OBJECTIVES OF PROTECTION OF INTELLECTUAL PROPERTY IN THE CONTEXT OF INFORMATION SECURITY

Hristo A. Desev

Abstract: *Encouraging of innovation activity and the rightholders protection against cyber threats are the forefront of state (national) strategies for intellectual property. Intellectual property as particularly valuable intangible assets (databases, trade secrets and know-how, computer programs, etc.) are the subject of new threats in cyberspace. Intellectual property protection in cyberspace (including modern technical means) creates the required level of competitiveness for the rightholders.*

Keywords: *intellectual property, intellectual property protection against cyberthreats, rights to the results of intellectual activity*

ОСОБЕНОСТИ НА ЗАЩИТАТА НА ИНТЕЛЕКТУАЛНАТА СОБСТВЕНОСТ В КОНТЕКСТА НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Христо А. Десев

Национален военен университет " В. Левски" гр. Велико Търново
Факултет "Артилерия ПВО и КИС" гр. Шумен

Съвременните цифрови технологии и използването на глобалните информационни мрежи промениха кардинално схващанията и разбиранията за натрупване и обмен на информация. Тази информационна революция предизвиква изменения в принципите на защита на интелектуалната собственост. Глобалната интернет среда и развитието на информационно-комуникационните технологии изискват адекватно регулиране на отношенията при използване на интелектуалната собственост. Засилването на комерсиализацията на интелектуалната собственост и повишаването на инвестиционната привлекателност доведоха до изключително широко използване на правата върху нея, като средство на междуфирмената борба.

В докладите на Европейското патентно ведомство и Комисията за хармонизиране на вътрешния пазар се подчертава, че отраслите работещи с интелектуална собственост са 39%от общата промишлена дейност, като в тези отрасли средната работна заплата е с 40% по-висока от останалите. Подобни са и анализите на патентното ведомство на САЩ.

Съвременната епоха на „интелектуален капитализъм" и свободно предприемачество търговските сделки са тясно обвързани с пазарен обмен на нематериални (интелектуални продукти). Правата на интелектуална собственост осигуряват на инвеститорите своеобразни гаранции в инвестиционния риск и дори имат стойност на своеобразна обменна валута. Паралелно с това изградената система за ускоряване на инвестиционното развитие, чрез системата за защита на интелектуалната собственост се съпровожда с ефекта на понижаване на конкуренцията и по-високи разходи за достъп до продуктите и технологиите.

По експертни оценки транснационалните корпорации отделят съществено място на интелектуалната собственост в стратегиите за разширяване на позициите си на световните пазари. Основната цел е получаване на преимущество в отделни отрасли и услуги. Воденето на патентни войни чрез блокиране на научно-техническите разработки на конкурентите са свързани с активни форми на защита на перспективни сектори на пазара от всички държави. Показателен в това отношение е ЕС, който инициира преразглеждането на договора Safe Harbor с търговското министерства на САЩ за трансфер на персонални данни за американски компании в ЕС. Конкретния

повод е програма за обобщаване на данни PRISM на САЩ която нарушава основна директива на ЕС за защита на данните (EU Data Protection Directive).

Р. България не е изключение от тези тенденции – използване на емейли и мобилни съобщения с подвеждаща информация, подмяна или фалшифициране на официални уебсайтове и домейни, злоупотреби със социални мрежи и профили с цел манипулация, създаване на паника, бизнес измами и обществени въздействия в значителни размери.

Отворен стои въпросът за надеждността на информационни източници в интернет, за достоверност на новините, съобщенията и авторите.

Последствията от кибер заплахи и нерегламентирани действия в информационно-комуникационната среда имат икономическо измерение и морално отражение върху репутацията на фирмите които съхраняват и управляват базите от данни. По оценки на Великобритания ежегодно фирмите търпят загуби от пробив в интелектуална собственост между 18-20 млрд. лири. Показателен за степента и стойността на заплахата е случаят с „Vodafone" ФРГ. В 2014г. фирмата „изпусна" в мрежата данни за два милиона души от 36 млн. свои клиенти (имена, банкови кодове, адреси, сметки), само с бързата намеса рискът от пряка заплаха за клиентите беше минимизиран. Тези случаи и създадените около тях ситуации принуждават правителствата да предприемат активни контрамерки.

