Лапа Олександр
студент
Македон Галина
асистент
ВП НУБіП України «Ніжинський агротехнічний інститут»
м. Ніжин

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Зі зростанням науково-технічного прогресу буде зростати важливість питання інформаційної безпеки. Інформаційну безпеку трактують як стан захищеності встановлених законодавством норм та параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини та суспільства як суб'єктів цих процесів та відносин

У світі навіть існує Міжнародний день захисту інформації, який святкується 30 листопада. Про нього в 1988 році оголосила американська Асоціація комп'ютерного обладнання. В цьому році було зафіксовано першу масову епідемію хробака і фахівці задумалися над необхідністю комплексного підходу до забезпечення захисту інформації.

Ще один факт, що підтверджує важливість даного виду управління – результати опитування компанії PriceWaterHause Coopers, яке вона провела у 2014 році серед 10 тис топ-менеджерів із 115 країн світу.

Так світове зростання кількості інцидентів в області інформаційної безпеки в 2012 році складало 17%, а у 2013 – 25%.

Основними джерелами загрози інформаційній безпеці респонденти називали: хакерів (32%), нинішніх співробітників (31%), колишніх співробітників (27%), поточних постачальників послуг (19%), конкурентів (14%). Це свідчить про те, що невід'ємною складовою забезпечення інформаційної безпеки є кадрова політика компанії.

Наслідками інцидентів в сфері інформаційної безпеки є: витік інформації про співробітників (35%), витік чи втрата даних про клієнтів (32%), втрата внутрішніх даних (29%), крадіжка даних про клієнтів чи співробітників (23%). Середній же розмір збитку від такого інциденту оцінюється на рівні $ 531.

Про важливість інформаційної безпеки говорить той факт, що в 2000 році міжнародним інститутом стандартів ISO розроблено та запроваджено спеціальний стандарт інформаційної безпеки – стандарт ISO 17799 [1]. Цей стандарт встановлює єдині правила та підходи до побудови системи інформаційної безпеки та встановлює можливість аудиту інформаційних систем з точки зору безпеки. Окремим розділом у стандарті виділено управління доступом до ресурсів ІС. Управління доступом передбачає контроль доступу до ресурсів системи та послуг, що надаються, а також протидію несанкціонованої активності у системі. Санкціонований доступ до ресурсів системи має дозволяє забезпечити:

- авторизацію користувачів на початку робо- ти з системою; – встановлення різним користувачам системи різних прав до доступу до її ресурсів;

- встановлення кожному користувачеві переліку допустимих операцій, що можуть змінювати стан інформаційної бази;

- встановлення меж та контроль доступу до перегляду інформаційних ресурсів користувачами з різними рівнями допуску.

Зневага питаннями захисту інформації може призвести до повного банкрутства. Тому питання аналізу загроз і ризиків є визначальним при побудові ефективної системи захисту інформації. Однак, за оцінками фахівців, лише не більше 5% підприємств використовують власні методики аналізу ризиків, що дозволяють виконувати кількісний аналіз та оптимізацію підсистеми інформаційної безпеки. 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 при розв'язанні 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. Статистика у сфері інформаційної безпеки свідчить, що близько 80% зловмисників належить до інсайдерів. У компаніях телекомунікаційної галузі на їх дії припадає близько 90% фінансових утрат. Людський фактор завжди був і є одним із найважливіших ризиків будь-якого бізнесу, оскільки більшість інцидентів відбуваються саме з вини співробітників. Навмисний відплив часто важко відрізнити від ненавмисного, однак це не завжди потрібно, оскільки наслідки для підприємства при будь-якому із цих варіантів можуть бути катастрофічними. Те, що більшість керівників не знають джерел внутрішніх загроз, говорить про те, що бізнесом приділяється недостатньо уваги інформаційній безпеці, що, утім, є одним із найважливіших факторів існування підприємства. Аналіз, проведений на підприємствах середнього бізнесу, показав, що випадкові кібер-атаки виникають частіше і потенційно можуть нашкодити більше, ніж навмисні атаки інсайдерів. У результаті дослідження з'ясовано, що більшість підприємств приділяють набагато більше уваги захисту від навмисних внутрішніх атак, ніж від більш частих і потенційно більш руйнівних випадкових внутрішніх інцидентів. Поза увагою залишаються питання потенційних внутрішніх ризиків, що виходять від співробітників, які мають доступ до критично важливих систем і секретної інформації. Хоча керівники усвідомлюють існування таких ризиків, турбота про зовнішню інформаційну безпеку часто переважує інші питання.

Надійно гарантувати бізнес від перерахованих негативних явищ можна тільки на основі формування ефективної системи забезпечення інформаційної безпеки. Однак тут існують певні проблеми, що належать, швидше за все, до

організаційно- фінансових. Першою і найбільшою проблемою у створенні системи інформаційної безпеки є відсутність розуміння в керівництва необхідності створення такої системи. Багато керівників підприємств не усвідомлюють, що створювати систему інформаційної безпеки просто необхідно, бо своєчасне створення її позбавить підприємство збитків, а іноді навіть і врятує бізнес. Друга проблема при створенні системи інформаційної безпеки – відсутність достатньої кількості фінансових коштів. Відсутність фінансування з мінімального бюджету для створення системи інформаційної безпеки зустрічається також дуже часто. Приміром, у США і країнах Євросоюзу на створення системи інформаційної безпеки і підтримку її в актуальному стані виділяється від 30% прибутку компанії. В Україні ж якщо фінанси і виділяються, то разово й у недостатній кількості. Їх може вистачити хіба що на продовження ліцензії на антивірус. І лише деякі підприємства, які можна вважати скоріше винятком із правил, планують і приймають бюджет своєї системи інформаційної безпеки виходячи з реальних потреб. Третьою найнебезпечнішою проблемою є ситуація, коли є розуміння керівництва та необхідні кошти, але створення системи інформаційної безпеки доручають фахівцям, що не мають ані відповідної освіти, ані достатнього досвіду. Найчастіше це бувають системні адміністратори або відділ технічної підтримки. Вони, у свою чергу, розцінюють це як установку і налаштування антивірусу. Наявність внутрішнього зловмисника, найчастіше, узагалі не береться до уваги. Відповідно до статистики 70% порушень здійснюється внутрішніми зловмисниками. Ще частіше без належної уваги залишаються канали зв’язку, і переписка керівництва підприємства з діловими партнерами, із клієнтами стає незахищеною. 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 лягає на керівництво 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.

Список використаних джерел

1. Стандарт ISO 17799 [Электрон. ресурс]. – Режим доступа к ресурсу: http:// www.17799.com.

2. Закон від 16.07.1999 р. № 996-XIV "Про бухгалтерський облік та фінансову звітність в Україні"