МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Полукаров О. І., канд. техн. наук (каф. ОППЦБ КПІ ім. Ігоря Сікорського);
Гогот М. М., студентка (гр. УВ-51, ФММ КПІ ім. Ігоря Сікорського)

Прогрес зробив компанії залежними від інформаційних технологій, а з іншої сторони – вразливими до атак хакерів, комп'ютерних вірусів такою мірою, що багато керівників та власників підприємств вже не можуть відчувати себе в повній безпеці. Питання інформаційної безпеки стає важливим фактором у діяльності компанії, але разом з тим прогрес пропонує рішення, які можуть захистити інформацію та дані від зовнішніх проникнень.

Так що ж таке інформаційна безпека? Зазвичай під нею розуміють захищеність інформації і всієї компанії від навмисних або випадкових дій, що призводять до нанесення шкоди її власникам або користувачам. Забезпечення інформаційної безпеки має бути спрямована перш за все на запобігання ризиків, а не на ліквідацію їх наслідків. Саме прийняття запобіжних заходів для забезпечення конфіденційності, цілісності, а також доступності інформації і є найбільш правильним підходом у створенні системи інформаційної безпеки [3].

Будь-який витік інформації може призвести до серйозних проблем для компанії – від значних фінансових збитків до повної ліквідації. Звичайно, проблема витоків з'явилася не сьогодні, промислове шпигунство і переманювання кваліфікованих фахівців існували ще й до епохи комп'ютеризації. Але саме з появою ПК та інтернету виникли нові прийоми незаконного отримання інформації. Якщо раніше для цього необхідно було вкрасти і винести з фірми цілі стоси паперових документів, то зараз величезні обсяги важливих відомостей можна запросто завантажити на флешку або просто знищити за допомогою вірусів, влаштувавши диверсію.

Найчастіше «витікають» з компаній документи фінансового характеру, технологічні і конструкторські розробки, логіни і паролі для входу в мережу інших організацій. Але серйозної шкоди може завдати також витік персональних даних співробітників. Особливо це актуально для західних країн, де судові позови через таких витоків нерідко призводять до величезних штрафів, після виплати яких компанії зазнають серйозних збитків [2].

Але що найчастіше викликає загрози інформаційній безпеці?

1. Недбалість та/або неуважність працівників. Загрозу інформаційній безпеці компанії можуть нести цілком лояльні працівники, які навіть не замислюються про викрадення важливої інформації та даних. Ненавмисна шкода конфіденційній інформації завдається через звичайну недбалість або неуважність працівників.

2. Використання піратського ПЗ. Інколи керівники підприємств намагаються заощадити на купівлі ліцензійного програмного забезпечення. Але необхідно знати, що неліцензійні програми не дають достатнього захисту від

шахраїв, які зацікавлені у викраденні важливої для підприємства інформації за допомогою вірусів.

3. Віруси. Комп'ютерні віруси – це одна з найнебезпечніших сьогодні загроз інформаційній безпеки. Це підтверджують багатомільйонними збитками, які несуть компанії через вірусні атаки. Останнім часом значно збільшилась їх частота та рівень шкоди. Експерти вважають, що це можна пояснити появою нових каналів для проникнення вірусів.

4. Загрози з боку співвласників бізнесу. Саме легальні користувачі - одна з основних причин витоків інформації в компаніях. Такі витоку фахівці називають інсайдерськими [1].

Хоча кількість загроз постійно зростає, з'являються все нові й нові віруси, збільшується інтенсивність і частота хакерських атак, розробники засобів захисту інформації теж не стоять на місці. На кожну загрозу розробляється нове захисне ПЗ або вдосконалюється вже наявне.

Більшість сучасних підприємств приділяють багато уваги онлайн-присутності бізнесу. Для організації інформація є його цінним активом. Інформація про клієнтів, інформація про співробітників, комерційна таємниця - все це становить інформацію. Інформація складається з кожного біта даних, що проходить через організацію [5].

Незахищена інформація часто піддається порушенням та несанкціонованому доступу. Важливі дані в невірних руках не тільки призводять до падіння бізнесу, але також призводять до більш серйозних наслідків, таких як залякування, переслідування та експлуатація.

Ефективність безпеки інформації посилюється тим фактом, що організації тепер більш взаємопов'язані, ніж будь-коли. Основна частина конфіденційних даних, які піддаються постійно зростаючим інтернет-загрозам (наприклад, шкідливим кодам, хакерству та ін.), потребує регулярної безпеки. Зараз багато працівників працюють через Інтернет. З податкових записів до персональних електронних листів, усе перебуває під загрозою несанкціонованого доступу [4].

Інформаційна безпека – це завжди комплексна система, всі складові якої мають не допустити витоку конфіденційних відомостей технічними каналами, а також перешкодити сторонньому доступу до носіїв інформації. Все це, відповідно, гарантує цілісність даних при роботі з ними: обробці, передачі і зберіганні, які повинні здійснюватися обов'язково в правовому полі. Грамотно організовані технічні заходи дозволяють визначити використання спеціальних електронних пристроїв несанкціонованого зняття інформації, розміщених як в приміщенні, так і в засобах зв'язку [2].

