Дацун А. О.

УДК 005.92:004.056

Магістр 2 року навчання
факультету обліку і аудиту ХНЕУ ім. С. Кузнеця

СУЧАСНІ ТЕНДЕНЦІЇ В ГАЛУЗІ ІНФОРМАЦІЙНОГО ЗАХИСТУ ПІДПРИЄМНИЦТВА

Анотація. Розглянуто сутність безпеки інформації як важливої складової економічної безпеки підприємства. Визначено основні загрози та проблеми забезпечення інформаційного захисту підприємницької діяльності, а також можливі шляхи їх усунення.

Аннотация. Рассмотрена сущность безопасности информации как важной составляющей экономической безопасности предприятия. Определены основные угрозы и проблемы обеспечения информационной защиты предпринимательской деятельности, а также возможные пути их устранения.

Annotation. The article considers the nature of information security as an important component of a company economic security. The article also defines the main threats and problems of business information security and the possible ways of their removal.

Ключові слова: інформаційна безпека, підприємництво, захист інформації, хакери, програмне забезпечення, джерела загроз, хмарні сервіси.

Поняття "інформація" має розгалужену структуру та безліч значень для різноманітних сфер життєдіяльності. До цього часу немає єдиного наукового визначення терміна "інформація". Найчастіше автори, розглядаючи це поняття, намагаються виділити своє визначення, яке б повністю задовольняло обрану тему. З точки зору різних галузей знань дане поняття описується своїм специфічним набором ознак. "Інформаційний захист" – це організаційні, правові, технічні та технологічні заходи для попередження загроз інформаційній безпеці та усунення їх наслідків. Проблемі розгляду даного поняття присвячено досить багато наукових публікацій. Інформаційний захист набуває все більшого значення, адже в останній час активно розвивається підприємництво.

Провівши аналіз останніх досліджень у сфері інформаційного захисту підприємництва, можна зробити такі висновки. Даній проблемі в літературі присвячено дуже мало уваги. Безліч питань так і залишаються невирішеними. Проблемою інформаційного захисту підприємницької діяльності займається ряд таких авторів і науковців, як: Гасанов Р. М., Ананський Є. В., Кудін Д. В., Красноступ Н. Д., Шпунт Я. В., Гриняєв С. Н. Треба також зазначити, що питання інформаційного захисту та інформаційної безпеки активно обговорюється на наукових прес-конференціях, на національних та міжнародних конференціях, у науковій пресі.

Метою даного дослідження є визначення впливу інформаційної безпеки на діяльність суб'єктів підприємництва та відстеження сучасних тенденцій в галузі інформаційної безпеки.

Для створення і підтримки ефективної та продуктивної діяльності підприємства, воно може здійснювати ряд специфічних заходів. Інформаційний захист на підприємстві є дуже важливим.

У зв'язку зі швидкозмінними умовами ринку кожне підприємство повинно дбати про захист ресурсів підприємства. Вчені досить часто на перший план виносять захист інформації як специфічного і найважливішого ресурсу, що є в обігу підприємств.

Захист інформації – це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [1].

Підприємці повинні не тільки покладатися на державу, але й самі дбати про інформаційну безпеку. Але найчастіше відповідні підрозділі служби безпеки починають створюватися лише тоді, коли конфіденційна інформація вже була втрачена. Починати створення системи треба з оцінки загроз безпеки діяльності комерційного об'єкта, а, виходячи з отриманих результатів аналізу, приймається рішення про побудову всієї системи захисту і вибираються необхідні засоби.

Безпека інформації – це стан захищеності інформації (даних), при якому забезпечуються її (їх) конфіденційність, доступність і цілісність [2].

Під загрозами конфіденційної інформації прийнято розуміти потенційні чи реально можливі дії щодо інформаційних ресурсів, що призводять до неправомірного оволодіння інформацією, яка охороняється. Такими діями є:

- ознайомлення з конфіденційною інформацією різними шляхами і способами без порушення її цілісності;
- модифікація інформації у кримінальних цілях як часткова або значна зміна складу або змісту відомостей;
- руйнування (знищення) інформації як акт вандалізму з метою прямого нанесення матеріального збитку.

