УДК 355.40:004.056.5

Анфіса Нашинець-Наумова,

канд. юрид. наук, доцент,
завідувач кафедри публічного та приватного права
Київського університету імені Бориса Грінченка

ДОСТУП ДО КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ: ЗАПОБІГАННЯ НОВИМ ВИКЛИКАМ І ЗАГРОЗАМ

Не секрет, що сьогодні інформація відіграє значно більшу роль у житті будь-якої компанії або державної організації, ніж пару десятків років тому. Хто володіє інформацією, той володіє світом, а хто володіє чужою інформацією, той набагато краще підготовлений до конкурентної боротьби, аніж його суперники. У статті автор намагався продемонструвати стурбованість, яку проявляють майже всі організації щодо внутрішніх загроз інформаційній безпеці. Найбільший рейтинг небезпеки припадає на витік конфіденційної інформації.

Ключові слова: конфіденційна інформація, витік інформації, ІБ-інциденти, атака, захист інформації.

Постановка проблеми. Нині темпи розвитку України характеризуються значними економічними та політичними перетвореннями. В умовах ринку та конкуренції виникають проблеми, пов'язані із забезпеченням безпеки не тільки фізичних і юридичних осіб, їхньої майнової власності, а й інформації, що має комерційне значення, інших відомостей, зокрема про результати інтелектуальної діяльності: секрети виробництва, службові секрети та інші.

Інформація – найважливіший продукт суспільного виробництва, постійно нарощуваний ресурс людства; сьогодні це найбільш цінний і ходовий об'єкт у міжнародних економічних відносинах. На міжнародному рівні сформувалася система поглядів на інформацію як на найцінніший ресурс життєзабезпечення суспільства, що має соціальне значення.

Інформація, безсумнівно, є одним із найбільш цінних і водночас вразливих активів будь-якої компанії. Чим менша кількість людей має до неї доступ, тим більшою цінністю володіє інформація. У спробі забезпечити належний захист даних від будь-яких загроз компаніям слід вживати всіх необхідних заходів, які дадуть змогу забезпечити їхню цілісність і секретність. Одна з ключових цілей в зв'язку із цим – запобігання несанкціонованому доступу та незаконному розголошенню інформації нинішніми або колишніми співробітниками.

Аналіз останніх досліджень і публікацій із цієї теми. Конфіденційна інформація є об'єктом наукового аналізу багатьох вітчизняних і зарубіжних дослідників, зокрема І.Л. Бачило, В.М. Брижка, Р.А. Калюжного, В.А. Копилова, Н.В. Кушакової, П.І. Орлова, Г.Г. Почепцова, С.П. Росторгуєва, М.Я. Швеця та інших. У працях цих вчених аналізується взаємозв'язок інформації та права; захист інформаційних ресурсів, зокрема персональних даних; визначальні чинники інформаційної безпеки підприємства; питання відповідальності за поширення недостовірної інформації; правові проблеми інформатизації тощо.

Мета статті. Водночас подальшого дослідження потребують проблеми правового регулювання доступу до конфіденційної інформації, що й ставить за мету наша стаття.

Виклад основного матеріалу. 2016 рік приніс справжній шквал інцидентів, пов'язаних з конфіденційною інформацією, інформаційною безпекою: від масового фішингу з використанням податкової інформації, проломів в WordPress, компрометації корпоративної електронної пошти і DDoS-атак до підозр у «зломі» президентських виборів. При цьому немає підстав вважати, що в 2017-му ситуація покращиться – все може стати тільки гірше з урахуванням того, що зловмисники продовжують розвивати навички соціальної інженерії, знаходять нові способи підсовувати шкідливий продукт, зламувати вразливі бази даних і за допомогою мобільних технологій проникати в корпоративні мережі та акаунти приватних осіб [1, с. 65].

За словами Дениса Макрушина, антивірусного експерта «Лабораторії Касперського», кількість направлених на бізнес атак програм-вимагачів та їх окремого виду – шифрувальників – стрімко зростає. Причому ризику піддаються практично всі галузі: освіта, ЗМІ, фінанси, шоу-бізнес, державний сектор, виробництво, транспорт. Особливо хотілося б виділити охорону здоров'я – в 2016 році лікарні стали популярною метою: наприклад, медичний центр в Голлівуді заплатив 17 тисяч доларів за розблокування комп'ютерів; були атаковані кілька лікарень в Німеччині та Великобританії. Всього ж із січня по кінець вересня 2016 року кількість атак на компанії збільшилася в три рази: якщо в січні 2016 року атаки робилися в середньому кожні дві хвилини, то у вересні 2016 року – вже кожні 40 секунд. У січні 2017 року були зламані сервери Міністерства закордонних справ Королівства Таїланд, а також низки інших урядових організацій, включаючи, Міністерство інформації та комунікаційних технологій, Департамент податків і зборів, Адміністративний суд, Королівський флот та інші департаменти уряду Таїланду.

