човека или организацията, която извършва подслушването, и в повечето случаи могат да бъдат спрегнати като активни средства за подслушване. Но какво би се случило, ако някой улавя сигналите от устройството-клиент и записва трафика му. На практика това е възможно, но поради криптирането на сигнала се смята, че предаваната информация е защитена. Това съвсем не е така.

С развитието на електронните устройства все по-голяма популярност набират така наречените SDR(Software Defined Radio). Те разполагат с множество предимства пред традиционните радио приемници / предаватели. На първо място те са много по-евтини и достъпни, ако е нужно те да бъдат променени и профилирани в даден диапазон това става много лесно само чрез промяна на софтуера им, лесно и евтино могат да бъдат подобрени, сравнително малки са по размер, а приетите чрез тях сигнали лесно могат да бъдат записани и обработени на почти всеки съвременен компютър или мобилно устройство.

Инструментите за подслушване в съвремието са именно SDR-ите. Доказателство за това са нискобюджетните TB тунери с формата на флаш памет, които могат да бъдат закупени на много ниска цена и да бъдат използвани като SDR само чрез инсталиране на необходимите драйвъри на всеки един компютър.

Практически всеки телефон може да бъде подслушан в няколко лесни стъпки. Естествено всяко следващо поколение на GSM технологията предоставя по-голяма защитеност, но все пак тя не е достатъчна, ако разговорът бъде записан. Подслушващия на практика трябва да знае към коя базова станция е свързано мобилното устройство, неговият идентификационен номер, както и номера на СИМ картата. Същият трябва да се намира в близост до устройството, между него и клетката. Разликата между 2G и 3G е тази, че втората е много по-добре защитена и подслушващия трябва да запише разговора за да го разкриптира по-късно. 3G технологията използва алгоритъм наречен “Kasumi”, който доказано е разбит и отново цената на необходимия софтуер е сравнително ниска, а в интернет пространството свободно се разпространява “open source” софтуер, който дава възможности за лесно сканиране, откриване и записване на въпросните комуникации.

Друга слабост на 2G е наличието на услуга в използвания от него MAP портокол. Тъй като той е асиметричен и се контролира от базовата станция, на практика може да се отвори гласов канал на подслушваното устройство, без изобщо то да е било набирано.

Стандартно всички мобилни устройства са настроени да работят на възможно по-новото поколение в GSM стандарта, тоест при възможност дадено устройство да работи в режим 2G и 3G, то по подразбиране ще избере 3G. Но в случай на смущения, отново по подразбиране мобилния апарат ще се превключи от 3G към 2G.

Начините за защита са очевидни. За да е сигурен собственикът на устройството, че то не се подслушва, трябва да се зададе работата му в режим 3G и по-висок, а за всяко превключване собственикът да бъде уведомяван. Съществуват и устройства, които динамично променят своя идентификационен номер, като по-този начин предоставят по-добра защитеност и в значителна степен затрудняват подслушването.

Кат цяло GSM устройствата са удобни и неминуемо ще бъдат част от ежедневието на всеки, но като всяка безжична технология те имат своите слабости, над които предстои да бъдат отстранявани. Известни са начини за защита, но най-ефективният естествено си остава да не се предава чуствителна информация по този способ.

Литература:

1. Computer networking , James F. Kurose and Keith W. Rose

2. Network Protocols Handbook , Javin Technologies

3. Wireless Reconnaissance in Penetration Testing, Matthew Neely, Alex Hamerstone and Chris Sanyk

МЕТОДИ ЗА АТАКУВАНЕ НА WIFI МРЕЖИТЕ И ЗАЩИТА СРЕЩУ ТЯХ

Трифон Р. Терзиев **Камен И. Иванов**

Висше военноморско училище „Никола Й. Вапцаров“, Варна 9026
ул. „ Васил Друмев“ 73 GSM: 0886491738 e-mail: t.terziev@abv.bg

METHODS FOR ATTACKING WIFI NETWORKS AND HOW TO PROTECT AGAINST THEM

Trifon R. Terziev **Kamen I. Ivanov**

Abstract *: The report is focused on vulnerability and methods for unauthorized access in access points and ways to protect end users from possible attacks in wireless networks which use WiFi technology.*

Keywords *: wifi , connection , technology , data , security*

В съвремието технологиите търпят изключително развитие. Достигнахме до фаза, в която всеки носи устройство в джоба си понякога по-мощно и по-производително от обикновен персонален компютър. Телефоните, таблетите и компютрите ни вече съхраняват информация , засягаща работата, личния ни живот, дори отговарят за обработката и съхранението на информация, засягаща живота на хиляди, дори милиони души. Това налага разглеждането на съхранението, преноса и като цяло работата с чуствителна информация да се извършва с особено внимание. Да се подобрят навиците, разпоредбите и като цяло гледната ни точка за опасността, която може да представлява всяко едно устройство съхраняващо или работещо с дигитална информация.

Друг проблем са и портоколите, с които работят устройствата. С цел подобряване скоростта на услугите, опростяване на начините, по които функционират те, за да са по-достъпни до крайния им потребител, или просто пропускането на показателя сигурност в разработването им се появяват множество слаби звена в системите осигуряващи безопасната обработка и трансфер на информация. Появиха се портоколи, подсигуряващи по-безопасен пренос на информацията в интернет, като https, sftp,ftps ssh и др. Но дали това стига за да сме достатъчно защитени ?

Фокусът на настоящия доклад е насочен именно към една широко използвана технология, която крие в себе си опасности- безжичното предаване на данни, посредством радио вълни, завоювало едно от челните места в нашето ежедневие, а именно “Wifi” технологията. По същност това представлява предаване на информация на честоти 2,4 Ghz или 5,8 Ghz, като с течение на времето са се развили до някъде ефективни начини за защита на преноса, чрез използване на усъвършенствани начини на криптиране, като WPA2 с динамични ключове, интегриращи удачно криптографията за прикриване на информацията от нежелани наблюдатели. Удобството, което предоставя тази технология, всъщност е най-голямата й уязвимост.

Методът на работа на точките за достъп, както и на устройства, свързващи се с тях, е добре известен и общодостъпен. Той не е обект на настоящия доклад, затова ще спомена само, че всяко устройство разполага с физически адрес, или MAC адрес. Също така използвайки радио вълни трябва да имаме в предвид, че излъчената от нас и към нас информация е видима за всички разполагащи с подходяща мрежова карта и софтуер. В процеса на обмен на данни всяко устройство идентифицира себе си със своя MAC адрес и по тази причина е лесно да се определи кое устройство е точка за достъп, кое устройство е клиент и кой клиент към коя точка е свързан, а също така и какво количество информация се предава между тях.

Съществуват няколко вектора на атака в зависимост от точката за достъп, нейното криптиране, дистанцията на нападателя от нея, както и с каква мрежова карта и антена разполага. Затова можем да кажем,че има три основни вектора според удостоверяването на клиента от точката за достъп, които се използват, а именно:

1) Атакуване на точки използващи WEP криптиране- създадено през 1999 представлява начин за криптиране на WiFi трансфера на информация. Алгоритъма използва 40 битов симетричен ключ. По същество 24 битов инициализиращ вектор (Initialization Vector -IV) се прибавя към 40 битовия ключ за да се създаде 64 битов ключ, чрез който се криптира даден фрейм. За всеки фрейм се използва нов случайно генериран ключ. Но това именно е слабостта на този тип критиране, тъй като набора от ключове е ограничен до 29, което е с размер на фрейма 1 Kbyte и скорост на предаване 11 Mbps означава че на няколко секунди ключовете ще започнат да се повтарят. Затова това криптиране е сравнително лесно за разбиване. Достатъчно е да се уловят достатъчно пакети за да бъде разбито криптирането и да се сдобие нападателя с паролата за точката за достъп. ;

2) Атакуване на точки използващи WPA/WPA-2 криптиране - появило се от нуждата да бъде заместено ненадеждното WEP криптиране. Доста по-времеемко за разбиване, изисква по-добра подготовка от страна на атакуващия, тъй като са необходими списъци с предварително подготвени пароли и сравнително дълъг период от време за извършване на атаката.;

3) Атакуване на точки с WPS поддръжка- това е поддръжка на точките за достъп, свързана с възможността им да бъдат безжично свързани към устройства като принтери. По същество представлява парола от двойка четирицифрени ПИН кодове, която е изключително лесна за разбиване по метода “brute force”, ако няма включени допълнителни защити, като изчакване между опитите за свързване.;

Съществуват и точки за достъп, използвани в големите организации от клас “enterprice”. При тях всяка точка се свързва до радиосървър, от който получава информация за оторизираните клиенти които могат да се свържат към нея, както и може да бъде настройвана, т.е. да се задава или променя индивидуално име и парола за всяка точка за достъп. Преимуществото на този тип WiFi е че дори да бъде придобит неоторизиран достъп до дадена точка за достъп, не се компрометира цялата мрежа и радиосървъра има постояннен достъп до настройките на точката. В такива случаи най-често самият сървър става обект на атаки за придобиване на нужните права от атакуващия.

Неоторизираното свързване към дадена мрежа на нападателя му дава изключително много възможности да навреди на устройствата свързани към същата точка за достъп. Това създава предпоставки за кражба на данни, възможност да се наблюдава интернет трафика на клиентите и дори придобиване на пълни права

над устройствата им, чрез инсталиране на зловреден софтуер. Именно затова за потребителите е изключително опасно някой да се сдобие с паролата за точката им за достъп.

Предвид начина на работа на точките за достъп съществува вектор на атака, който е изключително опасен, като той заобикаля нуждата на атакуващия да се сдобие с паролата за точката за достъп. Това се осъществява чрез създаване на клонинг на рутера, като истинския рутер бива заглушен или изведен от строя. Тази атака е известна под името “Evil Twin”. Ключово за осъществяването и е именно извеждането от строя на връзката между клиента и точката за достъп и предоставянето от страна на атакуващия на по-силен сигнал отколкото на реалната точка за достъп, както и прекратяването на връзката между клиента и точката за достъп. Точката “клонинг” може да се създаде чрез устройства като лаптопи, таблети, а вече дори и чрез смартфони. Може да се използва специализиран хардуер, като продукта на Hack5- Pineapple, или се сглоби такъв с обикновен рутер, флашнат със специфичен фирмуер.

