Системите на интелектуалната собственост и на търговската тайна защитават от измами

Николай Крушков*

Резюме: Ожесточената конкуренция води със себе си интерес към всяка чужда незащитена бизнес информация. Целта е нейното придобиване и използване на пазара. Утвърдените бизнес единици с отлична репутация търсят и инвестират в нови и креативни информационни решения. Обикновените измамници използват всички начини за инкасиране на печалби на основата на чужди бизнес достижения, като използват слабостите в защитата на такава информация, за да могат да я придобият. Тази реалност изисква разпознаване на видовете ключова бизнес информация, както и знания в областта на закрилата на информацията: чрез законова закрила, както и чрез закрила с вътрешни нормативи, правила и процедури.

Ключови думи: интелектуална, собственост, информация, търговска, тайна.

JEL: A20, C8, D23, D83, F52, L51, L86, M14.

Увод

С космическото развитие на информационните технологии и глобалната информационна свързаност в наши дни, информацията вече се е превърнала в стратегически технологичен ресурс. Конкурентоспособността изисква реализиране на интегрирана система за защита на бизнес информацията. На свой ред, достигането до чужда незащитена бизнес информация и нейното използване на пазара е сред негласните корпоративни интереси както на утвърдени бизнес единици с отлична репутация, така и на обикновени измамници, търсещи начини за инкасиране на печалби на основата на чужди бизнес достижения. Не е нужно да се аргументира необходимостта от предприемането на всеобхватни интегрирани мерки за защита на корпоративната бизнес информация, но е ясно, че е нужна система от мерки за защита на ключовата бизнес информация от една страна, но и ефективното управление на системата.

1. Видове информация, която се използва от бизнеса и следва да се защитава

Възможното класифициране на видовете информация според нейните основни предназначения може да приеме следното разделение:

1) **Държавна и служебна тайна**, които се използват от бизнеса в условията на обществени поръчки с достъп до класифицирана информация. Държавната и служебна-

* Николай Крушков е доктор по икономика, главен асистент в Институт по творчески индустрии и бизнес.

та тайна не могат да бъдат обект на споделяне, предоставяне или използване извън кръга на определен кръг служители, които са получили достъп до нея, след като същите са проверени за надеждност по сложна нормативно регулирана процедура.

2) **Производствена и търговска тайна** е бизнес информация, която е определена като такава от притежателя ѝ с нарочен вътрешен норматив, взети са мерки за нейната защита и нейното неразпространение извън кръга от лица, работещи с нея. Тя е обект на най-строга защита, защото не е предназначена за „продажба“ или лицензиране до момента, в който се продаде цялото търговско дружество. Всякакво споделяне на производствена или търговска тайна би довело до загуба на конкурентоспособност.

3) **Интелектуална собственост** са иновативни решения, които, по силата на различни закони в областта, представляват изключителна собственост на своите притежатели. За разлика от търговската тайна, интелектуалната собственост е предназначена за лицензиране. Закрилата е срочна. За достигането до творческия резултат са вложени ресурси. В срока на закрилата следва да се върнат вложените инвестиции и да се реализира печалба. Тя следва да се рекламира и предлага пазарно.

4) **Ноу-хау** е информация, акумулирана на основата на знания, умения и опит, която е практически приложима в производството или професионалната практика и която е защитена от това, че не ѝ е дадена публичност, а е запазена в тайна от притежателя ѝ – на негова лична отговорност, защото няма нормативен акт или вътрешни правила, които да я закрилят. Тя обикновено е предназначена за „продажба“ или лицензиране, без да се ползва от законова закрила. Обикновено е предназначена за лицензиране, защото нейното предоставяне не би следвало да наруши степента на конкурентоспособност на притежателя ѝ, а да възвърне вложени инвестиции.

5) **Обща (ежедневна) делова информация, включително свързаност, мрежи и достъп на служители до данни,** която е от значение за ефективността на деловите процеси и която обикновено не е защитена или е само ограничено защитена с частични процедурни решения (като например: забрани за използване на лични комуникатори и лични мейли в делова среда; изисквания за съгласуване на предложения и решения с правни и бюджетни звена, изискване за RFID карти за достъп до сгради, помещения, принтерни устройства; камери за наблюдение в служебни помещения; изисквания за лични пароли за достъп до делова информация и съхранение на лог файлове) и други решения, които по-скоро разделят административни нива служители, отколкото защитават информацията.

