Толмазов Є. О., Решетняк Ю. О.

Дніпровський національний університет імені Олеся Гончара (Україна)

ПРОБЛЕМАТИКА ЕКОНОМІЧНИХ АСПЕКТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Однією з проблем економічних аспектів безпеки підприємства можуть стати витрати на захист інформації та обладнання: підприємства можуть затрачувати великі кошти на захист інформації та обладнання від крахів, викрадення, вибухів і інших загроз.

Захист інформації і обладнання є необхідним для забезпечення надійності функціонування підприємства, а також для захисту конфіденційної інформації, яка може бути використана для зловживання підприємством і його клієнтами. Наприклад, викрадення конфіденційної інформації може призвести до зниження конкурентоспроможності підприємства і збитків фінансового характеру. Щоб захистити інформацію та обладнання приймаються різні заходи, такі як встановлення захисного ПЗ, шифрування інформації, встановлення систем контролю доступу, створення резервних копій інформації та проведення регулярних аудитів безпеки. Також важливо проводити навчання співробітників щодо безпеки інформації та обладнання, щоб вони могли спостерігати за можливими загрозами і реагувати на них у відповідному часі.

Однак, незалежно від заходів, які приймаються, витрати на захист інформації та обладнання залишаються великим навантаженням для підприємства. Це може впливати на конкурентоспроможність та прибуток підприємства, а також заважати розвитку його бізнесу. Тому є важливість розроблення рішень щодо ефективного керування витратами на захист інформації та обладнання. Це може включати в себе оптимізацію витрат на захист, так як вибір найбільш ефективних методів та технологій, а також розробку стратегії управління ризиками.

Також, є можливість співпраці з іншими підприємствами чи індустріями, щоб ділитися знанням та ресурсами щодо захисту інформації та обладнання. Це може допомогти скоротити витрати та збільшити ефективність захисту.

Важливо знаходити баланс між захистом інформації та обладнання і витратами, щоб максимально зберегти ресурси підприємства і забезпечити максимальну захищеність. Регулярне моніторинг та аудит систем захисту інформації

та обладнання, а також постійне підвищення рівня компетентності співробітників в цій області, є ключовими факторами для ефективного керування цією проблемою.

Розвиток інформаційних технологій і зростання кількості загроз для інформації та обладнання підприємств, зміцнюють потребу в ефективному захисті інформації та обладнання. Необхідно вдосконалювати системи захисту інформації та обладнання і поліпшувати процеси керування витратами на їх захист, щоб забезпечити максимальну безпеку для підприємства та його активів.

Проте, не всі витрати на захист інформації та обладнання можуть бути зрозумілі і опрацьовані. Наприклад, розбіжності в оцінці витрат між різними відділами можуть виникати із-за розбіжностей у визначенні необхідності захисту інформації та обладнання. Тому, важливо створювати зрозумілу стратегію захисту інформації та обладнання, яка буде підтримуватися всіма відділами і співробітниками підприємства.

Щоб зменшити ці витрати і забезпечити максимальну захищеність, потрібно розробляти і вдосконалювати системи захисту інформації та обладнання, спостерігати за ризиками і розробляти плани реагування на них.

Крім того, потрібно приділяти увагу вибору партнерів та постачальників, які мають високі стандарти захисту інформації та обладнання. Це допоможе знизити ризики викрадення інформації та захисту від несанкціонованого доступу.

Загалом, захист інформації та обладнання є необхідним засобом для забезпечення безпеки підприємства та його активів. Тому, є важливим створювати ефективну стратегію захисту інформації та обладнання, яка буде оптимізувати витрати, не завдаючи значного впливу на економіку підприємства.

Не менш важливо є розробка і впровадження політики захисту інформації та обладнання, яка буде враховувати всі можливі ризики, які можуть виникнути. Це може включати в себе заходи щодо конфіденційності і безпеки даних, а також регламентування доступу до інформації та обладнання.

Також можна впровадити в метод 80/20, що є Принципом Парето. Як його можливо застосувати? Цей метод передбачає, що за допомогою зосередження уваги на головних 20% аспектів, які потрібно захистити, можна досягнути 80% ефективності. Тобто, підприємство повинно сфокусуватися на тих 20% мережних систем, даних, обладнання та іншому, що є найбільш важливими для бізнесу та захисту. Після того, як будуть визначені пріоритетні аспекти, варто зосередити

свої витрати на них, щоб забезпечити максимальну безпеку для інформації та обладнання підприємства.

Список використаних джерел:

1. Яковенко В.С., Зайцева Н.В. Консолідація даних у бізнес-аналізі діяльності підприємств. Глобальні та національні проблеми економіки. 2015. № 8. С. 1222-1227
2. Королькова В.В., Яковенко В.С. Статистичний аналіз стану злочинності в Україні. *Економіка та Фінанси*. 2016. №. 10. С. 4-11.
3. Яковенко В.С., Правікова В.Ю. Принципи створення та обігу криптовалют, інструментарій їх дослідження. *Економіка. Фінанси. Право*. 2018. № 12(2). С. 4-8. URL: http://nbuv.gov.ua/UJRN/ecfipr_2018_12(2)__3.