Подобни зловреди точки за достъп, могат да бъдат използвани с различна цел. Те може да се използват като инструмент за сдобиване на нападателя с паролата до истинската точка за достъп, като на потребителя се предлага достоверно изглеждаща страница в която той трябва да попълни нужната на нападателя информация. Също така могат да се използват като инструмент за осъществяване на атака от типа “Man in the middle”. Последната дава възможност на нападателя да рутира целия интернет трафик на клиента през себе си като така може да разглежда, записва и дори манипулира съдържанието което достъпва той в Интернет.

Характерна слабост на WiFi е че поради начина по който работи, а именно като междинно звено между сървъра и клиента, същата създава предпоставки да бъде достъпена чуствителна информация. Дори да се използват криптиране, като https, ftps или ssh то е валидно за трансфера на информация от сървъра до точката за достъп и по този начин съдържанието на информацията може да бъде лесно изложено на атакуващия, ако той използва атака в която трафика се рутира през него, както в горепосочения случай.

Както беше описано, WiFi технологията има множество от слабости, които я правят опасна при изпокзването и в този вид, но естествено има начини по които тя може да бъде използвана безопасно. Така например, ако точките за достъп са междинно звено във VPN комуникацията между клиента и VPS-а, то сигурността на трафика ще е изцяло зависима от настройките на използвания сървър, чрез който може да се достъпи интернет мрежата. Дори и в случаите, когато клиентът е подложен на атака от типа “Man in the middle”, неговото устройство, както и трафика от и към него са с гарантирана сигурност, благодарение на алгоритмите, използвани при VPN.

Друга алтернатива, защитаваща мрежата, но не и клиента, попаднал под атака, е използването на допълнителните настройки в по-качествените точки за достъп, позволяващи отделянето на клиентите един от друг, като им осигурява директен достъп до интернет. Но както беше споменато, това не е цялостно решение за конкретната уязвимост, което в зависимост от статута на атакувания клиент отново може да се окаже сериозен проблем.

В заключение, безжичното предаване на информация чрез Wifi е удобство, но в същото време може да се окаже и сериозен пропуск в сигурността на клиентите.

Уязвимостта на WiFi е продукт на самата функционална същност на технологията. Тя създават предпоставки за неоторизиран достъп в мрежите, както в домовете, така и в бизнеса и държавните учреждения. Начин за противодействие на този тип заплахи е използването на допълнителни мерки, обезпечаващи сигурността на клиентите, като употреба на VPN или частични решения, като отделяне на клиентите един от друг. Естествено технологията има редица преимущества, като мобилност в сравнение с LAN мрежите и сравнително високи скорости на предаване и приемане на информацията, но употребата й все пак трябва да бъде съобразена с нуждата от защитеност на мрежата и степеннта, до която може да се позволи тя или даден клиент от нея да бъдат компрометирани.

Литература:

1. Computer networking , James F. Kurose and Keith W. Rose
2. Network Protocols Handbook , Javin Technologies
3. Wireless Reconnaissance in Penetration testing, Matthew Neely, Alex Hamerstone and Chris Sanyk
4. Hacking with Kali, James Broad and Andrew Binder

УЯЗВИМОСТИ В БЕЗЖИЧНИТЕ МРЕЖИ, ИЗПОЛЗВАЩИ СТАНДАРТ IEEE 802.11

Трифон Р. Терзиев Николай П. Николов

Висше военноморско училище „Никола Й. Вапцаров“, Варна 9026
ул. „ Васил Друмев“ 73 GSM: 0886491738 e-mail: t.terziev@abv.bg

VULNERABILITIES IN THE WIRELESS NETWORKS USING IEEE 802.11 STANDART

Trifon R. Terziev Nikolay P. Nikolov

***Abstract** : One of most popular wireless technologies in nowadays is IEEE 802.11. It is widely used in wide array of occasions, but WiFi has vulnerabilities we must be aware of.*

***Keywords**: wifi , technologies , protocol , attack , hacking*

В съвремието безжичните технологии заемат челно място относно начините, по които можем да достигнем Интернет. Във всяко едно направление на нашето ежедневие ние ги използваме под различен начин - като точки за достъп в кафенетата, университетите, летищата, домовете ни; като средства за далечна комуникация и др. Затова е важно те да бъдат достатъчно сигурни.

Безжичните технологии навлизат бързо, паралелно с развитието на Интернет. Още от началото на 90-те години на миналия век са разработени редица стандарти намерили различно предназначение за военни и цивилни цели, но един от най-масовите е “IEEE 802.11 wireless LAN” или по-известен с търговското си наименование- WiFi.

На практика са разработени няколко стандарта за WiFi: 802.11b, 802.11a,802.11g и др.

В таблица 1 са представени с главните си характеристики някои от съвременните стандарти. Съвременните устройства (рутери, аксес пойнти) обединяват два, три и повече от тези стандарти в себе си.

Таблица 1

Стандарт	**Честотен диапазон**	**Скорост на приемане/предаване**
802.11a	2.4 - 2.485 GHz	до 11 Mbps
802.11b	5.1 – 5.8 GHz	до 54 Mbps
802.11g	2.4 – 2.485 GHz	до 54 Mbps

Макар да се различават, стандартите споделят доста общи характеристики. Всички те използват един и същ протокол за свързване и разпределяне на достъпа на устройствата към точката за достъп- CSMA, или по-успешния му варянт CSMA “carrier sense multiple access/ collision avoidance”. Една и съща структура на фрей-

мовете при предаване на информация и една и съща възможност за намаляване на скоростта на предаване, в случаите когато разстоянията са по-големи.

Безжичното предаване на данни е изключително удобно, но то притежава и множество слабости и недостатъци. Те се пораждат както от начина на предаване (безжично), така и от протоколите, които се използват. Познаването на тези слабости може да е от изключителна важност в случаите, когато технологията се използва като звено от ключова инфраструктура или когато по него се предава чуствителна информация. Фокуса на доклада е насочен именно върху недостатъците на технологията които я предразполагат към невъзможност за изпълняването на нейните функции, а именно да се предава информация.

В случаите, когато технологията е единствен способ за предаване на информация в дадено звено, като част от ключова инфраструктура (безжични терминали за заплащане във вериги магазини, предаване на информация относно функционирането на машини или електроника ангажирана с охранителна дейност), заглушаването на сигнала, или влошаването на комуникацията, може да се окаже сериозен проблем.

Освен общоизвестните начини за заглушаване на безжични сигнали- чрез джамъри на определените честоти, стандарт IEEE 802.11 е податлив и на други начини по които може да му се въздейства. Един от тях е чрез използването на основния протокол CSMA/CA. Макар да са налични няколко начина за свързване на множество клиенти към една точка за достъп и управлението на предаването и приемането на информация от и към тях, създателите на стандарта са предпочели да взаимстват успешния метод, използван в Ethernet мрежите – CSMA/CD(“carrier sense multiple access/ collision detection”). Макар да са подобни CSMA/CD и CSMA/CA се различават, а също така проблем се явява и степента на “изгубена” информация при предаване на безжичните точки.

Основната разлика между CSMA/CD и CSMA/CA се крие в начина, по който те управляват и се справят с произволното свързване на клиенти и предаването/ приемането на информация. Докато алгоритъма на Ethernet мрежите “слуша” за друго предаване на информация на същия канал и в случай на налично такова- прекратява излъчването, като след даден интервал от време реинициира процеса, WiFi алгоритъма функционира по различен начин. За това има две основни причини. Първата е, че за да има възможност устройството опериращо с този стандарт да засече друго излъчване(WiFi мрежовите карти на лаптопи, таблети, смартфони и др.), то трябва да разполага със скъп и мощен хардуер, който може едновременно да получава и изпраща информация на големи разстояния, което е икономически неизгодно за производителите. Но по-важното- устройството не може да предвиди наличието на препятствия по пътя на предаването на сигнали, или наличието на скрити от него други устройства. Именно защото WiFi устройствата не използват CSMA/CD веднъж започнали да предават даден пакет от информация- те не спират докато не изпратят целия пакет, а в случаите когато не получат потвърждение, че същия е получен- те го изпращат отново.

Стандарт IEEE 802.11 разполага със начини за справяне с горепосочените слабости, но именно те се явяват и недостатъците, които откриват вектори за атака върху протокола. В случаите когато WiFi стандарта трябва да се справи с прекалено голямата загуба на пакети, поради слабия сигнал, породен от големи разстояния или наличие на препятствия по пътя на предаване- съществуват три решения:

увеличаване силата на сигнала, разпределяне на информацията на по-малки порции и проверка дали същата е получена, или комбинация от двете. Първото решение е свързано с хардуера на устройството и може да доведе до бързото изтощаване на батерията(ако има такава) и от друга страна е ограничено в зависимост от възможностите и мощностите на излъчване на устройството. Второто решение е софтуерно и е свързано с функция на 802.11 MAC портокола. При него предаващото устройство излъчва малък пакет от информацията, след което изчаква потвърждение от приемащото устройство, че е получило целия пакет, ако не получи такова изпраща пакета отново. Това може да се окаже недостатък, ако излъчвателя (мрежовата карта) на приемащото устройство няма достатъчна мощност за да излъчи потвърждение, или ако се противодейства, това потвърждение да не бъде получено.

Друг вектор за атака е решението приложено от стандарта IEEE 802.11, с проблема свързан с наличието на устройства, скрити едно от друго фиг. 2. Самото наличие на две устройства, които използват една и съща точка за достъп, а не се "виждат" е сериозен и като цяло опасен вектор на атака в случай на заглушаване на WiFi технологията. Това се проявява когато и двете устройства "виждат" точката и тъй като "не виждат", че друго устройство вече излъчва към нея, те приемат че тя е свободна и започват да изпращат информация към нея едновременно, което довежда до положение в което точката за достъп може да бъде неизползваема и за двете, поради количеството изгубени пакети породени от факта, че двете се заглушават. А факта, че стандарта използва протокол CSMA/CA означава че излъчването на което и да е от заглушаващите се устройства не прекъсва, докато целия пакет информация не бъде изпратен. Самото решение на този проблем по своему, отново се явява вектор за атака. Стандарта IEEE 802.11 оперира със свой протокол за разпознаване на устройствата и работа с тях – 802.11 MAC . Той въвежда две кратки съобщения RTS (request to send) и CTS (clear to send), които на практика "резервират" точката за достъп за даден клиент. Когато клиента излъчи RTS, точката за достъп излъчва CTS, което има двойна функция. Тъй като CTS-а е адресиран до определен MAC адрес- той едновременно казва на клиента изпратил RTS, да изпрати информацията и в същото време уведомява всички останали клиенти, че точката за достъп е заета.

