Марунич А. В.

УДК 316.774-049.5

Магістр 1 року навчання
факультету обліку і аудиту ХНЕУ ім. С. Кузнеця

ЗАХИСТ ІНФОРМАЦІЇ ЯК ОСНОВНА СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Анотація. Визначено сутність поняття "інформаційна безпека підприємства" з різних точок зору. Розглянуто основні проблемні питання забезпечення інформаційної безпеки підприємства. Виявлено головні загрози впливу на інформаційну безпеку підприємства та запропоновано заходи щодо їх усунення.

Аннотация. Определена сущность понятия "информационная безопасность предприятия" с разных точек зрения. Рассмотрены основные проблемные вопросы обеспечения информационной безопасности предприятия. Выявлены главные угрозы влияния на информационную безопасность предприятия и предложены меры по их устранению.

Annotation. The essence of the concept of information security has been defined from different perspectives. The major issues of information security of a company have been considered. The main threats of the impact on information security of a company have been identified and measures to eliminate them have been proposed.

Ключові слова: інформація, інформаційна безпека підприємства, захист конфіденційної інформації, загрози, інформаційні ризики.

Сьогодні інформаційна сфера складає інтегруючу основу життєдіяльності суспільства, а забезпечення інформаційної безпеки визнається однією з концептуальних засад його подальшого розвитку. Значення інформації в житті людини сьогодні складно переоцінити. Діяльність щодо отримання та обробки інформації займає досить багато часу. Підсвідомо людина зіштовхується з величезною кількістю джерел інформації і є, відповідно, частиною глобального інформаційного обміну. У той же час в умовах розвитку інформаційних технологій процес пошуку й обробки інформації істотно прискорюється, що робить доступними практично будь-які джерела інформації в умовах реального часу. Цілеспрямовані або ненавмисні впливи на інформаційну сферу з боку зовнішніх або внутрішніх джерел можуть завдавати серйозної шкоди цим інтересам і становлять загрози та ризики для безпеки. Тому інформаційна безпека в сучасних умовах є однією з необхідних умов нормального функціонування підприємства [1].

Усе більш очевидною стає залежність загального рівня економічної безпеки підприємства від інформаційної складової. Розуміючи важливість інформаційного розвитку української держави та входження до світового інформаційного простору, Законом України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" було задекларовано, що розвиток інформаційного суспільства в Україні та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя визначається одним із пріоритетних напрямів державної політики [2].

У цілому інформація пронизує усі сфери життя суспільства, створюючи нову основу розвитку економіки, культури і взагалі нову характеристику соціуму.

Вивченням питання інформаційної безпеки займалися такі вчені, як: Кормич Б. А., Іванов О. В., Сергієнко Л. А., Бачило І. Л., Цимбалюк В. С., Фурашев В. М., Гуцу С. Ф., Тацюра М. Ю., Марущак А. І., Сороківська О. А. [1 – 10].

Проте, проблема інформаційної безпеки підприємства залишається недостатньо дослідженою. Це пов'язано з тим, що автори більшу увагу приділяють забезпеченню інформаційної безпеки держави, а також відсутністю цілеспрямованого підходу до проблеми в цілому у тих учених, які розглядали роль інформації в діяльності підприємства.

Мета статті полягає у вивченні основних вимог щодо забезпечення інформаційної безпеки підприємства, в розробці основних заходів щодо попередження виникнення загроз втрати та знищення інформації.

У системі забезпечення безпеки все більшого значення набуває забезпечення інформаційної безпеки підприємства. Це пов'язано зі зростаючим об'ємом інформації, що поступає, вдосконаленням засобів її зберігання, передачі та обробки. Перехід значної частини інформації в електронну форму, використання локальних і глобальних мереж створюють якісно нові загрози

конфіденційної інформації. Необхідно зазначити, що у наукові літературі відсутній єдиний погляд на зміст поняття "інформаційна безпека підприємства", що є надзвичайно актуальним на сучасному етапі розвитку інформаційних технологій і супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору.

Так, О. Сороківська визначає інформаційну безпеку підприємства як суспільні відносини щодо створення і підтримки на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [7]. М. Танцюра характеризує інформаційну безпеку підприємства як збереження конфіденційності, цілісності та доступності інформації; доступність – це властивість бути досяжним та придатним до використання авторизованими сутностями; цілісність – це властивість захищеності точності та повноти даних; конфіденційність – це властивість захищеності інформації від неавторизованого використання фізичними особами, сутностями та процесами. Інформаційні активи – це знання чи дані, які мають цінність для організації [9].