6) **Друга защитена лична информация като лични данни, банкова тайна,** данъчно-осигурителна тайна и други, която информация обикновено не влияе на деловите процеси, а е предназначена за защита на личната неприкосновеност на лицата от необоснован интерес, злонамереност или обикновено любопитство.

Разпознаването на видовете бизнес информация е в основата на изграждането на ефективна система за защита срещу измами, която закриля корпоративната информация, но не ограничава и не забавя работните процеси на предприятието.

2. Защита срещу измами чрез ефективна закрила на ключовата корпоративна информация

Системата за корпоративна сигурност включва редица мерки в много направления на техническата, физическата, процедурната и информационната сигурност.

Тук ще се спра само на необходимостта от разграничаване на законовата закрила на корпоративната информация (когато информацията отговаря на конкретни критерии) и закрилата на корпоративната информация на основата на вътрешни правила и процедури.

2.1. Законова закрила:

Различни закони закрилят информацията, представляваща държавна тайна; тази, представляваща служебна информация (тайната по закона за подземните богатства, тайната по кодекса на труда, тайната по закона за публично предлагане на ценни книжа и много други, свързани с: лекарската тайна, следствената тайна, тайната на осиновяването, тайната на кореспонденцията); *личните данни; банковата информация; данъчна и осигурителна информация; интелектуалната собственост.*

Интелектуалната собственост включва закриляни обекти на индустриална собственост, обекти на художествена собственост и нови обекти на собственост, които се защитават от няколко закона на национално ниво, както следва:

- изобретенията и полезните модели от закона за патентите и регистрацията на полезните модели;
- марките, указанията за произход и наименованията за произход от закона за марките и географските означения;
- промишленият дизайн от закона за промишления дизайн;
- произведенията на литературата, науката и изкуството, изпълненията, записите на филми, звукозаписите, програмите на радио и ТВ организациите и базите данни от закона за авторското право и сродните му права;
- новите сортове растения и породи животни от закона за закрила на новите сортове растения и породи животни;
- топологията на интегралните схеми от закона за топологията на интегралните схеми.

Законово закриляната информация гарантира интересите на собствениците ѝ. Това е така, защото законите на страната създават ред за използване на такава информация от една страна, а от друга осигуряват търсенето на отговорност за всяко неоторизирано използване на такава информация, което може да се реализира по граждански, административен или наказателен ред. Тук са налице предпоставките за въздържане и възпиране от всякакви измамни действия, свързани с неразрешено използване на законово защитена информация, именно заради неизбежната отговорност пред закона.

2.2. Защита срещу измами чрез създаване на вътрешни нормативи, правила и процедури за закрила на ключова корпоративна информация

Бизнес единиците сами определят кръга от информация, която закрилят. Сами създават своите правила и процедури за закрила на корпоративната си информация. Това се отнася за всяка ключова корпоративна информация, която не се закриля по силата на закон. Този начин на защита на корпоративната информация – с вътрешни нормативи, вътрешни правила и процедури, получава все по-голямо значение в деловия свят. Ключовата корпоративна информация включва:

1) **Производствена и търговска тайна** се защитава от Закона за защита на конкуренцията, но само концептуално. Ако се подходи творчески при определянето на вида бизнес информация, представляваща производствена и търговска тайна, всяко предприятие може в огромна степен да създаде ефективна защита на много и съвсем различни аспекти на бизнес дейността срещу неоторизирано разгласяване от

страна на служители, срещу чужд негласен корпоративен интерес или срещу такъв на спекуланти, готови да получат печалби в т.ч. със средствата на измамата.

Може би именно тук е мястото да се спомене, че незнанието на това що е интелектуална собственост, както и това що е производствена и търговска тайна, води до загубата на конкурентно предимство на предприятието изключително бързо. От гледна точка на корпоративната сигурност, всяко предприятие може и следва да идентифицира, опише и предприеме необходимите мерки, за да защити своята производствена и търговска тайна, така и по отношение на интелектуалната собственост.

Примерното изброяване на видовете корпоративна информация, които от гледна точка на сигурността следва да бъдат включени в списъка с информация, определена като производствена и търговска тайна с вътрешен норматив на бизнес единицата, включва:

- бизнес цели и стратегии за развитие на предприятието;
- годишен план на предприятието;
- процес на ценообразуване;
- данни от сключени/подготвяни договори;
- подготвяне на нови продукти и развойна дейност;
- данни от проучвания на пазара и др.