Тъй като точките за достъп и клиентите излъчват информация за себе си, като собствен MAC адрес, канал, на който работят, тяхното име и още, позволява определена точка за достъп или клиент да бъдат клонирани или да се изпратят специално изработени CST или RTS пакети, като бъдат маскирани като лигитимни пакети от даден клиент или точка за достъп. Това може да доведе до влошаване на работата на мрежата или срив. Този метод не се практикува, макар да е възможен, тъй като има слабости в стандарта, които позволяват заглушаване на сигнала или нарушаване на връзката между устройствата по много по-лесен начин.

Един от най-сериозните недостатъци на стандарта IEEE 802.11 е наличието на пакет, който позволява даден клиент да бъде изключен от дадена точка за достъп (deauthentication frame). Изфабрикуването на подобен пакет отдавна се практикува, като средство за различни WiFi атаки, тъй като е лесно, не изисква достъп на атакуващия до точката за достъп(не е нужно да е свързан към нея), а също така не е необходимо и наличие на скъп хардуер за да бъде излъчен подобен пакет.

Като пример в доклада ще разгледаме устройство, програмирано със специфичен фирмуер. То е създадено като доказателство за това, че подобен тип заглушител е възможен. За целите на доклада програмирахме такова устройство и го изпитахме в наша мрежа, като отчетохме приблизителната му далечина да действие и времето му на работа в решим заглушаване със захранване от външна батерия.

Устройството е програмирано да създава точка за достъп, която предоставя интерфейс, позволяващ ни да сканираме района за активни точки за достъп. След сканиране извежда имената, MAC адресите, криптирането, канала, количеството информация предавано от и към устройствата и силата на сигнала на точките за достъп. При избор на дадена точка ни дава възможност за откриване на клиентите свързани с нея. Възможностите за атака са няколко, като те са както към даден клиент, така и към всички налични в района. Самата атака изключва единичен клиент или всички в района от точката им за достъп. Осъществяването на атаката се основава на използването на фрейм от 801.11 протокола, наречен "deauthentication frame". Това е възможно тъй като същия не е криптиран, нужно е да са известни само MAC адресите на точката и клиента, като не е нужно дори въпросното устройство да е свързано в мрежа с тях. Има и допълнителна опция, предоставена от устройството която дава възможност за "spoof" на мрежата с лъжливи точки със същото или с произволно генерирано име.

Създаването на подобнен заглушител е изключително достъпно, поради ниската себестойност на нужните компоненти, както и оупън сорс фирмуера, който може да бъде изтеглен свободно от няколко места в Интернет. То може да бъде управлявано от всякакво устройство с наличен Wifi- както компютри, така и мобилни телефони. Предвид ниския разход на енергия на платката (при максимално натоварване- около 100mA/h), свързването му към обикновена батерия с капацитет 10 000mAh му осигурява автономност около 100 часа или 4 дни. В тестовете които проведохме установихме ефективен радиус на действие около 20-25 метра. Малкия му размер позволява устройството, заедно с батерията да бъдат скрити сравнително лесно.

В заключение можем да кажем, че безжичното предаване на информация чрез Wifi е много удобно, но и в същото време може да бъде много ненадеждно. Уязвимостта на тази технология се основава в слабости на стандарта IEEE 802.11, които създават предпоставки връзката между устройствата да бъде лесно прекъсната или заглушена с маломощни и компактни устройства. Високите скорости на предаване на информация при по-новите устройства, както и широкото разпространение на технологията имат много положителни аспекти, но областите и предназначението, по което се използва трябва да бъдат добре преценени.

Литература:

1. Computer networking , James F. Kurose and Keith W. Rose
2. Network Protocols Handbook , Javin Technologies
3. The Hacker Playbook, Peter Kim
4. Hacking and Penetration testing with low power devices, Philip Polstra

ТЕРОРИЗМЪТ - ЗАПЛАХА ЗА НАЦИОНАЛНАТА СИГУРНОСТ НА РЕПУБЛИКА БЪЛГАРИЯ

Мерал М. Галиб **Христина Й. Косева**

Шуменски университет „Епископ Константин Преславски", Шумен
Факултет по технически науки
e-mail: meralmhmd@abv.bg, hristinaii_@abv.bg

TERRORISM - A THREAT TO NATIONAL SECURITY OF THE REPUBLIC OF BULGARIA

Meral M. Galib **Hristina I. Koseva**

The University of Shumen „Bishop Konstantin Preslavski'', Shumen
The faculty of technical sciences
e-mail: hristinaii_@abv.bg

***Abstract**: Terrorism has never ceased to remind yourself. Too often in the name of a cause sacrificing a lot of people to demonstrate the power and meaning of this. Constantly devise strategies to combat it, changing legislation closer punishment for perpetrators of criminal acts, but it can not eliminate it.*

***Keywords**: Strategy for Combating Radicalisation and Terrorism, Terrorism, Radicalisation*

Ключова задача с неимоверна важност и актуалност за съществуването и устойчивото развитие на даден народ, общество и държава е непрекъснатият системен и всеобхватен анализ на рисковете на различни равнища и от различен вид. Именно на основата на такъв продължаващ и постоянен системен анализ, както и последващата такъв анализ прогноза, е възможно осъществяването на съответните превантивни, т.е. изпреварващи мероприятия и действия. Последните пък следва да осигурят ако не премахване на заплахите, произтичащи от тези рискове, то поне рязко намаляване на равнището на вредно въздействие и загуби, ако евентуално тези заплахи се осъществят по един или друг начин.

Терористичните атаки от последните месеци в редица европейски държави очертават тенденция на увеличаващ се риск от терористична дейност. Няма съмнение, че това се отнася в равна степен и за България, която не е изолирана във все повече глобализиращия се свят. Това поставя следните въпроси: до каква степен са подготвени страните и в частност България да се справят с нарастващата заплаха, какво трябва да се подобри в политиките им за превенция и кои са факторите, на които трябва да се обърне сериозно внимание.

Един от основните рискове, които способстват за увеличаващата се терористична заплаха е дейността на Ислямска държава (ИД) - организация, която си поставя за цел установяване на халифат първо на територията на Близкия Изток, а след това и в целия свят. С цел да затвърди позициите си в Сирия и Ирак, тя упражнява безкомпромисно насилие и зверства срещу всички свои противници, военни правителствени сили и цивилното население. Изграденият от организацията медиен облик, пропагандата и наличието на финансов ресурс способстват за привличането и обучението на членове от цял свят. Според някои анализатори, сред бойците на ИД значителна част са европейци, като оценката на броя им варира между 3000 и 5000 души. [1]

Тепърва България ще се изправи пред заплахата от "чуждестранните бойци", които се сражават като част от ИД, когато тези хора ще започнат да се завръщат по родните си места. Мерките, които се взимат от антитерористичната коалиция срещу ИД могат да накарат голяма част от чуждестранните бойци, да се завърнат в страните си или да отидат в региони на други конфликти, където да продължат да развиват терористична дейност. Част от тях ще се опитат да преминат през България при своето завръщане, което поставя въпроса как да се справи страната ни с тях. И тук се поставя въпросът за действията, които трябва да бъдат предприети спрямо „чуждестранните бойци" – да се изолират и задържат, което би превърнало страната в обект на атаки, или да се пропускат контролирано с цел тяхното задържане на териториите на други държави. Няма единно виждане дали заловените "чуждестранни бойци" трябва да бъдат изолирани от обществото или да се направи опит за тяхната дерадикализация и интеграция. В тази връзка е важно изработването на стратегия, координирана с други държави от НАТО и ЕС.

Стратегията отразява волята и вижданията на българското правителство за политики за противодействие на радикализацията и тероризма, с по-силен фокус върху превенцията, без да се подценява значимостта и ролята на реактивните мерки. Документът обединява действащите към момента стратегически и концептуални документи в тази сфера. Стратегията за противодействие на радикализацията и тероризма (СПРТ) има хоризонт на действие до 2020 г., с междинен преглед и актуализиране към средата на 2018 г. Стратегията е отворен документ, който може да бъде допълван с нови елементи при внезапни и значителни изменения в средата за сигурност.

Стратегията за противодействие на радикализацията и тероризма се основава на българските национални интереси, определени в съответствие с Конституцията, законите на страната и на Стратегията за национална сигурност на Република България. Настоящата Стратегия съответства на Глобалната стратегия на Организацията на обединените нации за противодействие на тероризма 1, релевантните резолюции на Съвета за сигурност на ООН2 , съответните конвенции на ООН3 , както и на Стратегията за вътрешна сигурност на Европейския съюз4 , Стратегията на Европейския съюз за борба срещу тероризма5 ; Стратегията на ЕС за борба срещу радикализацията и набирането на терористи6 , Решенията на Срещата на върха за противодействие на насилствения екстремизъм7 и приетите планове за действие. СПРТ взема под внимание целите на Националната стратегия в областта на миграцията, убежището и интеграцията, Националната стратегия за интеграция на лицата, получили международна закрила в Република България, Националната

стратегия на Република България за интегриране на ромите, Стратегията за образователна интеграция на децата и учениците от етническите малцинства.

Комплексът от мерки за противодействие на радикализацията и тероризма обединява дейностите на държавните органи, институции, организации и гражданите за изграждане и използване на способности за разкриване, възпиране, предотвратяване и активно противодействие на рисковете, заплахите и последиците, породени от насилствената радикализация и тероризма.

Противодействието на радикализацията и тероризма е всеобхватна, общодържавна, общонационална и многопластова дейност с единно ръководство, планиране, финансово и ресурсно осигуряване и с децентрализирано изпълнение, при което отделните структури имат относително голяма свобода на действие при постоянна и ефективна хоризонтална координация помежду си.

Противодействието на явленията, свързани с екстремизма, радикализацията и терористичните дейности, налага обединение на всички разполагаеми и релевантни национални ресурси или такива по линия на европейската и международната солидарност. При противодействието на горепосочените негативни явления е от съществено значение взаимодействието със страните от Европейския съюз, съюзниците от НАТО и други стратегически партньори.

През последните няколко години ясно се проявява тенденция на разпространение и засилване на радикализацията и тероризма в глобален план, което засяга сигурността и интересите и на Република България. От особено значение за появата на тази тенденция са конфликтите и кризите в Близкия изток (Сирия, Ирак и Йемен), Африка (Либия, Мали, регионът около езерото Чад и Африканския рог), Южна Азия (Афганистан и Пакистан), както и политическата и икономическата нестабилност в страни от Западните Балкани.