У результаті витоку даних у Таїланді в Мережу потрапила конфіденційна інформація про кілька тисяч державних службовців і здобувачів роботи, включаючи номери телефонів і банківських рахунків, електронну пошту та зашифровані паролі. За даними видання Heakread.com, опубліковані в Інтернеті дані становлять усього 1% від загальної кількості вкрадених файлів [2, с. 35]. Як результат тайська армія планує залучити на службу «білих хакерів». Кібервоїни надаватимуть допомогу уряду в боротьбі з кіберзлочинністю та допоможуть поліпшити систему безпеки державних серверів, яка піддалася дискредитації багаторазовими атаками хакерів. Щорічно «Лабораторія Касперського» проводить дослідження, в ході якого компанії розповідають що трапилось з ними і про свої плани щодо інформаційної безпеки. Дані цього дослідження свідчать: від шифрувальників страждають українські компанії. При цьому 15% організацій так і не змогли відновити доступ до цінної інформації. Примітно, що кожна п'ята компанія великого бізнесу воліла заплатити кіберзлочинцям викуп, незважаючи на те, що це не гарантувало повернення файлів [3, с. 124].

Діана Соловйова, керівник групи підтримки систем інформаційної безпеки компанії ICL Services, вважає, що для оперативного виявлення атак потрібні компетентні людські ресурси. Бізнесу необхідно більше інвестувати не в нові продукти, а в розвиток компетенцій співробітників, які зможуть перетворювати ці багатомільйонні «модні іграшки» на інструменти, що реально працюють [4].

«У фахівців галузі інформаційної безпеки гуляє такий жарт: всі компанії діляться на два типи: ті, які вже знають, що їх зламали, і ті, яких теж зламали, але вони про це ще не в курсі. Але в кожному жарті є частка жарту, і раннє виявлення, а тим більше запобігання інцидентам – це одна з актуальних і вкрай важких завдань. Їх рішення за допомогою поведінкового аналізу Великих Даних видається правильним і найбільш перспективним, оскільки подібний функціонал допомагає виявляти аномалії, які можуть свідчити про ті чи інші ІБ-інциденти», – говорить Марія Воронова, провідний експерт з інформаційної безпеки, керівник напрямку консалтингу InfoWatch [4].

На підтвердження вищезазначеного ми можемо привести приклад ІБ-інциденту, який відбувся на початку 2017 р.: витік третьої серії четвертого сезону серіалу «Шерлок» (Sherlock), який нелегально з'явився в Інтернеті 14 січня 2017 р. – за день до прем'єрного показу на телеканалі BBC [4].

Як пояснює аналітичний центр InfoWatch, число витоків інформації зростає в усьому світі: за перші шість місяців 2016 року цей зріст склав 16%, а в трійці лідерів за кількістю витоків даних – США, Росія та Великобританія. У двох третинах усіх випадків витік даних відбувався з вини внутрішніх порушників.

З-поміж популярних телесеріалів на Заході відомі випадки витоків спойлерів і сценарію до серіалу «Гра престолів» (Game of Thrones), а також фрагментів серіалу «Ходячі мерці» (The Walking Dead) [5].

Півторагодинна серія «Шерлока» високої якості не могла бути передана, наприклад, електронною поштою через великий розмір файлу, але легко могла бути завантажена на знімний носій або завантажена в хмару, що спричинило витік в силу навіть ненавмисних дій порушника. Це підтверджує статистика аналітичного центру InfoWatch: за останні три роки частка витоків в результаті випадкових дій співробітників організацій збільшилася на 34% до 79,7%. На витік даних через мережевий канал, включаючи відправлення через браузер, припадає більше половини всіх випадків, зростає частка витоків на знімних носіях [5].

З точки зору шкоди такий витік міг позначитися на рейтингу показу серії, адже частина глядачів вже бачили її в Інтернеті, а також призвести до фінансових втрат і збитків в аспекті іміджевого складника.

Зараз більшість іноземних компаній висувають вкрай жорсткі вимоги щодо дотримання угод про конфіденційність, особливо якщо справа стосується передачі виняткових прав на результати інтелектуальної діяльності. Штрафи обговорюються заздалегідь і можуть доходити до сотень тисяч доларів. Підписуючи такі угоди, вітчизняні компанії не можуть не замислюватися про забезпечення конфіденційності отриманих відомостей.

