УДК 005.92:004.056

Нечай Л. О.

Магістр 2 року навчання
факультету обліку і аудиту ХНЕУ

ІНФОРМАЦІЙНА БЕЗПЕКА СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ ТА ФАКТОРИ ЇЇ РОЗВИТКУ

Анотація. Розглянуто сутність інформаційної безпеки як важливої складової економічної безпеки підприємства. Визначено основні проблеми, пов'язані з захистом інформації на підприємстві, та можливі шляхи їх усунення. Запропоновано заходи щодо створення ефективної системи інформаційної безпеки суб'єктів господарювання.

Аннотация. Рассмотрена сущность информационной безопасности как важной составляющей экономической безопасности предприятия. Определены основные проблемы, связанные с защитой информации на предприятии, и возможные пути их устранения. Предложены мероприятия по созданию эффективной системы информационной безопасности субъектов хозяйствования.

Annotation. The article describes the essence of information security as part of the economic security of the enterprise. The main problems related to the protection of information at the enterprise are considered and possible ways to handle them are offered. Measures to create an effective information security of economic entities ave suggested.

Ключові слова: економічна безпека, інформаційна безпека, конкуренція, економічні загрози, промислове шпигунство, заходи безпеки, джерела загроз.

Стабільне функціонування, зростання економічного потенціалу будь-якого підприємства в умовах ринкових відносин багато в чому залежить від наявності надійної системи економічної безпеки. Інформація, яка стосується всіх напрямів діяльності підприємства, стає найбільш цінним і дорогим ресурсом, а проблема захисту інформації посилюється появою нових загроз. Тому інформаційна безпека є однією зі складових частин економічної безпеки, яка формує модель захищеності підприємства від внутрішніх та зовнішніх загроз.

Питанням інформаційної безпеки присвячено наукові праці зарубіжних та вітчизняних вчених, таких, як: О. Голубченко, А. Циплаков, Т. Васильців, В. Богуш, О. Юдін, Л. Донець, Н. Ващенко, В. Цимбалюк, Т. Ткачук, Є. Степанова та ін. [1 – 9].

Так, Голубченко О. Л. під інформаційною безпекою організації розуміє цілеспрямовану діяльність її органів та посадових осіб із використанням дозволених сил і засобів з досягнення стану захищеності інформаційного середовища підприємства, що забезпечує її нормальне функціонування і динамічний розвиток [1].

Циплаков А. С. пропонує розглядати визначення інформаційної безпеки підприємства як набір засобів, методів і робіт, орієнтованих на захист інформаційної інфраструктури підприємства від будь-яких зовнішніх або внутрішніх загроз, які можуть призвести до крадіжки, псування, або несанкціонованої зміни даних на серверах або робочих станціях [2].

Васильців Т. Г. визначає інформаційну безпеку підприємства як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [3].

Більшість науковців під інформаційною безпекою підприємства розуміють комплекс організаційно-управлінських, режимних, технічних, профілактичних заходів, спрямованих на захист інформаційного середовища організації від внутрішніх та зовнішніх загроз.

Таким чином, мова йде про захист інформації, якою володіє підприємство (виробляє, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні. Крім того, під інформаційною безпекою розуміється захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може бути нанесення збитку самій інформації, її власникам або підтримуючій інфраструктурі.

Інформаційна безпека підприємства на практиці включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку. Елементами цієї системи є: правовий, організаційний, інженерно-технічний захист інформації, а основною її характеристикою – комплексність. Структура системи, склад і зміст елементів, їх взаємозв'язок залежать від об'єму та цінності інформації, яку захищають, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи.

Погіршення стану криміногенної обстановки в державі, спроби суб'єктів господарювання та представників окремих політичних сил впливати на перерозподіл власності, протиправні дії конкурентів, зростання їх фінансових потужностей та технічної оснащеності, корпоративний шантаж, дає підстави вважати, що найближчим часом буде зберігатися тенденція до ускладнення оперативної обстановки навколо суб'єктів господарювання [2]. Визначення та прогнозування можливих загроз і усвідомлення їх небезпеки необхідні для обґрунтування, вибору та реалізації захисних заходів, що адекватні загрозам для інтересів підприємства [3].

Таким чином, джерела зовнішніх загроз можуть бути випадковими і запланованими та мати різний рівень

кваліфікації (кримінальні структури, потенційні злочинці і хакери, нечесні партнери, технічний персонал постачальників послуг тощо).