Тероризмът е сред основните заплахи за сигурността, а също и за живота, здравето, свободите и правата на гражданите. Разпространението на оръжия за масово унищожение, нарастването на военните потенциали, глобализацията и лесният достъп до модерни информационни технологии, организираната престъпност, нелегалният трафик на хора, оръжия и наркотици; демографските, енергийните и екологичните проблеми, рисковете от технически и природни катастрофи са други източници на напрежение, които могат да се окажат в сложна взаимна причинно-следствена връзка с тероризма.

На този етап най-реалните и непосредствени рискове и заплахи за Република България от радикализация и тероризъм възникват като следствие от активността на различни терористични групировки и формирования с потенциал в глобален план, сред които т.нар. „Ислямска държава в Ирак и Леванта“ (ИДИЛ), „Ал Кайда” и свързаните с тях аналогични структури.

Наличието на голям брой чуждестранни бойци от европейски държави в състава на различни екстремистки и терористични формирования в конфликтните зони увеличава риска и заплахата срещу Република България. Завръщащите се в страните на произход джихадисти, силно радикализирани и с богат боен опит, генерират сериозни рискове и заплахи за сигурността не само на съответните държави, но и за региона като цяло, включително за Република България. Тази категория лица има повишен потенциал за пропагандиране на радикални идеи, за изграждане на логистични структури и мрежи за подпомагане на тероризма и за създаване на терористични формирования в района.

Преминаването през територията на България на чуждестранни бойци и завръщането им в страните на произход генерират рискове и заплахи за сигурността както на съответните държави, така и за България.

Рискове от радикализация за Република България съществуват и във връзка с обучението на наши граждани в религиозни образователни центрове извън страната, където се проповядва екстремистка идеология. Не може да се изключи вероятността завръщащите се у нас след обучение лица да се ангажират в пропаганда на радикални идеи и опити за реализацията им в страната.

При цялостната оценка на съответните рисковете за Република България следва да се има предвид и нарастващата обвързаност и сътрудничество под различни форми на терористичните формирования със структурите на организираната престъпност в Европа, особено в Западните Балкани. Подобно взаимодействие създава допълнителни предпоставки за засилване на радикализацията и на заплахите от тероризъм в региона.

Участието на страната в световната антитерористична коалиция поражда допълнителни рискове и заплахи за Република България и за българските контингенти в различни кризисни точки по света като потенциален обект на терористични действия.

Съществена част от генераторите на рискове за националната сигурност, и най- вече терористичните и екстремистките формирования, имат мрежова организационна структура, което ги прави много гъвкави и адаптивни. Специфичната субординирана структура на службите за сигурност и обществен ред следва да се приспособява към новите изисквания за бърза оперативна координация между отделните компетентни хоризонтални нива, с цел по-ефективно противодействие на горепосочените престъпни организации и формирования. Ако не бъде осъществено приспособяването на службите за сигурност и обществен ред, могат да се създадат предпоставки за дефицит от възможности за противодействие.

По отношение на потока от незаконно влизащи в Република България имигранти е известно, че се стремят към държави - членки на ЕС, осигуряващи стабилни социално- битови и финансово-икономически условия, но не и към връщане в страната на произход. В същото време оставащите в Република България имигранти не могат да получат в пълна степен очакваните от тях придобивки. В тази връзка степента на радикализацията на тези общности лесно може да ескалира от нулева до критична под влияние на разнородни фактори.

Според приетата Стратегия за противодействие на радикализацията и тероризма (2015-2020г.) противодействието на тероризма изисква прилагане на системни, едновременни, координирани и синхронизирани действия в четири основни сфери на дейност:

- Превенция - чрез идентифициране и предприемане на конкретни мерки по отношение на факторите, допринасящи за радикализацията на отделни лица и групи, както и да предотврати превръщането им в терористи. Дейността по превенция срещу въвличането в терористична дейност е системно свързана с дейността по превенция на радикализацията. [2]
- Защита на гражданите и обектите от критичната инфраструктура на държавата. Намаляване на потенциалната уязвимост на обществото в случай на терористична атака е от съществено значение. [3]

- Противодействие на пряка терористична активност, съставляваща реална заплаха, посредством събиране на разузнавателна информация, разследване на получени сигнали и заплахи, разбиване на терористични и екстремистки групи, разрушаване на каналите за финансиране на терористична дейност, както и недопускане на лица, съпричастни към терористична дейност, да се сдобият с оръжия за масово унищожение. Повдигане на обвинения и изправяне на терористите пред съд.
- Преодоляване на последствията от пряка терористична дейност чрез адекватна реакция на компетентните структури. [4]

Разработването на система от планове за реакция при заплаха и овладяване на последствията от осъществен терористичен акт гарантира подготовката на държавата за противодействие на терористични заплахи.

Анализите на риска от терористичен атентат и оценка на възможните щети и жертви следва да бъдат актуализирани и да са в основата на ефективно планиране и подготовка за реакция на държавните органи, гражданите и бизнеса.

С помощта на компетентните държавни структури да се изработи механизъм за оказване на съдействие на български граждани, станали обект или жертва на терористичен акт на територията на трети държави.

Създаването на национална система за реагиране при кризи е основа за ефективен отговор на терористична дейност.

Изводи:

Въпреки че рисковете от тероризъм като цяло са се увеличили, в никакъв случай не следва да се счита, че извършването на терористични актове срещу България и български граждани е неизбежно. Необходима е сериозна и многопосочна дейност на превенция и усилване на способностите на държавата за анализ и действия.

Защитата на живота и здравето на гражданите от терористични атаки е от изключително значение. Те се защитават чрез система от национална сигурност, която трябва да се изменя според обстоятелствата. Част от тази система са действията за борба с тероризма.

Литература:

1. Стратегия за противодействие на радикализацията и тероризма
2. http://znanieto.net/diplomni/details/4779/27/Отбрана,-Полиция/Борба-с-тероризма
3. http://www.mvr.bg/NR/rdonlyres/03D112AA-56ED-4203-8206-5AEE7FAAE134/0/Antiterorist_strategy.pdf
4. http://www.dnevnik.bg/bulgaria/2016/03/23/2727981_kak_bulgariia_protivodeistva_na_teroristichnite_zaplahi/
5. http://elearn.uni-sofia.bg/mod/page/view.php?id=5770
6. https://www.president.bg/docs/1390231470.pdf
7. https://news.bg/politics/za-narastvashti-teroristichni-zaplahi-u-nas-prez-2015-ta-dokladva-razuznavaneto.html
8. http://pogled.info/avtorski/Nako-Stefanov/riskovete-za-natsionalnata-sigurnost-na-balgariya.73589

НАЦИОНАЛНА СИСТЕМА ЗА УПРАВЛЕНИЕ ПРИ КРИЗИ

МЕРАЛ М. ГАЛИБ **ХРИСТИНА Й. КОСЕВА**

Шуменски Университет „Епископ Константин Преславски”, Шумен
Факултет по технически науки
e-mail: meralmhmd@abv.bg, hristinaii_@abv.bg

NATIONAL SYSTEM FOR CRISIS MANAGEMENT

MERAL M. GALIB **HRISTINA Y. KOSEVA**

The University of Shumen „Bishop Konstantin Preslavski’’, Shumen
The faculty of technical sciences
e-mail: hristinaii_@abv.bg

Abstract: *After the Cold War emphasis on security is management, prevention, prevention of crises. This question works very much in NATO. The EU has a strategy for crisis management.*

Keywords*: National System for Crisis Management, crisis, security*

Кризите като обществено явление повече или по-малко, пряко или косвено са свързани с необходимост от защита на стабилността и сигурността на държавата или на отделни области на обществения живот. По своята същност биват природни, екологични, технологични, икономически, социално-политически, военни и др.. По своя обхват се делят на локални, областни, национални, регионални или международни. Всяка криза, независимо от нейното естество, се характеризира с време, възможност за нарастване и елемент на изненада.

Съществуват множесто определения за криза, като всяко едно може да претендира за рационалност, но може би най- общото се свързва с определянето й като ситуация, съдържаща заплаха. Според едно от многото определения, тя е ситуация, определена от изменението на външните или вътрешните фактори на средата и се определя от три характерни черти:

- заплаха за основните ценности на обществото;
- крайно ограничено време за разрешаване на ситуацията;
- високо ниво на неопределеност.

Те винаги възникват и се развиват много бързо, в остър дефицит от време за предотвратяване на щетите, а като предпоставки за предизвикването им могат да бъдат природни бедствия, промишлени аварии, катастрофи и опасни замърсявания, епидемии, етнорелигиозни противоречия. гражданско неподчинение с масови

прояви на насилие, засилена дейност на местни и транснационални престъпни структури, терористични организации, агресивни военни действия на друга страна, масови бежански потоци и др. Като правило кризите съчетават различни видове кризисни ситуации.

Според Закона за управление при кризи, тя е внезапна или неочаквана промяна на установения начин на живот, предизвикана от човешката дейност, събития или природни явления, при които са нарушени или застрашени животът, здравето, имуществото на големи групи хора, територията, околната среда, културните и материалните ценности на държавата. [1]

Всички те се характеризират с/със :

- неочакваност;
- изключително висока степен на неопределеност в първоначалния момент на възникване;
- необходимост от бърза реакция;
- недостиг на време за вземане на обосновани решения;
- паника и стрес, неизбежно съпровождащи всяка криза;
- бърза ескалация на събитията;
- засрашаване живота,здравето, сигурността на хората.

Кризите се характеризират и с пространствени, времеви, комуникационни и социални параметри.

Пространствените параметри включват:

- зона на кризата;
- мястото,където тя се осъществява.

Времевите параметри се определят чрез:

- периода да действие на кризата;
- определяне на времето, през което съществуват опасности за хората при възникване на кризистни бедствия.

Социалните параметри обхващат:

- обществените настроения и нагласите на групите, засегнати от кризата.

Комуникационните параметри:

- определят се от изградените в обществото комуникационни способности за оценка и възприемане на информацията.

Управлението при кризи е съвкупност от принципни решения и мероприятия от различен характер, които се свеждат до следното:

- наблюдение на рискови фактори за сигурността;
- анализ и ранно предупреждение за възможни кризи;
- определяне на целите на управлението в конкретна кризисна ситуация;
- разработване на планиращи документи за използване на националните сили и средства и за взаимодействие с международните институции;
- подготовка на решения в хода на кризата, организиране и ръководство на действия и контрол върху резултатите от управлението на кризата;
- подготовка и осъществяване на следкризисна стратегия (програма);
- анализ на кризата и ефективността на мерките, предприети от институциите и органите;
- планиране на националната система за управление при кризи и предприемане на мерки за подобряването й.