Определението на производствената или търговска тайна е дадено в Закона за защита на конкуренцията: „Производствена или търговска тайна са факти, информация, решения и данни, свързани със стопанска дейност, чието запазване в тайна е в интерес на правоимащите, за което те са взели необходимите мерки“ (Закон за защита на конкуренцията, § 1, т. 9). Изразът „необходими мерки“ е елемент от технологията на управление на сигурността на информацията и включва:

- идентифицирането на тази информация в списък (с който следва да бъдат запознати всички служители с достъп до такава информация) и
- създаването на вътрешни правила за работа с такава информация (обикновено с нарочна заповед на главния изпълнителен директор).

2) **Общата (ежедневната) делова информация,** свързана с обмена на данни в информационни мрежи, е изцяло без нормативна закрила. Особено внимание следва да се отделя на управлението на нейната сигурност, като елемент от защитата на конкурентоспособността и защита от измами. Нейната ежедневна използваемост от всички служители е в основата на нейната уязвимост. Корпоративната сигурност изисква създаване на защитени комуникационни канали, бази данни с нива на достъп, ефективни правила и процедури за обмен на информация вътре и извън организационната единица, както и обучение на служителите.

3) **Патентна информация,** която се предоставя публично в патентните ведомства на съответните държави и включва описанието на новото техническо решение. Тази информация изисква особено внимание от гледна точка сигурност. Тя винаги е обект на интерес от страна на корпоративното разузнаване на конкурентите, но и на различни лица, които са готови да спекулират с чуждите творчески достижения, в т.ч. и със средствата на измамата. Трябва да се спазват различни правила за запазване на ключови данни при описанието на изобретението, така че да не може всеки прочел заявката при нейната публикация с лекота да стигне до световната новост на решението, която се претендира.

4) **Произведенията на науката,** които попадат в общата закрила на произведенията на литературата и на изкуството по смисъла на закона за авторското право и сродните права, но имат самостоятелна роля и значение, необвързано по същe-

ство с литературата или изкуството. „Произведенията на науката се включват в широкия спектър на обекти на интелектуална собственост, но не са изследвани и изяснени като такива“ (Цакова, 2009, с. 9). Нещо повече, нито един от международните или националните актове не дава легална дефиниция на понятието „произведения на науката“. Дадено е определение, което дефинира произведенията на науката като „обективираните резултати от научно-изследователска дейност на човека, които представляват постиженията от научната му работа“ (Цакова, 2009, с. 10). От бизнес гледна точка „научният потенциал не е пасивен обект за получаване на информация, а активен субект на развитие на иновациите и приложението им в практиката“ (Димитров, 2017 г., с. 143). В допълнение, научните резултати биха могли да се доразвият до изобретения, промишлен дизайн или полезни модели, като същевременно „произведенията на науката съдържат знание, което е потенциал за ноу-хау“ (Цакова, 2009, с. 258). Тази реалност на отсъствие на легална дефиниция, в съчетание с обстоятелството, че правата върху научните резултати имат потенциал за изобретение, полезен модел, промишлен дизайн или ноу-хау, като научните резултати винаги са на конкретен учен (изследовател), поставя акцент в корпоративната сигурност върху резултатите в науката и технологиите от една страна, и върху човека, създаващ наука и технологии, от друга. В съвременен план, „стратегията за успешно развитие е във функционална зависимост от проектираните и произвеждани във фирмата нови продукти“ (Маркова, 2015) (Откриваем на: www.arcfund.net/fileSrc.php?id=22389). По-конкретно, „идеите за нови продукти, разработването им до проект за внедряване в производството трябва да са базирани върху последните достижения в областта на: науката, техниката и дизайна в съответната продуктово-технологична област“ (Маркова, 2015) (Откриваем на: www.arcfund.net/fileSrc.php?id=22389). Това ще рече, че са възможни спекулации, в т.ч. измами с твърдения за „произведения на науката“ в различни аспекти на бизнес дейността в условията на отсъствие на легална дефиниция на понятието, за което корпоративната сигурност трябва да е особено внимателна.