Специфіка забезпечення інформаційної безпеки в медіабізнесі така, що в компаніях цієї сфери, як правило, працюють творчі люди, у чималій кількості використовуються мультимедійні дані великих розмірів, а також тиражуються типові IT-системи. Стандартні технології захисту, які історично застосовувалися в медійному бізнесі, такі як використання «сліпого дубляжу», обмеження на доступ акторів озвучення до всього матеріалу, черговість надання серій правовласником, так само як і традиційні методи охорони, сьогодні вже не забезпечують необхідної захищеності, і технології інформаційної безпеки могли б в цьому допомогти. Можна довіряти власному персоналу, але контроль робочої діяльності співробітників повинен здійснюватися на рівні, адекватному ризикам порушення інформаційної безпеки, які досить високі. Мінімально необхідні дії для захисту містять запровадження систем моніторингу інформаційних потоків і запобігання витоків даних. Це сувора рекомендація міжнародних стандартів і кращих практик у сфері забезпечення інформаційної безпеки [6, с. 14].

У 2016 році ми зіткнулися з компрометацією персональних даних у результаті дій політичних «хактивістів». Таким чином, тема витоків даних прийшла не тільки в бізнес, шоу-бізнес, а й у політику, ставши, наприклад, одним із помітних сюжетів поточної американської виборчої кампанії.

Отже, можна говорити про те, що будь-який витік інформації несе в собі ті чи інші негативні економічні наслідки для компанії. З цією думкою згодні й представники індустрії інформаційної безпеки, які говорять про те, що не-

шкідливих витоків даних не буває – будь-який із них несе в собі шкоду для бізнесу, якщо не зараз, то в майбутньому. Іноді досить важко передбачити, де і коли «вистрілять» ті документи, які інсайдери винесли з вашого офісу сьогодні. Буває, що проходить кілька місяців або навіть кілька років, перш ніж інформація зробить свою чорну справа, потрапивши, наприклад, на очі журналістам або конкурентам. Саме тому дуже важливо захищати дані комплексно, а не ділити їх на більш важливі та менш важливі. Інформація, яка не призначена для публіки, повинна залишатися закритою. А це означає, що її слід захистити від можливих витоків [7, с. 119].

Загалом всі канали витоку можна розділити на дві групи. До першої відносяться зловмисні викрадення інформації, до них також можна віднести всі інсайдерські ризики, тобто коли людина, група людей або навіть самі співробітники компанії намагаються викрасти конфіденційну інформацію, переслідуючи при цьому свої корисливі цілі. Друга група – це витік через необережність або помилку з боку співробітників. Як показує практика, саме другий варіант найчастіше зустрічається. Звичайно ж, це ні в якому разі не говорить про те, що про загрозу інсайдерів або шпигунство конкурентів можна забути.

За останні кілька років сформувалися кілька основних причин втрати даних. Тому захист від витоку інформації фокусується в основному на них, не забуваючи при цьому про інші прийоми розкрадання даних [8, с. 261].

1. Втрата незахищених носіїв, тобто дисків, флешок, карт пам'яті, ноутбуків тощо.

2. Випадкові зараження програмами-шпигунами під час некоректного поводження з Інтернетом, виходу без наявності захищеного доступу або ж підключення пристроїв, які були раніше заражені.

3. Виникнення технічних помилок під час роботи із секретними і конфіденційними даними, у разі їх публікації в Інтернеті тощо.

4. Відсутність обмежень щодо доступу до даних для співробітників компанії.

5. Атаки з боку зловмисників, які намагаються проникнути в систему, заразити вірусами тощо.

Сьогодні фахівці пропонують захищати інформацію за допомогою системи DLP – Data Leak Prevention (запропоновано агентством Forrester у 2005 р.).

У межах створення системи DLP вирішуються завдання:

– запобігання витоків конфіденційної інформації за основними каналами передачі даних;

– веб-трафік, що витікає (HTTP, FTP, P2P та ін.);

– електронна пошта загальна, корпоративна (внутрішня);

– системи швидкого обміну відомостями, мережевий та локальний друк;

– контроль за доступом до пристроїв і портів введення-виведення, до яких належать: дисководи, CD-ROM, USB-пристрої, інфрачервоні, принтерні (LPT) і модемні (COM) порти.

Як показують опубліковані дані опитування Deloitte провідних світових фінансових компаній, 49% респондентів зафіксували внутрішні інциденти (пов'язані з IT-безпекою) за останні 12 місяців. У 31% випадків інсайдери занесли віруси зсередини корпоративної мережі, а з інсайдерським шахрайством зіткнулися 28% респондентів, 18% організацій стали жертвами витоку приватної інформації клієнтів, а 10% виявили, що інсайдери скомпрометували корпоративну мережу. Організації, які постраждали від внутрішнього витоку, зізнаються, що велика частка загроз є наслідком недолугості або недбалості службовців (людський фактор – 42%, операційні помилки – 37%), а не злого умислу інсайдерів. Правда, 28% стали жертвою ретельно продуманого і професійного шахрайства, а 18% компаній позбулися приватної інформації клієнтів саме через те, що інсайдери цілеспрямовано допустили витік. Щоб не допустити такі інциденти в майбутньому, 80% опитаних фінансових компаній здійснюють моніторинг дій службовців, а 75% вводять різні обмежувальні заходи на використання тих чи інших технологій або пристроїв [9].