Националната система за управление при кризи осигурява действията по предотвратяването и овладяването на кризи на територията на страната или извън нея – при изпълнение на задължения, произтичащи от международни договори, по които Република България е страна. [2]

В състава й влизат:

- органите на управление;
- центровете за управление;
- комуникационно- информационната система;
- силите за реагиране.

Системата осигурява анализ и оценка на риска, поддържане на готовност за действие, обмен на информация, ефективно използване на наличните ресурси и координация на действията на силите за реагиране при кризи при запазване на организационната им принадлежност. [3]

НСУК следва да гарантира подготовката на страната, населението и националното стопанство за защита при възникване на кризи, запазване и оптимизиране на съществуващите елементи на системата за управление при кризи, разработване на органи и механизми за дейност и в интегралната система за управление и осигуряване на съвместимост с механизмите за управление при кризи в НАТО и ЕС.

Организацията е целенасочена дейност на държавата, министерствата, ведомствата и местната администрация по поддържането в готовност на сили и средства за незабавни действия, подготовка и провеждане на операции при кризи. Тя включва мероприятия по:

- поддържане в готовност на органи, сили и средства за действия при кризи;
- непрекъснато събиране, обработване, изучаване, анализиране, обмен и съхранение на информация;
- планиране на операции при кризи;
- вземане на решения за управление при кризи;
- поставяне на задачи за изпълнение;
- организиране и поддържане на взаимодействието;
- организиране на управлението;
- организиране на всестранно осигуряване на силите;
- контрол на изпълнението на поставените задачи;
- оказване на необходимата помощ на подчинените.

Основните изисквания налагат постоянно функциониране на системата, устойчивост, непрекъснатост, оперативност, скритост.

Управлението при кризи в страната е способността на правителството, държавната и местната администрация чрез създадената ефективна управленска структура за планиране и координиране да изпълняват функционалните си задължения, като ръководят дейността на държавните органи и средства за овладяване на кризистни ситуации и насочват и координират действията на неправителствените органи и организации в тази сфера.

Във всяко ведомство се формира административно звено от ръководни и експертни кадри, за които подготовката и участието в управлението при кризи е основно функционално (щатно) задължение. Подготовката на компетентните органи се извършва по единен замисъл от национални, ведомствени, областни, общински и обектни планове.

Основните цели на управлението при кризи са следните:

- допринасяне към усилията на международната общност за премахване на рисковите фактори за сигурността и стабилността, за блокиране и разрешаване на действащи кризи и конфликти и за трайно премахване на предпоставките за възникване на такива в бъдеще;
- предотвратяване развитието на рискови фактори от различен характер в непреки и преки заплахи за сигурността на българските граждани, обществото, държавата и нацията;
- поддържане в готовност за действие на институционализирана система от органи, сили и средства за незабавно реагиране при кризи с различен характер в страната и в чужбина в съответствие с националните интереси и цели;
- управление на възникнали кризи, блокиране и предотвратяване на ескалирането им във въоръжени или военни конфликти.

Тези цели се постигат чрез създаване на система от органи, механизми, сили и средства, насочени към решаването на следните задачи:

- предварителна подготовка на държавата и системата за действие в кризисна обстановки, т.е. „превенция";
- неутрализиране или намаляване на рисковите фактори, т.е. „корекция";
- овладяване на ескалацията и разпространението на кризата, т.е. „противодействие";
- намаляване на интензивността на кризите, т.е. „редукция";
- ликвидиране на последствията, планиране и провеждане на мероприятия за предотвратяване на нови кризи, т.е. „реконструкция".

Принципите за изграждане на системата за управление при кризи са следните:

- единна система за разрешаване при кризисни ситуации;
- съчетаване на ведомствените системи от органи, сили и средства с териториалния принцип на планиране и управление при кризи;
- отговорност на длъжностните лица за разработване на планове за управление при кризи и за готовността на подчинените им органи, сили и средства;
- смесен способ за комплектуване на органите за управление и силите при ликвидиране на последствията от кризи,
- финансиране от държавния бюджет на дейностите по изграждането и функционирането на системата за управление при кризи.

Прилаганите процедури, материална, комуникационна, информационна база и органите, които ги осигуряват и използват, както и силите и ресурсите, формират механизъм за разрешаване при кризи. Ефективността на механизма зависи от организацията за провеждане на незабавен и непрекъснат процес на координиране както между компетентните държавни ведомства и органи, така и с НАТО, ЕС, ООН.

Опитът показва, че бедствията предизвикват сериозни нарушения на психическото състояние на населението, включително и сред ръководния състав, което често води до неадекватни действия и поведение и се отразява на организирането и провеждането на спасителни работи. Това налага да се усъвършенстват формите за повишаване на морално – психическата устойчивост на населението за управление на неговото поведение в критични ситуации. Цялостната дейност в това отношение по места се ръководи от местната и държавната администрация и от всички средства за масова информация. Важно условие за овладяване на психи-

ческата обстановка в критична ситуация е получаването на своевременна и достоверна информация и провеждането на широка разяснителна кампания.

Изводи:

Икономическата трансформация, глобализацията, дифузията и вездесъщността на информацията оказват съществено влияние и ще налагат промени в същността на управлението на кризи. Това предполага изключително да се залага на предварителното планиране, поддържането на определени ресурси, сили и средства за незабавно реагиране при създадена кризистна обстановка.

Процедурите за управление при кризи започват още в предкризисния и завършват в следкризисния период. Необходимо е да се реагира своевременно с провеждането на широк кръг от различни процедури, съобразени с динамичния характер на кризите.

Литература:

1. Закон за управление при кризи
2. Гочев, А. и колектив, „Ранно сигнализиране и предотвратяване на конфликти“, изд. „Албатрос“, С. 1997.
3. Христов, Ч. „Как да победим кризата“, ИК „Сиела“ 2002.
4. „Кризи и конфликти“ - изд. ВА „Г. С. Раковски“ 2004.

МИГРАЦИОННИТЕ ПРОЦЕСИ И ЗАПЛАХИТЕ ЗА НАЦИОНАЛНАТА СИГУРНОСТ НА РЕПУБЛИКА БЪЛГАРИЯ

Мерал М. Галиб **Христина Й. Косева**

Шуменски Университет „Епископ Константин Преславски", Шумен
Факултет по технически науки
e-mail: meralmhmd@abv.bg, hristinaii_@abv.bg

MIGRATION AND THREATS TO THE NATIONAL SECURITY OF THE REPUBLIC OF BULGARIA

Meral M. Galib **Hristina I. Koseva**

The University of Shumen „Bishop Konstantin Preslavski'', Shumen
The faculty of technical sciences
e-mail: hristinaii_@abv.bg, meralmhmd@abv.bg

***Abstract**: The refugee problem in Bulgaria emerged in the second half of 2013. The problem arises with the influx of refugees, mostly from Syria, the inability of the state to deal effectively with the problem and emerging social tension among Bulgarian citizens.*

***Keywords**: Refugee problem in Bulgaria, immigrants, crisis*

През есента на 2013 г. страната ни стана обект на непредвиден, непрогнозиран и неуправляем бежански поток откъм Близкия Изток и главно от Сирия, разкъсвана от военен конфликт с елементи на гражданска, етническа и религиозна война. Република България се оказа неподготвена да посрещне повече от 7 000 човешки същества, търсещи закрила, храна и подслон.

С изпълнението на Спешните мерки за преодоляване на кризата бяха създадени условия за бъдещото управление на ситуации, подобни на тази през 2013 г. Изградена бе материална база за настаняване на над 6 000 души. Бяха създадени условия за удовлетворяване на основните потребности на настанените лица (санитарно-хигиенни, основни комунални услуги, хранене), медицински грижи и достъп до процедурата за предоставяне на убежище. С придобитите мобилни съоръжения и технически средства има възможност да бъдат подготвени места за настаняване извън центровете ДАБ.

Миграционният натиск към Република България е изключително динамичен процес. При анализ на средата за сигурност се отчитат както глобалните и регионалните външни фактори, така и вътрешните процеси в областта на политиката, икономиката, сигурността и социалната сфера. Това позволява да се дефинират два основни генератора на заплахи с висок потенциал и значим риск за националната сигурност на България. Единият е свързан с последиците от кризата в Близкия Изток и липсата от страна на ЕС на напълно изградени единни системи за имигрантите (в т.ч. и бежанците) и за тяхната интеграция, което не позволява

цялостен и интегриран подход при разрешаване на проблемите. От една страна те насърчават бежанците да търсят закрила в страните от ЕС, а от друга – все още не е въведен принципът на релокация в страните-членки, на основата на обективни критерии, отразяващи техните реални възможности. Като резултат от това, европейските страни със засилен миграционен натиск, провокиран от кризата в Близкия изток, поемат непропорционален товар и непропорционални рискове за националната си сигурност.

Изхождайки от определението за национална сигурност, според което тя 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 става ясно,че миграционните вълни, които „заливат“ страната са пряка заплаха както за страната, така и за населението и по- точно за правата и свободите им като граждани на Републиката.

Държавната агенция за бежанците при Министерския съвет е агенция със специална компетентност в областта на прилагането на държавната политика за предоставяне на международна закрила в Република България. В рамките на процедурата на гражданите на трети страни (ГТС), търсещи международна закрила, се извършва регистрация, настаняване, оценка за принадлежност към уязвима група, медицинско изследване/подпомагане, провеждане на интервю/та, координация с компетентни органи и други релевантни нормативно определени дейности. По отношение на ГТС в процедура се изпълняват и мерки за културна и социална адаптация.

Дейността на ДАБ през 2016 година бе насочена към подобряване на процедурата по предоставяне на статут, увеличаването на капацитета за настаняване и подобряване условията на живот на лицата, търсещи закрила при съобразяване на определените годишни стратегически цели:

- постоянно взаимодействие с институциите на Европейския съюз (ЕС), Върховния комисар на ООН за бежанците (ВКБООН) и бежанските служби на държавите-членки на ЕС по задачи и проблеми в областта на убежището и бежанците;
- укрепване на административния капацитет и развитие на съществуващата инфраструктура за приемане и настаняване на търсещи закрила чужденци;
- предоставяне на международна закрила на чужденци в Република България по Закона за убежището и бежанците (ЗУБ) и усъвършенстване на административните производства, провеждани по молбите за статут;
- ефективно управление и усвояване на средствата от европейските фондове.