3. Ключови аспекти на управлението на информационната сигурност срещу измами

Технологията на управлението на сигурността на информацията задължително разгръща интегрирана система от действия, която включва комплекс от взаимосвързани и взаимообусловени мероприятия:

1) Определяне на системното, йерархичното и функционалното „място“ на компетентния орган, отговарящ за сигурността на корпоративната информация: конкретен служител или цяло структурно звено.

2) Делегиране на управленски и контролни правомощия и осигуряване на бюджет за дейността.

3) Идентифициране на информацията, която попада в графата „конкурентен ресурс“ на бизнес единицата, която следва да се защитава.

4) Създаване и въвеждане на система от корпоративни правила и процедури, съобразно изискванията на средата за сигурност за защита на информацията: чрез системата на интелектуалната собственост, чрез системата на производствената и търговската тайна, чрез ноу-хау и други.

5) Запознаване на ръководството на бизнес единицата и на служителите с правилата и процедурите за защита на корпоративната информация, доколкото имат отношение към утвърждаването, въвежда-

нето в сила, контрола на правилата и процедурите и отчетността по тях.

6) Обучение на състава: първоначално и текущо.

7) Периодично „учебно“ тестване както на системата за информационна сигурност, т.нар. „пенетрейшън тестове“. Това позволява надграждането ѝ чрез отстраняване на констатираните слабости.

Заключение

От гледна точка на технологията за управление на информационната сигурност срещу измами, от съществено значение е обстоятелството, че корпоративната информация следва да се разглежда в две направления: корпоративна информация, която е закриляна по силата на закон и корпоративна информация, която трябва да се защити чрез вътрешни за предприятието правила и процедури.

За целите на запазването на конкурентоспособността на всяко предприятие е необходимо идентифицирането на ключовата корпоративна информация и предприемане на система от мерки за нейната защита срещу неоторизирано използване. Тази част от корпоративната информация, която не попада в обхвата на законовата закрила под формата на интелектуална собственост на предприятието, изисква предприемане на набор от мерки от страна на служителите, които осъществяват дейността по информационна сигурност. Съвременната бизнес реалност и висококонкурентната среда във всички отрасли налага разработване, възприемане и прилагане на вътрешните правила и процедури за защита на ключовата производствена и търговска тайна от страна на всяко предприятие.

Системата е ефективна когато включва провеждането на първоначално и текущо обучение на всички служители, периодично тестване на системата за информационна сигурност и надграждането ѝ в съответствие с новите реалности.

Цитирани източници:

Закон за защита на конкуренцията, Обн. ДВ. бр. 102 от 28 ноември 2008 г., § 1, т. 9.

(Zakon za zashtita na konkurentsiyata, Obn. DV. br. 102 ot 28 noemvri 2008 g., § 1, t. 9)

Димитров, Н., Съвременен инструментариум за оценяване на сигурността: апробиране на модела за оценяване на енергийната сигурност и сигурността на енергийните ресурси в България”, 2017. С., Издателски комплекс – УНСС, с. 143.

(Dimitrov, N., Savremenen instrumentarium za otsenyavane na sigurnostta: aprobirane na modela za otsenyavane na energiynata sigurnost i sigurnostta na energiynite resursi v Bulgaria, Izdatelski kompleks – UNSS, S, 2017, s. 143)

Маркова, М., 2015. „Политики в дизайна като интелектуална собственост“, „Иновации, основани на дизайн в Европа: политическа рамка, приоритети и предизвикателства“, Фондация „Приложни изследвания и комуникации“, София, 12 март 2015 г. (Откриваем на: www.arcfund.net/fileSrc.php?id=22389)

(Markova, M., 2015. „Politiki v dizayna kato intelektualna sobstvenost“, „Inovatsii, osnovani na dizayn v Evropa: politicheska ramka, prioriteti i predizvikatelstva“, Fondatsia Prilozhni izsledvania i komunikatsii, Sofia, 12 mart 2015 g. (Otkrivaem na: www.arcfund.net/fileSrc.php?id=22389)

Цакова, В., 2009. Произведенията на науката като обект на интелектуална собственост, УИ „Стопанство“, с. 9, 10, 258.

(Tsakova, V., 2009. Proizvedeniyata na naukata kato obekt na intelektualna sobstvenost, UI „Stopanstvo“, s. 9, 10, 258)