Відомі на сьогоднішній день загальні методи забезпечення інформаційної безпеки складаються з *організаційно-технічних, економічних* та *правових*.

Організаційно-технічні методи інформаційної безпеки включають [1]:

- систему забезпечення інформаційної безпеки (під нею ми маємо на увазі комплекс заходів (внутрішні правила роботи з даними, регламент передачі відомостей, доступ до них і т. д.) і технічних засобів (використання програм і приладів для збереження конфіденційності даних));

• розробку, експлуатацію і вдосконалення вже наявних засобів захисту інформації;

• перманентний контроль над дієвістю заходів, що проводяться в галузі забезпечення інформаційної безпеки.

Останній пункт особливо важливий. Без методики оцінки дуже важко визначити ефективність інформаційної безпеки. Якщо ефективність падає, то необхідно терміново вносити корективи (для цього і потрібна перманентність контролю).

Вони тісно взаємопов'язані з правовими методами інформаційної безпеки. **Правові** методи безпеки складаються з [1]:

• ліцензування діяльності в частині забезпечення інформаційної безпеки;

• сертифікації технічних засобів інформаційного захисту;

• атестації об'єктів інформатизації згідно відповідності нормам інформаційної безпеки.

Третя складова, **економічна**, включає [1]:

• складання програм по забезпеченню інформаційної безпеки;

• визначення джерел їх фінансового забезпечення;

• розробку порядку фінансування;

• створення механізму страхування інформаційних ризиків.

Що ж стосується економічної складової інформаційної безпеки, то її основне правило – вартість системи інформаційної безпеки не повинна бути вище, ніж вартість відомостей, які необхідно захистити. Окрім цього, необхідно захищати заздалегідь певну інформацію, а не всю підряд (останнє недоцільно з економічної точки зору).

Серед засобів інформаційного захисту можна виокремити [3, 5]:

1. Фізичні засоби захисту інформації. До них відносяться обмеження або повна заборона доступу сторонніх осіб на територію, пропускні пункти, які оснащені спеціальними системами. Також великого поширення набули карти для контролю доступу.

2. Базові засоби захисту електронної інформації. Це незамінний компонент для забезпечення інформаційної безпеки компанії. До цих засобів відносяться численні антивірусні програми, а також системи фільтрації електронної пошти, які захищають користувача від небажаної або підозрілої кореспонденції. Корпоративні поштові скриньки обов'язково мають бути обладнані такими системами. Крім того, необхідна організація диференційованого доступу до інформації та систематична зміна паролів.

3. Резервне копіювання даних. Це рішення, яке має на увазі зберігання важливої інформації не лише на конкретному комп'ютері, але і на інших пристроях: зовнішньому носії або сервері. Останнім часом особливо актуальною стала послуга віддаленого зберігання різної інформації в «хмарі» дата-центрів.

4. План аварійного відновлення даних. Крайній захід захисту інформації після втрати даних. Такий план необхідний кожній компанії для

того, щоб в максимально стислі терміни усунути ризик простою і забезпечити безперервність бізнес-процесів.

5. Шифрування даних при передачі інформації в електронному форматі (end-to-end protection). Щоб забезпечити конфіденційність інформації при її передачі в електронному форматі застосовуються різні види шифрування. Шифрування дає можливість підтвердити справжність інформації, що передається, захистити її при зберіганні на відкритих носіях, захистити програми та інші інформаційні ресурси компанії від несанкціонованого копіювання та використання.

Отже, захист інформації повинна здійснюватися комплексно, відразу по декількох напрямках. Чим більше методів буде задіяно, тим менше ймовірність виникнення загроз і витоку, тим стійкіше положення компанії на ринку.

Питання інформаційної безпеки займає все більш важливе місце в діяльності компанії. Успіх підприємницької діяльності значною мірою залежить від уміння розпоряджатися таким цінним товаром, як інформація, адже головним ресурсом замість капіталу стає саме інформація.

Література

1. Герасименко О. В. Інформаційна безпека підприємства: поняття та методи її забезпечення / О. В. Герасименко, А. В. Козак. – 2015. – №2.
2. Низенко Е. І. Забезпечення інформаційної безпеки підприємництва: / Е. І. Низенко, В. П. Каленяк. – Київ, 2014. – 134 с. – (МАУП).
3. Северина С. В. Інформаційна безпека та методи захисту інформації / С. В. Северина. // Вісник Запорізького національного університету. – 2016. – №1. – С. 155–160.
4. Методи забезпечення інформаційної безпеки [Електронний ресурс] // Навчальні матеріали онлайн – Режим доступу до ресурсу: https://pidruchniki.com/15950210/politologiya/metodi_zabezpechennya_informatsiynoyi_bezpeki.
5. Ensure information security and awareness in the workplace [Електронний ресурс] // 360training – Режим доступу до ресурсу: https://www.360training.com/blog/ways-to-ensure-information-security/.