У свою чергу, існують не менш небезпечні внутрішні джерела загроз до яких, як правило, відносяться висококваліфіковані фахівці у галузі розробки та експлуатації програмного забезпечення і технічних засобів, знайомі зі специфікою розв'язуваних завдань, структурою й основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, які мають можливість використання штатного устаткування і технічних засобів мережі (основний персонал, представники служби захисту інформації, допоміжний персонал, технічний персонал).

Також потребують уваги технічні засоби, що є джерелами потенційних загроз безпеки інформації, які можуть бути зовнішніми, а саме: засоби зв'язку, мережі інженерних комунікацій, транспорт та внутрішніми – неякісні технічні засоби обробки інформації, неякісні програмні засоби обробки інформації, допоміжні технічні засоби.

Сутність загроз інформаційної безпеки зводиться, як правило, до нанесення того чи іншого збитку підприємству (організації). Тобто моральна і матеріальна шкода діловій репутації організації; моральний, фізичний чи матеріальний збиток, пов'язаний із розголошенням персональних даних окремих осіб, матеріальний (фінансовий) збиток від розголошення конфіденційної інформації чи збиток від дезорганізації в роботі всього підприємства [4].

Сучасний стан інформаційної безпеки відрізняється її нестабільністю. Це означає, що підприємство повинно застосовувати щоденні методи захисту, які відповідали б його специфіці.

Виходячи з проведеного дослідження, найбільш важливими факторами становлення системи інформаційної безпеки підприємств є:

відсутність єдиної державної політики в галузі забезпечення інформаційної безпеки підприємств;

недосконаліть нормативної правової бази, що регулює відносини в галузі забезпечення інформаційної безпеки підприємств, а також недостатня правозастосовна практика;

недостатній контроль за розвитком інформаційного ринку з боку державних структур і суспільства;

низький рівень захищеності інтересів фізичних і юридичних осіб в інформаційній сфері.

Узагальнюючи сучасний стан інформаційної безпеки підприємств, можна визначити основні фактори і перспективи її розвитку:

удосконалення законодавства у сфері інформаційної безпеки сприятиме її розвитку, а також дотриманню всіх встановлених норм і правил;

на підприємствах слід створювати і впроваджувати системи інформаційної безпеки, що сприятиме комплексному захисту інформації в країні в цілому;

удосконалення методів захисту інформації – шлях до захисту від найбільш небезпечних загроз, які становлять небезпеку підприємству;

для захисту комерційної інформації організацій, повинні залучатися державні кошти, так само, як виділяються кошти на захист державної таємниці. Часом витік комерційної інформації підприємства може привести до серйозних негативних наслідків, а також погіршення іміджу країни та інвестиційної привабливості;

підприємствам слід створювати служби інформаційної безпеки, або покладати ці функції на співробітників, компетентних у даній сфері;

підприємствам слід приділяти особливу увагу як при працевлаштуванні співробітників, так і при їх звільненні, дотримуючись усіх норм безпеки та попереджаючи витік інформації. Трудовий договір, що підписується співробітником, повинен неодмінно містити пункт про нерозголошення комерційної таємниці;

суб'єктам господарювання слід користуватися виключно ліцензійними засобами захисту інформації і послугами перевірених фірм, що мають репутацію і пройшли ліцензування;

підприємствам слід звести до мінімуму використання співробітниками портативних носіїв інформації на підприємстві, а також мати доступ до корпоративних досліджень.

Варто відмітити той факт, що збереження бізнесу, його розвиток і підтримка конкурентоспроможності підприємства потребують створення ефективної системи управління інформаційною безпекою, комплекс організаційних, технічних, програмних і криптографічних, засобів і заходів щодо захисту інформації в процесі традиційного документообігу при роботі виконавців із конфіденційними документами і відомостями, при обробці інформації в автоматизованих системах різного рівня та призначення, при передачі каналами зв'язку, при веденні конфіденційних переговорів.

Слід зазначити, що інформаційна безпека підприємства забезпечується власними силами суб'єктів господарювання, їх службою безпеки або уповноваженою особою завданнями яких є забезпечення безпеки підприємства, виробництва, продукції та захист комерційної, промислової, фінансової, ділової та іншої інформації незалежно від її призначення і форми при всій різноманітності можливих каналів її розповсюдження та різноманітних дій конкурентів. Тому підбір кадрів повинен виконуватись на належному рівні, оскільки недостатні професійні знання, некомпетентність може призвести до серйозних наслідків, що можуть безпосередньо вплинути на фінансову діяльність і стійкість підприємства на ринку.