Проблемите на информационната сигурност са обект на основни законодателни инициативи от ЕС. Утвърдената Стратегия за кибер сигурност (EU Cyber Security Strategy) фиксира и задължава страните членки да спазват минимални изисквания в сферата на кибер сигурността:

- ✓ направления за профилактиране на кибер мрежи и системи;
- ✓ разкриване на механизми за намаляване на последствията;
- ✓ повишаване на нивото на готовност от бизнес организациите.

Стратегията е насочена към стимулиране създаването на високо-защитени продукти на информационната индустрия и тяхното сертифициране чрез стандарти за киберзащита обхващаща дори облачните технологии. Този документ е съобразен с останалите документи в съюза: Директива за защита на частния животв цифровото пространство (E-Privacy Directive 2002/58/EC), Директива за защита на критичната инфраструктура (European Critical Infrastructures Directive 2008/114/EC), Директива за защита на данните (Data Protection Directive 95/46/EC). Защитата на данните в информационните технологии и личните данни е разгледана в специални директиви на Евро парламента и Евро комисията (Directive 2013/40/EU on attacks against information systems) и (General Data Protection Reglament EC 2016/679 (GDPR). Редица държави са разработили собствени документи – ФРГ е утвърдила Стратегия за безопасност и мерки за взаимодействие между обществени и държавни органи и търговските дружества за взаимопомощ в сферата на кибер сигурността.

Великобритания тества иновационни форми на взаимодействие между бизнеса и държавата (CISP), които задължават операторите на данни да предприемат технически и организационни мерки за защита , а за финансовите институции да проследяват финансови операции.

Важно значение отделят и САЩ със специален указ на президента за формиране на държавна политика за подобряване на условията за кибер сигурност.

Всички разработени стратегически и доктринални документи за информационна сигурност са тясно обвързани със стратегията за интелектуална собственост.

Предприетите мерки срещу лъжливи сведения, интелектуално пиратство, нарушаване на правата в Интернет обхващат:

✓подобряване на откритостта и законосъобразността на политиките и международните преговори;

✓работа с данни за добросъвестно използване;

✓повишаване на ефективността на взаимодействията;

✓засилване на защитата на ITот нарушения в на чужди сайтове домейни от първо ниво за поддръжка на националните фирми и международния пазар.

Прилагането на разработените стратегии предполагат развитие на иновационен процес за генериране и внедряване на новите идеи на пазара за повишаване на икономическия растеж и конкурентно способността на фирмите. Патентните процедури, търговските марки и защитата на авторските права са основно средство за определяне на правата на собственост върху изобрете-

нията и творческите идеи. Тези основни параметри на правната рамка гарантират защитата на интелектуалната собственост и икономическата изгода на инвестициите. Нещо по-вече без IT защита изобретателите, които влагат време и средства за разработване на нови продукти ще са в неизгодно положение спрямо компания, която копира продукта от Интернет без да заплаща труд, талант и т.н.т. При прилагането на тези стратегии ЕС и САЩ визират основно Китай.

Основните изводи от реализацията на подобни стратегии позволяват да се постигнат следните резултати:

- ✓ активизиране на процеса за създаване на интелектуална собственост;
- ✓ повишаване на качествата на интелектуалната собственост и инвестиционния ефект;
- ✓ подобряване защитата на авторските права;
- ✓ засилване влиянието на IP в ключови отрасли на икономиката с преференциално патентоване;
- ✓ производство на висококачествени материали и технологии за екологично развитие и нисковъглеродни емисии;
- ✓ подобряване на трансферите на важната гражданска продукция;
- ✓ права върху лицензии, уставни капитали и активи;
- ✓ подобряване на ефективността на управление на интелектуалната собственост, чрез правилно управление на информационните потоци;
- ✓ поддържащи юридически и патентни услуги при защита на търговските марки, авторските права и др.

Резултатите от интелектуалната дейност и средствата за индивидуализация на стоките, дейностите и услугите са нематериални активи, които имат материално и стойностно измерение. Патентите, промишлените образци, софтуера, ноу хау в производствата и др. съдържащи новаторски технологии и хуманитарни знания в световния пазар имат ценност за своите създатели.