Враховуючи дані визначення, варто погодитись з А. Марущаком, який наголошує, що інформаційна безпека підприємства – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів з досягнення стану захищеності інформаційного середовища організації [8].

Отже, підсумовуючи зазначене, варто наголосити, що пріоритетним напрямом у процесі забезпечення інформаційної безпеки підприємства є збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг.

Погіршення на підприємстві таких параметрів інформації, як конфіденційність, цілісність, доступність, достовірність тощо, може призвести до досить негативних наслідків: збоїв у функціонуванні систем управління технологічними процесами й іншими критичними системами; розголошення відомостей, що становлять комерційну й інші види таємниць; порушення достовірності персональних даних фізичних осіб.

Результатом перерахованого можуть стати: погіршення ділових відносин із партнерами; зриви переговорів, втрата вигідних контрактів; невиконання договірних зобов'язань; необхідність проведення додаткових ринкових досліджень; відмовлення від рішень, що стали неефективними через розповсюдження інформації, і, як наслідок, – фінансові втрати, пов'язані з новими розробками; втрата можливості запатентувати результат науково-технічної діяльності або продати ліцензію; зниження цін або обсягів реалізації; втрати ділової репутації; більш жорсткі умови одержання кредитів; труднощі в постачанні і придбанні устаткування тощо [5].

У визначених ситуаціях зневага питаннями захисту інформації може призвести до повного банкрутства. Тому питання аналізу загроз і ризиків є визначальним під час побудови ефективної системи захисту інформації.

Водночас дії внутрішніх порушників, такі, як недбалість співробітників, крадіжки інформаційних ресурсів та IT-устаткування, фінансові й інші види шахрайства з використанням інформаційних систем і ресурсів тощо, набагато рідше стають предметом уваги у ході розв'язання проблем інформаційної безпеки у випадку, якщо вони розглядаються у відриві від загальних завдань забезпечення економічної безпеки.

Результати досліджень показують, що більшість підприємств не вживають достатніх заходів для захисту від дій інсайдерів. Хоча навмисних атак зловмисників стає все більше, практика показує, що випадкові помилки, неуважність до правил безпеки впливають на діяльність підприємства набагато більше, ніж атаки шахраїв. Багато керівників підприємств можуть не бачити очевидного зв'язку між утратою доходів і відсутністю фінансових ресурсів у системі інформаційного захисту. Тому, в першу чергу, необхідно подати проблему у зрозумілому для бізнесу вигляді. Це завдання керівництва служби інформаційної безпеки господарюючого суб'єкта, що має виявити і наочно показати власникам підприємства весь спектр загроз в інформаційній сфері, а також переконати, що протистояти їм можна тільки на основі створення і упровадження ефективних систем захисту інформації [5].

Створюючи такі системи, необхідно враховувати, що, по-перше, для ефективного захисту інформаційних ресурсів потрібна реалізація цілої низки різноманітних заходів, які можна розподілити на три групи: юридичні, організаційно-економічні й технологічні. По-друге, хоча розробкою заходів у кожній із трьох груп повинні займатися фахівці відповідних галузей знань, які застосовують свої способи і методи для досягнення заданих цілей, кінцевий успіх значною мірою буде залежати від того, наскільки в рамках системного підходу вдасться визначити і реалізувати взаємні зв'язки між відповідними визначеннями, принципами, способами і механізмами захисту.

Аналіз поглядів і концептуальних підходів до формування сучасних ефективних систем інформаційної безпеки підприємства дозволив сформулювати основні функції та завдання і намітити організаційні основи функціонування відповідних підрозділів інформаційної безпеки.

У сучасному поданні рольових функцій служби інформаційної безпеки можна виділити чотири напрями [4]:

1) розробка методології та методик аналізу загроз, оцінки рівня інформаційної безпеки підприємства і системи її забезпечення;

2) організація і здійснення конкретних видів діяльності із захисту інформації;

3) експлуатація технічних засобів захисту інформації;

4) аудит і контроль функціонування системи інформаційної безпеки підприємства.