У галузі захисту інформації, завдання забезпечення інформаційної безпеки повинні вирішуватися системно, тобто різні засоби захисту (апаратні, програмні, фізичні, організаційні і т. д.) повинні застосовуватися одночасно і під централізованим управлінням. При цьому компоненти системи повинні "знати" про існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і від внутрішніх загроз.

На сьогоднішній день існує велика кількість методів забезпечення інформаційної безпеки: засоби ідентифікації та автентифікації користувачів; засоби шифрування інформації, що зберігається на комп'ютерах і передається по мережах; міжмережні екрани; віртуальні приватні мережі; засоби контентної фільтрації; інструменти перевірки цілісності вмісту дисків; засоби антивірусного захисту; системи виявлення вразливостей мереж і аналізатори мережних атак.

Усе більшою популярністю для захисту інформації користуються криптографічні методи. Інтерес комерційних структур до них значно зріс у зв'язку зі зменшенням вартості перехоплення інформації, що передається електронною поштою чи функціонує в системі електронних платежів. Найпоширенішими вважаються методи кодування та шифрування інформації. Поряд з ними використовуються методи розділення та стиснення даних.

У процесі захисту передачі усної інформації використовують методи аналогового скемблірування та дискретизації мови з подальшим шифруванням.

Один із перспективних напрямів захисту інформації сформулювали сучасні методи стенографії, що базуються на різних принципах, забезпечують таємницю самого факту існування секретної інформації в тому чи іншому середовищі за допомогою відповідних засобів: невидимих чорнил, мікрофотознімків, таємних каналів та засобів зв'язку з плаваючими частотами тощо.

Незважаючи на використання зазначених методів, забезпечення інформаційної безпеки підприємства на належному рівні можливе лише тоді, коли інформаційна складова економічної безпеки розглядатиметься як невід'ємний елемент процесу управління підприємством.

Таким чином, проблема інформаційної безпеки має дуже загострений характер, оскільки разом з величезною кількістю методів захисту інформації, збільшується та урізноманітнюється кількість потенційних загроз і дестабілізуючих факторів. Таким чином, керівництво підприємства повинно прогнозувати можливі чинники зниження захищеності інформації та оснащувати себе системами захисту від них.

На сьогодні, питання безпеки інформації потрібно розглядати не просто як розробку приватних механізмів захисту, а як реалізацію системного підходу, що включає комплекс взаємопов'язаних заходів, які повинні розширюватись та вдосконалюватись. Тому впровадження регламентів інформаційної безпеки при використанні телекомунікацій, дотримання персоналом внутрішніх нормативних актів, а також досягнення конфіденційності, цілісності та доступності інформації дозволять не тільки підвищити результативність системи інформаційної безпеки, але і будуть сприяти зміцненню зовнішніх позицій підприємства.

Наук. керівн. Петряєва З. Ф.

Література: 1. Голубченко О. Л. Політика інформаційної безпеки / О. Л. Голубченко. – Луганськ : Вид. СНК ім. В. Даля. 2009. – 300 с. 2. Циплаков А. С. Стратегія забезпечення належної економічної безпеки підприємства / Циплаков А. С. – К. : Істина, 2004. – 144 с. 3. Васильців Т. Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення : монографія / Т. Г. Васильців. – Львів : Арал, 2008. – 154 с. 4. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К. : МК-Прес, 2006. – 432 с. 5. Донець Л. І. Економічна безпека підприємства : навч. посібн. / Л. І. Донець, Н. В. Ващенко. – К. : Центр учбової літератури, 2008. – 240 с. 6. Цимбалюк В. С. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальні кіберцивілізації) / В. С. Цимбалюк // Підприємництво, господарство і право. – 2007. – № 3. – С. 88–91. 7. Ткачук Т. П Формування системи інформаційної безпеки бізнесу / Т. Ткачук // Бізнес і безпека. – 2009. – № 4. – С. 19–23. 8. Степанова О. М. Розвиток інформаційної системи підприємства / О. М. Степанова // Вісник Східноукраїнського національного університету ім. В. Даля – 2008. − № 20. – С. 47–43. 9. Прокоф'єва Д. М. Підприємницьке шпигунство в системі інформаційних злочинів [Електронний ресурс] / Д. М. Прокоф'єва // Украинский центр информационной безопасности. – Режим доступу : www.bezpeka.com/library/lib_aspect.html.