Джерелами зовнішніх загроз є: недобросовісні конкуренти; злочинні угрупування та формування; окремі особи та організації адміністративно-управлінського апарату.

Джерелами внутрішніх загроз є адміністрація підприємства; персонал; технічні засоби забезпечення виробничої і трудової діяльності.

Заходи захисту інформації: запобігання – тільки авторизований персонал має доступ до інформації та технології; виявлення – забезпечується раннє виявлення злочинів і зловживань, навіть якщо механізми захисту були обійдені; обмеження – зменшується розмір втрат, якщо злочин все ж таки відбувся, незважаючи на заходи його запобігання і виявлення; відновлення – забезпечується ефективне відновлення інформації при наявності документованих і перевірених планів з відновлення [3].

У 2012 році багато підприємств постраждали від цілеспрямованих атак. Логічно припустити, що великі організації і надалі будуть привертати увагу кібер-злочинців, і тому їм доведеться посилити заходи захисту від Advanced Persistent Threats (APT). Зловмисники створюють програми для злому і заробляють гроші на їх продажу третім особам. Хакери обмінюються інформацією один з одним, тому нові успішні техніки злому швидко поширюються і починають застосовуватися більш широко. Незабаром небезпека цілеспрямованих атак на IT-ресурси компаній вийде на новий рівень: "засоби нападу" стануть настільки дешевими і легкодоступними, що атак слід очікувати не лише великим компаніям, але навіть малому бізнесу й індивідуальним користувачам [4].

Не лише українські, але й зарубіжні підприємства за 2012 рік – початок 2013 року зіштовхнулися з проблемою шкідливого програмного забезпечення (ПЗ) та спаму. На сьогоднішній день є такі дані: українські компанії, що постраждали від шкідливого ПЗ, – 72 %, у тому числі ті, що постраждали від спаму, – 70 % [4].

З метою попередження та мінімізації даних загроз, провідними IT-центрами було розроблено програми, що здійснюють запити на відповідні дані, без яких встановити ту або іншу програму на робочий комп'ютер неможливо. Вже останні дослідження показують ефективність такого підходу.

Дуже значущою для підприємств постала проблема використання персональних мобільних приладів на робочих місцях. Лише за 2012 рік за допомогою мобільних приладів було викрадено приблизно 46 % інформації різноманітних підприємств. Але важливим у вирішенні цього питання є той факт, що дані прилади належать саме працівнику, а отже, є його власністю. Тому, перш за все, потрібно розпочинати роботу саме з цього пункту. Вже сьогодні розпочалася активна робота з користувачами таких мобільних приладів. На деяких підприємствах України заборонено проносити на територію окремих підрозділів такі прилади. Таким чином, значно підвищується рівень інформаційної безпеки підприємства. Але викликають занепокоєння не лише приватні пристрої, але й корпоративні. Приблизно 30 % підприємств вбачають у такого роду способах зв'язку значну проблему, а майже 18 % підприємців повідомляють, що в цьому році почали приділяти значно більше уваги цьому питанню, аніж минулого року.

Також слід зазначити, що більш ніж 44 % компаній втрачають інформацію через вірусні атаки. При цьому помітно зросла кількість випадків втрати критично важливої для бізнесу інформації. За останній рік з такою проблемою зіткнулося майже 25 % підприємств.

Для боротьби із зовнішніми та внутрішніми загрозами, а також із метою підвищення продуктивності праці IT-відділ компанії обмежує доступ користувачів до певних ресурсів. Цікаво те, що перше місце в даному списку займають онлайн ігри. Приблизно 67 % відсотків компаній обмежують їх використання. Приблизно 53 % компаній здійснюють теж саме щодо популярних соціальних мереж. Майже 19 % компаній повністю обмежують доступ до такого типу Інтернет-ресурсів, а майже 23 % накладають обмеження. Цікавим є те, що також на багатьох підприємствах такі обмеження залишаються лише на словах [4].

В останні роки все більшої популярності набувають так звані хмарні технології, або хмарні сервіси. Майже 41 % підприємців вважає, використання "хмари" є реальною можливістю посилити інформаційний захист.

Хмарні технології – це технології, які надають користувачам Інтернету доступ до комп'ютерних ресурсів сервера і використання програмного забезпечення як онлайн-сервісу.