Далі необхідно з'ясувати, наскільки серйозні втрати може принести підприємству настання інформаційного ризику на кожен конкретний інформаційний об'єкт. Втрати від настання інформаційного ризику можуть бути подані у такий спосіб (таблиця) [4].

Таблиця

Втрати від настання інформаційного ризику

Величини ризику	Опис
0,1 – 0,2	Оголошення інформації принесе незначні моральні і фінансові втрати підприємству
0,2 – 0,3	Втрати від інформаційної атаки є, але вони незначні, основні фінансові операції і становище підприємства на ринку не порушено
0,3 – 04	Фінансові операції не ведуться протягом деякого часу, за цей час підприємство зазнає збитків, але його становище на ринку і кількість клієнтів змінюються мінімально
0,4 – 0,6	Значні втрати на ринку й у прибутку. Підприємство втрачає значну частину клієнтів
0,6 – 0,8	Втрати дуже значні, підприємство на період до року втрачає становище на ринку. Для відновлення становища потрібні великі фінансові інвестиції
0,8 – 1,0	Підприємство припиняє існування

Необхідно зазначити, що класифікацію збитку, нанесеного атакою, має оцінювати власник інформації або працюючий із нею персонал. Оцінку ймовірності появи атаки краще довіряти технічним співробітникам підприємства.

З різних організаційних схем функціонування підрозділів, що відповідають за інформаційну безпеку підприємства (функції такого підрозділу покладаються на системних адміністраторів; зазначений підрозділ знаходиться у структурі служби інформаційної безпеки, що підкоряється вищому керівництву), найкращим є варіант, за якого підрозділ інформаційної безпеки входить до складу служби економічної безпеки підприємства. Саме в цьому випадку створюються найкращі можливості розв'язання проблем інформаційної безпеки в контексті загальних завдань безпеки бізнесу.

Таким чином, у сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки господарюючого суб'єкта. У свою чергу, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, але й національної економіки в цілому. Особливої уваги потребує реальне втілення запропонованих заходів щодо забезпечення інформаційної безпеки, які мають стати основою для формування та реалізації інформаційної політики підприємства, захисту інформації від внутрішніх та зовнішніх загроз.

Наук. керівн. Петряєва З. Ф.

Література: 1. Бачило И. Л. Гражданское общество и право / И. Л. Бачило // Информационные ресурсы России. – 2005. – № 3. – С. 10–15. 2. Про основні засади інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 9 січня 2007 року // Офіційний вісник України. – 2007. – № 8. – Ст. 273. 3. Гуцу С. Ф. Правові основи інформаційної діяльності : навч. посіб. / С. Ф. Гуцу. – Х. : Нац. аерокосм. ун-т "Харк. авіац. ін-т", 2009. – 48 с. 4 Иванов О. В. Информационная составляющая современных войн / О. В. Иванов // Вестн. Моск. ун-та. Сер. 18 : Социология и политология. – 2004. – № 4. – С. 64–70. 5. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. д-ра юрид. наук / Б. А. Кормич. – Х., 2004. – 44 с. 6. Сергиенко Л. А. Культура и гражданское общество / Л. А. Сергиенко // Информационные Ресурсы России. – 2007. – № 6. – С. 1–6. 7. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи [Електронний ресурс] / О. А. Сороківська. – Режим доступу : http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2 010_2_2/032-035.pdf. – Назва з екрану. 8. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки / А. І. Марущак // Державна безпека України. – 2011. – № 21. – С. 92–95. 9. Тацюра М. Ю. Проблемні аспекти стандартизації у галузі інформаційної безпеки підприємства / М. Ю. Тацюра // Матеріали Другої наук.-практ. конф. "Сталий розвиток та екологічна безпека суспільства в економічних трансформаціях" 23–24 вересня 2010 року, м. Бахчисарай, НДІ сталого розвитку та природокористування, РВПС України НАН України, Кримський інститут КНЕУ ім. Вадима Гетьмана / М. Ю. Тацюра. – Сімферополь : Фенікс, 2010. – С. 451–453. 10. Цимбалюк В. С. Окремі питання щодо визначення категорії "інформаційна безпека" у нормативно-правовому аспекті / В. С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004. – № 8. – С. 30–33. 11. Фурашев В. М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки / В. М. Фурашев // Інформація і право: науковий журнал. – К. : НДЦПІ НАПрН України, 2012. – № 1(4). – С. 46–56.