Тому сучасні виклики інформаційній безпеці, конфіденційній інформації зумовлені не тільки зовнішніми чинниками, що характеризуються намаганням зверхніх суб'єктів впливати на інформаційний простір з метою забезпечення власних інтересів, а й внутрішніми.

Висновок

Наявні загрози та виклики у сфері інформаційної безпеки, найбільша частина яких припадає на витік конфіденційної інформації, вказують на необхідність подальшого вдосконалення правового та технічного врегулювання в означеному напрямі та кардинальної трансформації системи захисту інформаційної сфери загалом.

Крім того зрозуміло, що зазначене вдосконалення потребує відповідного фінансування. Тому ще в грудні 2016 року Кабінет Міністрів України виділив Мінфіну та Державній казначейськый службі 80 млн грн із резервного фонду на оновлення мережевого обладнання після хакерських атак. У свою чергу Міністерство фінансів має намір витратити в 2017 році 51,9 млн грн на забезпечення кібербезпеки державних інформаційних ресурсів. Сподіваємось, що кошти підуть на покупку серверного та комутаційного обладнання, систем зберігання даних, антивірусного захищеного доступу до мережі Інтернет.

Список використаних джерел:

1. Качинський А.Б. Пріоритети в кібернетичній безпеці / А.Б. Качинський // Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти : матеріали наук.-практ. конф. (6 жовтня 2016 р.) / Упоряд. : В.М. Фурашев. – К. : НТУУ «КПІ імені Ігоря Сікорського», Вид-во «Політехніка», 2016. – С. 65–74.

2. Жук С.Я. Тенденції та перспективи розвитку інформаційної боротьби й інформаційної зброї / С.Я. Жук, В.О. Чмельов, Т.Н. Дзюба // Наука і оборона. – 2006. – № 2. – С. 35–41.

3. Качинський А.Б. Безпека, загрози та ризик / А.Б. Качинський. – К. : ІПНБ РНБО; НА СБ України, 2004. – 472 с.

4. Прогнозы в области информационной безопасности на 2017 год: [Електронний ресурс]. – Режим доступу : http://aladdin-rd.ru/company/pressroom/articles/45115/.

5. Російський Перший канал назвав попередню причину витоку останнього епізоду «Шерлока» [Електронний ресурс]. – Режим доступу : http://dt.ua/CULTURE/rosiyskiy-pershiy-kanal-nazvav-poperednyu-prichinu-vitoku-ostannogo-epizodu-sherloka-230211_.html.

6. Роговский Е.А. Глобальные информационные технологии – фактор международной безопасности / Е.А. Роговский // США и Канада : экономика – политика – культура. – 2011. – № 6. – С. 3–26.

7. Нашинець-Наумова А.Ю. Проблеми правового регулювання доступу до конфіденційної інформації на підприємстві / А.Ю. Нашинець-Наумова // Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право» : зб. наук. праць. – 2012. – № 4 (25). – С. 119–124.

8. Харрис Ш. Кибервойн@: пятый театр военных действий / Ш. Харрис. – М : Альпина нон-фикшн, 2016. – 390 с.

9. Lehtinen R. Computer Security Basics O'Reilly / R. Lehtinen, D. Russell, G.T. Gantemi. – O'Reilly Media? 2006. – 312 с. – [Електронний ресурс]. – Режим доступу : http://www.kaspersky.ru.

Не секрет, что сегодня информация играет значительно большую роль в жизни любой компании или государственной организации, чем пару десятков лет назад. Кто владеет информацией, тот владеет миром, а кто владеет чужой информацией, то гораздо лучше подготовлен к конкурентной борьбе, чем его соперники. В статье автор пыталась продемонстрировать обеспокоенность, которую проявляют практически все организации внутренних угроз информационной безопасности. Наибольший рейтинг опасности приходится на утечку конфиденциальной информации.

Ключевые слова: конфиденциальная информация, утечка информации, ИБ-инцидентов, атака, защита информации.

It is no secret that today, information plays a much greater role in the life of any company or public organization than a couple of decades ago. Who owns the information, he owns the world and who holds a strange information, it is much better prepared to compete than his rivals. The author tried to demonstrate concern, which show almost all of domestic security threats. The highest rating of danger falls on the leak of confidential information.

Key words: confidential information, information leakage, information security incidents, attacks, information security.