Държавната агенция за бежанците при провежда националната политика в областта на международната закрила в изпълнение на Закона за убежището и бежанците. Тя провежда национална политика в областта на международната закрила в изпълнение на Закона за убежището и бежанците. След последните промени, които се извършиха през 2015г., чрез които в страната се въведе т. нар. Директива, България напълно отговаря на европейските и международни норми. Чрез Директивата в националното законодателство на страната се въвеждат стандарти за

определяне на граждани от трети държави или лица без гражданство като лица, на които е предоставена международна закрила, за единния статут на бежанците или лица, които отговарят на условията за субсидиарна закрила, както и за нейното съдържание, което се предоставя.

Като държава членка на Европейския съюз в съответствие с европейското законодателство България е длъжна да гарантира наличието на материални условия за прием, включващи жилище, храна и облекло, административен капацитет за законосъобразна процедура и социална и културна адаптация на търсещите международна закрила.

Съгласно Конституцията на Република България чужденците, които пребивават в страната, имат всички права и задължения по тази Конституция с изключение на правата и задълженията, за които Конституцията и законите изискват българско гражданство. Гарантирано е правото на свободен избор на местожителство, придвижване по територията на страната и напускането й. Това право може да се ограничава само със закон за защита на националната сигурност, народното здраве и правата и свободите на други граждани.

По отношение гражданството, български гражданин е всеки, на когото поне единият родител е български гражданин или който е роден на територията на Република България, ако не придобива друго гражданство по произход. Българско гражданство може да се придобие и по натурализация.

България също не остана встрани от проблема. Кризата постави българската сигурност в риск, най-вече поради сухопътната граница и опасността от създаване на нов балкански маршрут през страната. Броят на хората, които навлизат незаконно в България, все още (относително) не е много висок, но съществува напрежение за бъдещето.

Тази ситуация се отрази и на преобладаващите позиции в българското общество по отношение на имигрантите, навлизащи в страната през последните три години. В определени моменти основните перспективи, проблеми и възприятия за имигрантската криза приемаха различна форма. Първоначално беше налице преобладаващо желание за подкрепа и помощ към тези хора. Постепенно обаче, българското общество като че ли се отърси от наивността и възприе една по-крайна позиция на противопоставяне на имигрантите. Това се дължи най-вече на усещането за неспособност от страна на държавата да защити сигурността на българския народ. Нещо повече, поредица от ключови фактори допринесоха за страха и недоверието към имигрантите в страната. Такива източници на страх са както битовите инциденти на индивидуално ниво: грабежи, престъпност, сбивания, извършени от имигранти, така и по-глобални фактори като състава на бежанския поток – голяма част от хората пресекли българската граница не са част от сочения за основен източник на имигранти регион на Ирак и Сирия. Особено в началото, голяма част от нелегалните имигранти идваха от Африканския континент. В допълнение, геополитическата сага, в която се превърна поведението на Турция и използването на бежанския поток като средство за прокарване на интереси и регионална дестабилизация, допринесе за все по-отрицателното настроение на българите към имигрантите в страната. С други думи, имигрантите постепенно започнаха да се възприемат не като хора, търсещи помощ (т.е. като бежанци), а като инструмент на външни влияния и ислямизация, имащ за цел да нанесе вреда както на България, така и на региона, и Европа, като цяло.

В тази обстановка различни агенции и институции периодично провеждаха свои социологически допитвания за отношението на българите към различни проблеми, свързани с бежанската криза. Бяха публикувани разнообразни статистики, мнения и заключения, като на тази основа се направиха и редица изводи. Какви са някои от основните тенденции в отношението на българите към бежанците, представени в изследвания на различни организации?

Според Държавната агенция за бежанците (ДАБ), в България от 1993 насам за бежански статут са кандидатствали общо 69 271 души. Над една четвърт от тях пристигат на българска територия след 2015: 19 737 кандидат бежанци са граждани на Афганистан, 18 665 имат сирийски гражданство, а 15 931 са от Ирак. България се възприема като транзитна дестинация за нелегалните имигранти, за които в основна цел се превърна сръбската граница и пътят към Западна Европа (и най-вече към Германия и скандинавските страни).[1]

В момента в България навлизат средно по 1500 бежанци на месец – предимно иракчани, афганистанци и сирийци. През 2015 страната ни е регистрирала 20 391 лица, които са потърсили защита от ДАБ. В края на август 2016 общият брой на бежанците, които са навлезли на българска територия, надвишава броя за цялата 2014 (11 081), а в началото на октомври надхвърля 15 100 души. Налице е тенденция основният поток от нелегалните имигранти в страната да идва от Афганистан и Ирак, и все по-малко от Сирия. От началото на 2016 в странта са пристигнали повече от 4500 афганистанци, 3000 иракчани и 1100 сирийци. Този състав на имигрантския поток повдига някои съмнения за произхода на кризата и допълнително допринася за „охлаждането“ на отношението на българите към имигрантите в страната. [2]

Информация за лицата, потърсили закрила, и взетите решения за 2017 година

Месец	***Брой лица, потърсили закрила***	*Предоставен статут на бежанец*	*Предоставен хуманитарен статут*	*Отказ*	*Спряно производство*	*Прекратено производство*	***Общ брой решения***
януари	421	34	29	243	451	765	**1522**
февруари	385	87	84	243	2108	1437	**3959**
Общо	**806**	**121**	**113**	**486**	**2 559**	**2 202**	**5 481**

В този ред на мисли, значителна част от българите възприемат като основна потенциална опасност разпространението на радикален ислям на територията на страната. Страх от ислямизъм изпитват 34% от пълнолетните български граждани.

Тези страхове се подхранват най-вече от зачестилата терористична дейност на лица свързани с Ислямска държава в Европа, както и от появата на ислямистки елементи в някои ромски квартали в страната (като тези в Пазарджишко например). С други думи, в основата на подхранването на страховете от ислямизация сред българското население стои един своеобразен синтез от външни и вътрешни фактори. [3]

Все по-отрицателните нагласи на българите към имигрантите в страната намират израз в сравнението между позициите от 2013 и тези от 2016. Налице е очевидна тенденция към увеличаване страховете на българите по отношение на имигрантите и възможното преминаване на големи мигрантски вълни през страната. През 2013 хората, които възприемат мигрантите като риск за сигурността, са били 55%, докато през 2016 делът им се увеличава до 79,4%. В допълнение, хора, които мислят, че бежанците носят рискове за здравето на местното население, е нараснал от 68% на 75%. [4]

Отрицателното отношение към имигрантите се потвърждава и от 78% от хората, които посочват, че ги възприемат като бреме за българската икономика. Според тези хора, големият брой мигранти може да доведе до финансови и икономически проблеми. Нещо повече, за много от българите, интеграцията на имигрантите е практически невъзможна поради религиозни и културни различия. Към подобна гледна точка се придържат почти 39% от пълнолетните български граждани. В допълнение към тази нагласа, около 49% от хората вярват, че българската държава е толкова слаба, че не може да осигури условия за интеграция на бежанците. [5]

Тези отрицателни нагласи се дължат на няколко основни фактора. Освен посочените съмнения за произхода на бежанския поток, геополитическите интереси и недоверието към турското поведение, налице са и други „по-вътрешни“ причини. У българите се наслоява усещането за липса на държава, която да е способна да поддържа сигурността на цялата си територия. Невъзможността да се защитят националните граници – символ, на което се превърна бавното и недотам сполучливо изграждане на оградата по турската граница – и корупцията в Гранична полиция – намерила своя най-краен израз в спечелването на обществена поръчка за превоз на бежанци от човек обвиняем за трафик на хора – допълнително допринесе за втвърдяването на позициите на българите спрямо имигрантите в страната. Усещането, че държавата е „разграден двор“, попаднал в капана на геополитическите сблъсъци в региона, доведе до проекция на негодуванието на българите към мигрантите. По този начин хора, които първоначално бяха сравнително добре настроени към пристигащите в страната ни имигранти, постепенно промениха позициите си в посока към пълно противопоставяне на този процес.

Най-крайното проявление на усещането за несигурност на българите, предизвикано от неспособността на държавата да защити територията си от нелегални имигранти, е появата на самоорганизиращи се групи – „ловци на бежанци“. В рамките на няколко месеца, отделни индивиди и групи, без каквато и да е авторизация от страна на държавата, в стила на паравоенните формирования, извършиха арести на хора пресекли нелегално границата. Част от тези арести бяха записани с камери и представени пред широката общественост. Тази незаконна

практика доведе до разделение в българското общество на „за“ и „против“ „гражданските арест“ на нелегални имигранти.

Изводи:

България е страна, която разполага с широк арсенал от методи, основани на правни и законови норми, за справяне не само с бежанците, които навлизат в териториите на страната, но и за събитията породени след възникването на т. нар. „Бежанска криза“, обхванала цяла Европа.

Като член на ЕС, България е задължена да гарантира закрилата на лица, със статут на бежанци, по начин и със средства, гарантиращи както правата и свободите на хората, така и националната сигурност.