Загалом ця технологія має як плюси, так і мінуси. Вона доволі економічна і доцільна для організацій, корпорацій, фірм тощо. Вона не потребує значних ресурсів обраного пристрою (КПК, планшет, смартфон, нетбук або комп'ютер), але вона вимоглива щодо доступу до Інтернету.

Одним із засобів захисту підприємницької діяльності є перехід документообороту підприємства на хмарні технології. В умовах все більшого наступу українських органів контролю на бізнес цей спосіб стає все актуальнішим. Адже майже всі поштові сервери на вимогу державних органів надають інформацію про своїх користувачів, у тому числі й електронні документи.

Перший плюс – при використанні віддаленого сервера комп'ютери не міститимуть жодної комерційної інформації. Тобто з легкістю можна навіть дати свій комп'ютер для користування будь-кому, і не боятися, що після цього важлива інформація кудись зникне.

Другий плюс – це легкість у користуванні. Інформація відкривається лише тим, хто має на це відповідний дозвіл. У разі виникнення будь-яких форс-мажорів, починаючи з візиту неочікуваних "гостей" і закінчуючи простими несправностями у роботі електропостачання, можна легко припинити роботу і почати її згодом з того місця, де зупинилися.

Третій плюс – повний захист конфіденційної інформації. Можливості послуги дозволяють клієнту чітко регламентувати коло користувачів сервера та маніпуляції, які здійснюються з його даними. Тобто в разі, коли хтось із співробітників вирішить скопіювати чи відправити якийсь файл із сервера, не маючи на те дозволу, його дії будуть просто заблоковані.

Але є також мінуси. Приблизно 21 % підприємців все ж таки вбачають у хмарних технологіях дуже серйозні загрози бізнесу. Але цей відсоток буде знижуватися щороку [4].

За результатами проведеного дослідження можна зробити висновок, що інформаційний захист є одним із найважливих завдань для підприємств. Шкідливе ПЗ, спам, віруси, неуважне поводження співробітників підприємств із конфіденційною інформацією – ось лише невеликий перелік тих проблем, з якими щоденно стикаються IT-фахівці компаній.

Підвищення рівня комп'ютерної грамотності персоналу є одним із найважливіших елементів захисту, а розуміння актуальних загроз і шляхів захисту від них необхідно для ефективного розвитку IT-інфраструктури підприємства.

У даний момент менше половини фахівців вважають свою компанію готовою до боротьби з сучасними загрозами, а передумови для серйозної зміни цієї ситуації поки недостатньо сильні.

Дуже важливим є впровадження на підприємствах таких методів захисту, як шифрування інформації, увага до персональних даних, готовність до цільових атак та робота з персоналом.

Наук. керівн. Петряєва З. Ф.

Література: 1. Про доступ до публічної інформації : Закон України "Відомості Верховної Ради України" (ВВР) – 2011. – № 32. – С. 314. 2. Красноступ Н. Д. Шпионские программы и методы защиты от них, НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа / Н. Д. Красноступ, Д. В. Кудин // Департамент специальных телекоммуникационных систем и защиты информации Службы безопасности Украины. – К., 2008. 3. Ананский Е. В. Защита информации – основа безопасности бизнеса / Е. В. Ананский // Бизнес и бизопасность. – 2009. – № 3. 4. Безпека організацій [Електронний ресурс]. – Режим доступу : http://www.bezopasnik.org/article/index.htm. 5. Гасанов Р. М. Шпионаж особого рода / Р. М. Гасанов. – М. : Мысль, 1989. – 276 с. 6. Гриняев С. Н. Современные тенденции в области защиты информации и информационной борьбы / С. Н. Гриняев // Сборник статей. – М. : МАКБП, 2000. – 334 с. 7. Гриняев С. Н. Информационная безопасность избирательных кампаний / С. Н. Гриняев, В. Н. Кудрявцев, Б. У. Родионов. – М. : МАКБП, 1999. – 104 с. 8. Шпунт Я. В. Угрозы в области информационной безопасности. Новые тенденции / Я. В. Шпунт // Информационная безопасность и непрерывность бизнеса. Спецвып. № 7. – М. : Intelligent Enterprise/Корпоративные системы, 2007. – С. 12–17.