Информацията за характера и съдържанието на новаторските разработки имат огромно значение за днешната конкурентна среда. Тяхното използване и разпространение се допуска при спазване на изключителните права на собственика във всичките форми на прилагане.

В този контекст следва Национална стратегията за кибер сигурност „Кибер устойчива България 2020“ да включи и насоки за по-ефективна защита на високите научно-технически разработки и авторски права. Усъвършенстването на такъв механизъм трябва максимално да защити интересите на собствениците и баланса между частното и общественото. В този аспект под кибер безопасност може да се разбира и защитата на интересите на интелектуална собственост. Кибер заплахите по отношение на интелектуалната собственост са обвързани с нарушаване на правата на собственост на самия обект.

Нарушенията на правата на интелектуална собственост включват неправомерно използване на резултатите от интелектуална дейност или средствата за индивидуализация, които причиняват вреда на притежателя във формата на неполучени приходи или загуби на имидж. Такъв тип заплаха е непосредственото използване на продукта или способа, а негова косвена проява е износа на такъв продукт или въвеждане на контрафактна функция. Заплаха за интелектуалната собственост са кибер атаките срещу възможността за използване на даден продукт, промяна в базата от данни с определена търговска информация, разгласяването на търговски тайни като заплаха за конфиденциалността. Полето на тези заплахи е Интернет от което произтичат някои систематични особености:

- ✓ лесен незаконен достъп до служебни и държавни тайни;
- ✓ хакерски атаки;
- ✓ несанкционирани намеси до програмни средства, вмешателство или промяна в бази от данни;
- ✓ разпространение на невярна информация за лица и фирми;
- ✓ нарушаване на авторските права;
- ✓ незаконно използване на търговски марки, наименования, WEB сайтове и документи;
- ✓ преднамерено използване на географски обекти, търговски обозначения за предизвикване на щети на техния истински притежател.

Трябва да отчетем, че правата върху патенти, търговски марки, микросхеми, софтуер, авторски произведения могат да са държавни, на частни лица и организации, на международни фирми

и обединения. Тази особеност предизвиква допълнителна ориентация на мерките за защита към приоретизация на различни нива.

Анализът на концептуалните подходи и националните стратегии за развитие на интелектуалната собственост и насочеността на стратегиите за кибер защита позволява да се направят някои изводи:

Задачата по повишаване на ефективността на защитата на интелектуалната собственост е свързана с развитието разширяването на предмета на дейност на самите обекти към които са насочени заплахите. Проблемите свързани със защитата на документи от различно ниво, глобализацията на интернет търговията и електронните услуги, използването на виртуални валути, възможностите за 3D принтиране значително повишава изискванията към кибер безопасността. Възниква необходимост за правно регулиране на отговорностите за Интернет доставчиците и информационните посредници, които са отговорни за съхранението и разпространението на материалите в мрежата. Правила за отговорност следва да се прилагат и към лицата получаващи достъп до масивите от данни, чрез рестрикции за забрана на достъпа, ограничения в ползване на книги филми без съгласието на собственика.

Значението на защитата на ценни технологии, информация в мрежите нараства с развитие на техногенната глобализация, аутсорсинга и удължаването на веригите от потребители. Увеличава се риска от разпространение на крадена информация в трети страни за търговски цели. Повишена задълбоченост следва да се отдели на промишления шпионаж в полза на конкурентите прилаган от ползвателите на определени масиви от данни в процеса на своята работа.

References:

1. EU Directive on the protection of undisclosed know-how and business information (trade secrets)against their unlawful acquisition, use and disclosure http://ec.europa.eu/

2. Национална стратегията за кибер сигурност „Кибер устойчива България 2020“

3. Stoyanova V, Possibilities for the application of social networks in transmission of secret information, International Scientific Conference CONFSEC ISSN print 2603-2945, ISSN online 2603-2953, year 1, ISSUE 2(2), 2017, Avaible from http://confsec.eu/sbornik/1-2017.pdf

4. Friedrich Geiger and Archibald Preuschat. Hacker Hits Vodafone in Germany. Wall Street Journal (Sept. 12, 2013).

5. Подробнее см.: Карцхия А.А. Права промышленной собственности в российском праве: навстречу вызовам современности. Lambert Academic Publishing. Germany,2013.