Литература:

1. http://www.airm-bg.org/nr_bg_bg.pdf
2. https://geopolitica.eu/spisanie-geopolitika/160-2016/broi-6-2016/2545-imigrantskata-kriza-i-balgarskite-strahove
3. http://bdi.mfa.government.bg/info/Module%2004%20-%20Diplomacia%20i%20sigurnost/preporachitelna%20literatura/A.Angelov/kontzeptziq%20za%20natzionalna%20sigurnost%20na%20Bg.htm
4. http://epicenter.bg/article/Migratsionnata-valna-i-zaplahite-za-natsionalnata-sigurnost/100557/11/0
5. https://geopolitica.eu/spisanie-geopolitika/160-2016/broi-6-2016/2545-imigrantskata-kriza-i-balgarskite-strahove
6. http://enterprise.bg/together/%D0%B8%D0%BC%D0%B8%D0%B3%D1%80%D0%B0%D0%BD%D1%82%D0%B8%D1%82%D0%B5-%D0%B2-%D0%B1%D1%8A%D0%BB%D0%B3%D0%B0%D1%80%D0%B8%D1%8F-%E2%80%93-%D0%B8%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D0%B8%D1%87%D0%B5%D1%81%D0%BA/
7. http://hermesbg.org/bg/nova-biblioteka/book-55/2622-vaprosat-s-bezhantsite.html

СИСТЕМА КИБЕРСИГУРНОСТ

Марияна Ст. Тодорова

Шумен , НВУ"В. Левски", Факултует"Артилерия, ПВО и КИС"- гр. Шумен, Катедра"Информационна сигурност" , E-mail: stilianova70@abv.bg

Тодор Цв. Чолаков

Шумен , НВУ"В. Левски", Факултует"Артилерия, ПВО и КИС"- гр. Шумен, Катедра"Информационна сигурност" , E-mail: totkata97@abv.bg

SYSTEM CYBERSECURITY

Mariana St. Todorova

Todor Cv. Cholakov

Абстракт: *Киберсигурността е посветена на развитието на киберконцепцията за сигурност - от раждането на понятието "информационна сигурност" в XX век до създаването на правни, организационни основи, използващи се в армията и за политически цели. Въз основа на анализа на съответните стратегически документи, закони и наредби са видни етапите на развитие на политиките за киберсигурността. Историческия преглед на системата киберсигурност позволява да се проследи динамиката на тази система, както и уникалния фон в оформянето на международната информация и средата за сигурност.*

Ключови думи*: киберсигурност, система*

Keywords*: cybersecurity, system*

За проблема в информационна сигурност започна да се говори много преди появата на Информационни комуникационни технологии /ИКТ/. Днес те се представят, като компютърни и мрежови технологии. В края на XX - началото на XXI век след промяна на ИКТ в подходите за защита на киберпространството се използва понятието „информационна защита".

Изясняването на същността, проявите и механизмите за постигане на сигурност на киберпространството е едно от най-значимите направления на теорията и практиката на съвременността. Трябва да се посочи обаче, че въпреки безусловната значимост на проблема все още не съществува еднозначно определение на киберсигурността. Преобладаващото разбиране или я отъждествява с, или я разглежда като аспект, страна на информационната сигурност [1]. Съществуват и мнения [Грънчаров, В., 2011, с. 55], основаващи се на тоталната „кибернетизация" на съвременния свят, които настояват за тяхното разграничаване и за разкриване на спецификата на киберсигурността в системата на националната сигурност. В настоящето изследване тази позиция се възприема като по-обоснована и като изразяваща по-точно както протичащите процеси в съвременното общество, така и същността на сигурността в киберпространството.

Като се изхожда от тази позиция, може да се приеме, че киберсигурността е свързана с постигането състояние на обществото, което ще може да предотврати и отрази заплахите, като осигури превъзходство в изграждането и функционирането на виртуалното (кибер) пространството чрез необходимата за това ресурсна („киберсилата"), субектна („киберспециалисти") и институционална (държавни специализирани органи и политики и законова и нормативна база) обезпеченост. Нейното постигане е свързано с всеобхватно преосмисляне на проблемите на сигурността, формиране на адекватни, на съвременните реалности концепции и осъществяване на система от взаимосвързани практически действия. Същите са водещи към изграждане на качествено „нова архитектура" на системата на националната сигурност като цяло. Главното в това преосмисляне е възприемането и утвърждаването на формулираната теза, че „основа" и „изграждаща конструкция" на „новата архитектура" на сигурността в комуникационното общество е киберсигурността, разглеждана във всичките й измерения - технологично-информационно, правно-институционално и политическо [2].

Като пример можем да използваме терористични атаки на 11 септември 2001 г., както и все по-голямата заплаха за икономиката, която до голяма степен зависи от ИКТ. Процеса катализира в системи за модернизация на сигурността в кибернетичното пространство и съоръжения за безопасност на критичната инфраструктура. Следствие на което киберсигурност в САЩ е започнала да се променя въз основа на трансформацията си. През 2009 г. в САЩ се появява "Всеобхватна национална киберсигурност". След идването на власт на Барак Обама информационните и комуникационни технологии са били активно употребявани като инструмент под наименованието "интелигентна сила". Система Киберсигурност претърпява корекции с цел постигане по-нататъшно разделение на ролите по високите етажи на администрацията. През последните 16 години в развитието на американската политика се формира целостта при използването на нападателни и отбранителни способностите на САЩ в киберпространството. Тя провежда серия от последователни действия, като:

- На първо място, Съединените американски щати изследват състоянието на киберпространството в земя, море и въздух.

- На второ място, са разработени и одобрени редица документи, включително с конституционен характер, в които са обосновани и обезопасени основите на защитни и нападателни операции от киберпространството.

- На трето място, при отбранителни операции в киберпространството е създаден контрол на структурата и специални звена, в които са активно привличани талантливи хакери.

Администрацията на Барак Обама започна да отделя все повече внимание на киберсигурността след успешните хакерски атаки .

Лиза Монако, съветник на президента по въпросите на националната сигурност коментира следният факт: „Киберзаплахите са един от най-сериозните проблеми на нашето време. Затова ще бъде по-добре да развием нашите рефлекси в борбата с тях, както направихме в борбата срещу тероризма",. САЩ смятат, че Китай и Северна Корея участват в кибератаките срещу правителствени и частни мрежи. [3]

Развитието на защитни и нападателни способности на киберпространството, както и използването на ИКТ в сграда с политическите цели за САЩ остава прио-

ритет. Тя продължава разработването на системи за кибернетична защита. Разширяването на действието на член 5 от Северноатлантическия договор относно действия в киберпространството неблагоприятства за развитието на международната сигурност. Все още не е възможно да се определи с точност и бързо идентифициране на източника на атаки от киберпространството. Това означава, че на нарушителя може да бъде "неопределен", въз основа на политически съображения и при липсата на доказателства . [4]

В политиките за киберсигурност в САЩ най-вече се търси реформиране на системата на международните отношения по начин, който можете свободно да разпространявате своето влияние върху обществото на други държави.

В много държави се смята, че интернет определено трябва да остане пространство на свобода и на общото наследство на човечеството; всеки трябва да има право на достъп до информация и правото на свобода на изразяване. В същото време никой не може да отрече факта, че свободата не е средство за толерантност, напротив средство за действия - както във физическия свят, така и във виртуалното пространство. В световен мащаб поради отсъствие на границите информация се пренася с интерактивност скорост. САЩ провежда последователно редица взаимосвързани политически и организационни мерки за да развива и използва капацитета на ИКТ, като средство, което да повлияе на чуждестранните аудитории.

Основните направления, методите и целите на новата политика подробно е описана в програмата "четиригодишен преглед на външната политика и развитие" през 2010 година.

Използвайки основните направления и методите от примера за киберсигурност в САЩ, можем да създадем план за правилно използване на киберсигурността в много области и човешката дейност в крайна сметка прави възможно информационното пространство да окаже влияние за правилно функциониране на държавата, обществото и отделния човек.

Използването на ИКТ, за да се намесва във вътрешните работи на суверенни държави, нарушение на обществения ред, подбуждане етнически, между различни раси и между религиозна омраза, пропаганда на расизъм и ксенофобски идеи или теории, водят до омраза и дискриминация, подбуждане на насилие.

В същото време, анализ на съществуващата информация показва, че държави включват в политиките си елементи ограничаващи въздействието на информацията деструктивно върху държавата, обществото, личността чрез филтриране интернет съдържанието. Също така има международно признати документи, уреждащи ограничаването на правата и свободите на интереси на националната сигурност, включително Международният пакт за граждански и политически права (член 19), Конвенцията Права на Европейския съюз (член 10).

Индивидуални инициативи и участие на работни групи от експерти на правителства, на ООН дава напредъкът в областта на информационната и административна сигурност. Това дава основание, че в бъдеще ще бъдат разработвани и приети правила за поведение на държавите в киберпространството.

Заключение:

В резултат на активното използването на информационните технологии във всички области на човешката дейност съществува зависимост между лица, обществото и държавата, както и надеждно функциониране на информация и комуникация в системите.

Зависимостта от своя страна води до появата на качествено нови заплахи, основани на използването на присъщите уязвимости в областта на информационното общество, някои случаи несъвместими с целите на поддържане на националната и международната стабилност на сигурност. В международен план източникът на заплахата може да бъдат терористи, киберпрестъпниците, както и държавата.

Има два основни подхода за защита срещу заплахи, произтичащи от глобалното информационно пространство – киберсигурността и защита на информация. Тези подходи са взаимно изключващи се. Въпреки това, те отразяват социално-културни, икономически и политически характеристики на страните фокусирани върху изпълнението на съответния национален интерес.

На сегашния етап политиката насочва развитието на глобалната информация в средата на интернет пространството и насърчаване на техните виждания за предоставяне на киберсигурността в променящата се геополитическа ситуация и формирането на многополюсен свят, който се проявява в проблемите в процес на разглеждане в поява на групи от единомислещи страни се придържат различни гледни точки за по-нататъшното развитие на световната информация инфраструктура.

Литература:

1. Грънчаров, В., Държавната политика по защита на информацията в началото на 21 век. В: Проблеми на информационната сигурност през XXI век, Шумен, 2011, с. 55

2. Динков, Д., Виртуалните общности в постмодерния свят. Икономически алтернативи, №4, 2011, с. 12.

3. https://technews.bg

4. https://fakti.bg/

СЪЗДАВАНЕ НА СКЛАД ОТ ДАННИ ЗА ОПРЕДЕЛЯНЕ НА РИСКА ЗА ИНФОРМАЦИОННАТА СИГУРНОСТ НА КОРПОРАЦИЯТА

Имрен Ш. Исмаилова **Николай Й. Досев**

Имрен Исмаилова, Шуменски Университет "Епископ Константин Преславски",
Катедра: "Управление на системите за сигурност",
e-mail: iismailova@uni-ruse.bg
доц. Николай Досев, Шуменски Университет "Епископ Константин Преславски",
Катедра: "Управление на системите за сигурност"
e-mail: ndosev@abv.bg

CREATING A DATA WAREHOUSE MODEL IN ORDER TO IDENTIFY CORPORATE INFORMATION SECURITY RISKS

Imren Sh. Ismailova **Nikolay Dosev**

***Abstract**: This paper focuses on creating a data warehouse model in order to identify corporate information security risks. Modeling process begins with decomposing a business organization's structure using systematic approach, to observe information flows between every department. Using this information a data warehouse model is created. Every department is separate database with specific information flows, which are organized in tables.*

***Keywords:** Data warehouse, Data Base, Departments, Systematic approach*

Въведение

Създаването на склада от данни започва с извличане на знанията, които се намират „вътре" в самата организация. Необходимо е преди прилагане методологията на конкурентното разузнаване аналитикът да разполага с информация за собствената/възложилата компания [3].

Методите, които се използват за извличане на знания, са посочени на фиг. 1. Върху избора на метод влияят три фактора: личностните особености на инженера на знанията, личностните особености на експерта и характеристиките на предметната област [4]. Поради тази причина, за целите на изследването е избрано да се използват текстологичните методи, а също и провеждане на интервю.

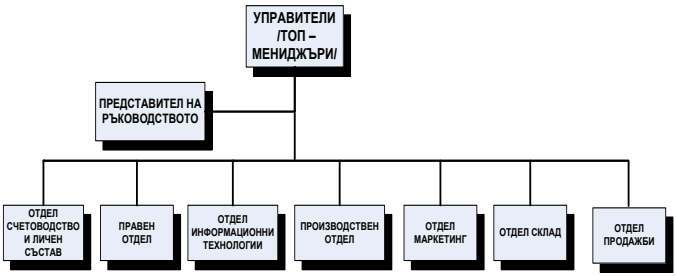
Фиг. 1. Методи за извличане на знания

Извличането на знания комбинира когнитивната психология, системния анализ, математическата логика и др. [4]. Именно системният анализ е приложен при проследяване на информационните потоци, протичащи в организацията.

Изложение

Първа стъпка от проектирането на системата за вътрешна информация е разглеждането на една най – обща структура на организацията – фиг. 2 [2,5].

Всеки един отдел, показан на фигурата се декомпозира използвайки системния анализ и подход, за да се проследят входящите и изходящите информационни потоци. Тези потоци ще бъдат използвани за създаването на бази от данни за всеки отдел.



Фиг. 2. Структура на бизнес организацията.

Следва да се отбележи, че описаните по-долу информационни потоци са приспособени към реални организации и поради тази причина може да има разминаване с теоретичната входно – изходна информация от отделите.

От гледна точка на ограничеността на фирмените ресурси е избрано да се създаде един сървър, в който ще бъдат „съхранявани" базите данни на всеки отдел.

Служителите на отделите няма да имат достъп до данните от останалите отдели с цел предотвратяване на злоупотреби.

Избрано е да се работи със система за управление на бази данни „Cronos pro", поради нейните функционални възможности.

Като пример ще бъде разгледан само Счетоводен отдел [1]. В този отдел постъпват (фиг. 3):

- фактури от външни контрагенти;
- договори с контрагенти;
- информация от складовете за наличности, покупки и продажби;
- информация от отдел продажби за реализираните продажби, съпроводени с документи - заявка, експедиционна бележка, стокова разписка, товарителница, фактура;
- информация за поръчките, възложени на организацията.

Фиг. 3. Входяща и изходяща информация от счетоводен отдел

Изходната информация от счетоводен отдел може да бъде обобщена в следните групи:

- отчет за управлението (нарича се още и „доклад за дейността") - структурата му е регламентирана от Закона за счетоводството – чл. 33 ал.1 и съдържа: „достоверно изложение за развитието на дейността и за състоянието на предприятието; важните събития, настъпили след годишното счетоводно приключване; предвижданото развитие на предприятието; дейността в областта на научните изследвания и проучвания; движението на акциите в съответствие с изискванията на действащото законодателство; друга информация по преценка на предприятието";

- справки за реализирана печалба, необходими както за статистика, така и за мениджъри, и за външни потребители на информацията;
- годишен финансов отчет. Неговата структура също е регламентирана от Закона за счетоводството – чл. 26 ал.1. и съдържа следните компоненти: баланс, отчет за приходите и разходите, отчет за капитал, отчет за паричен поток.

На фиг. 3 входящата информация в отдел личен състав е означена като „информация за работника", включваща - име, адрес, длъжност, присъствия, отсъствия през месеца, образование и квалификация, молби за отпуск, допълнителни споразумения, уведомления за сключен трудов договор, извършено количество работа за всеки един служител на организацията.

Освен нея отдел личен състав генерира:

- ведомост за работна заплата;
- рекапитулация за осигуровки;

Всеки тип входна и изходна информация представлява отделен масив от данни.

Като се използват данните от счетоводен отдел (фиг. 3), са проектирани таблиците, отговарящи на съответната входна и изходна информация.

1. Таблица „Поръчки", изобразена на фиг. 4, включва следните компоненти:

- пореден номер на поръчката;
- модел на изделието - обикновено представлява комбинация от букви и цифри и е специфичен за всяко изделие. Затова той влиза в състава на идентификационния набор, а полето има статус „задължителен", както е посочено в последната графа на таблицата;
- схема на изделието – наличието на схема не е задължително, но при повечето производствени предприятия, поръчката е придружена и със схематично изображение, затова е включена в състава на базата данни;
- съставни материали – в това поле се описват материалите, необходими за изработването на изделието. Тази графа е създадена за улесняване контрола на получените материали в склада;
- количество за изработка;
- краен срок за изработка – записва се крайния срок, в който поръчката трябва да бъде изработена. Това поле е създадено с цел улесняване организацията на производствения процес;
- дата на получаване на заявката.

Избрано е да се работи със сложен първичен ключ, в състава на който влизат полетата: име на клиента, модел на изделието и краен срок на изработка. По този начин се гарантира уникалността на записа.

Поръчки

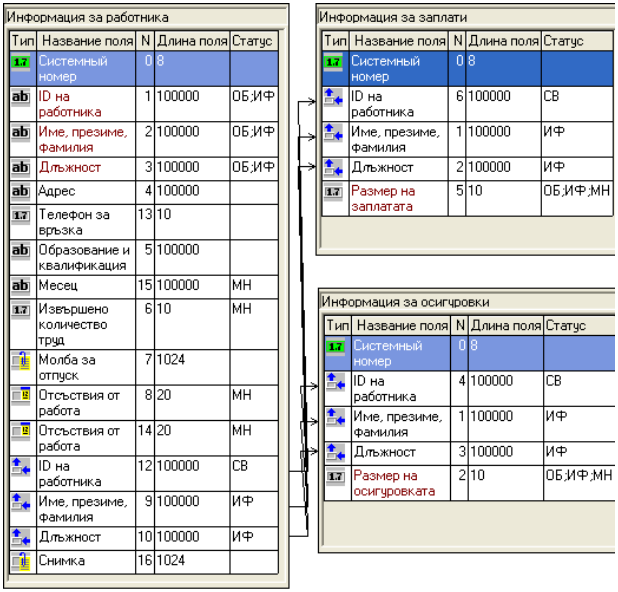
Тип	Название поля	N	Длина поля	Статус
1.7	Системный номер	0	8	
ab	Клиент	8	100000	ОБ;ИФ
1.7	Поръчка No	1	10	ОБ;ИФ
ab	Модел на изделието	2	100	ОБ;ИФ
	Схема на изделието	3	1024	ИФ
ab	Съставни материали	4	100000	ОБ;ИФ
1.7	Количество за изработка	5	10	ОБ;ИФ
	Краен срок	6	20	ОБ;ИФ
	Дата на получаване на заявката	7	20	ОБ;ИФ

Фиг. 4. Таблица „Поръчки“

2. Таблица „Информация за работника” – нейната структура е изобразена на фиг. 5. и включва следните полета:

- ID на работника – представлява уникален идентификационен набор, състоящ се от инициалите на работника и пореден номер. За тази таблица това е първичният ключ;
- име, презиме и фамилия на работника;
- длъжност;
- адрес;
- извършено количество труд –избрано е да бъде „множествено” т.е. да се състои от поле, в което да се записва съответния месец и извършеното количество труд от работника за месеца. Изготвено е по този начин, за да се прави справка при необходимост за заработката на служителя за предходни периоди;
- молба за отпуск - предвидено е като прикачен файл да се добавят молбите за отпуск на работника;
- отсъствия от работа – в това поле ще се отбелязват отсъствията от работа.

Последните три реда от таблицата служат за връзка между записите в тази таблица и таблици „Информация за заплати” и „Информация за осигуровки”. Целта е веднъж въведена, информацията за работника да бъде използвана и в другите две таблици, т.е. да се избегне повторяемостта на записите.



Фиг. 5. Таблица „Информация за работника“ и релация тип „едно към много” към таблици „Информация за заплати и осигуровки”

По аналогичен начин се постъпва и с данните от другите отдели.

Заключение

За разработването на модел на склад от данни е необходимо в началния етап да се извлекат знанията, намиращи в наличност в самата организация, поради две причини:

- Първо: преди прилагане на методологията на конкурентното разузнаване, аналитикът трябва да разполага с информация за собствената/възложилата компания.
- Второ: постига се разнообразие на наличната информация, което от своя страна води до получаване на цялостна представа за средата на сигурност в организацията.

Съгласно изискванията на стандарта за ИС и на стандарта за тестване на сигурността, за целите на изследването, уместни се явяват текстологичните методи за извличане на знания и интервюто.

Използван е системният анализ и подход за декомпозиране на организацията и проследяване на входно–изходните информационни потоци от всеки отдел. Същият е приложен и при определяне на данните, генерирани от взаимодействието на корпорацията със заобикалящата я среда, комбиниран с методиката на конкурентното разузнаване.

Литература

1. **Георгиев, Р.** *Делови решения и сигурност на организацията.* София : Софт-трейд, 2007. ISBN 978-954-334-056-9.

2. **Ернандес, М.** *Проектиране на бази от данни.* София : Софтпрес, 2004. ISBN 978-954-685-301-1.

3. **Начев, Й.** *Конкурентно разузнаване.Частна разузнавателна дейност* s.l.: Ciela, 2007. ISBN 13: 978-954-28-0025 3.

4. **Нешева, М.** *Извличане на знания. Лекции по Дисциплината „Експертни системи”*. [Online] 2012. http://www.fmi.uni-sofia.bg/Members/marian/ES_Course/Presentations/Lct11.ppt/view.

5. **Петков, А.** *Бази данни в управленските информационни системи*. Факултет "Бизнес и мениджмънт" - РУ "Ангел Кънчев". [Online] 2007. fbm.uni-ruse.bg/d/uis/L-2.pdf

М Е Ж Д У Н А Р О Д Н А
Н А У Ч Н А К О Н Ф Е Р Е Н Ц И Я

КИБЕРСИГУРНОСТТА В ИНФОРМАЦИОННОТО ОБЩЕСТВО

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 1 7

Предпечатна подготовка - Факултет „Артилерия, ПВО и КИС“ - Шумен