Максимова Ю. О.
старший викладач
Нікуліна О. Ю
здобувачка
Одеський національний університет імені І. І. Мечникова (Україна)

ОСОБЛИВОСТІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА СУЧАСНИХ ПІДПРИЄМСТВАХ

Сучасні підприємства стикаються з великою кількістю інновацій які впливають на їх діяльність. Глобалізація та розвиток інформаційних технологій, управління ризиками та інформаційна безпека стають дуже важливими для кожного бізнесу.

Цифрові технології все більше інтегруються в повсякденне життя та бізнес-процеси, забезпечення інформаційної безпеки стає найважливішим аспектом діяльності кожного підприємства. На сьогодняшній день захист конфіденційної інформації став життєво важливою проблемою для підприємств у різних галузях.

Одним із найефективніших способів захисту цифрових активів підприємства є впровадження системи управління інформаційною безпекою. Система управління інформаційною безпекою це системний підхід до управління та захисту інформаційних активів підприємства. Вона включає набір рішень, процедур і засобів контролю, які допомагають визначити, оцінити та зменшити потенційні ризики для даних підприємства, включаючи їх зберігання, обробку та передачу.

Основною метою системи управління інформаційною безпекою є забезпечення управління ризиком витоку конфіденційної інформації за межі підприємства.

Однією з найбільш широко визнаних і прийнятих систем управління інформаційною безпекою є ISO/IEC 27001, яка містить вказівки та вимоги щодо створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою [1].

Забезпечення інформаційної безпеки потребує комплексної трансформації, що включає не лише технологічні засоби, а й організаційні заходи протидії. Тільки шляхом спільного використання технічних та організаційних заходів можна створити надійну систему захисту інформації, здатну ефективно протидіяти загрозам інформаційної безпеки, таким як кібератаки, віруси і витік даних.

Ефективне управління інформаційною безпекою допомагає підприємствам запобігти збитків від витоку даних, забезпечує довіру клієнтів та партнерів, а також сприяє стійкості і довгостроковому розвитку бізнесу.

Управління ризиками та інформаційна безпека відіграють важливу роль у сучасних економічних теоріях і практиках, оскільки вони представляють фундаментальні аспекти, необхідні для забезпечення стійкості та переваг для розвитку організацій в умовах сучасного цифрового середовища.

Впровадження системи управління інформаційною безпекою надає підприємствам багато переваг, серед яких:

- управління ризиками, дає можливість виявляти й усувати потенційні загрози та вразливі місця структурованим і проактивним способом, зменшуючи ймовірність порушень безпеки;
- відповідність, дотримуючись стандартів, таких як ISO/IEC 27001, підприємства можуть продемонструвати свою відданість інформаційній безпеці та дотримуватись нормативних вимог, які можуть бути критичними для галузей із суворими правилами захисту даних, такими як Загальний регламент захисту даних (GDPR), Network and Information Security 2 (NIS2) або Digital Operational Resilience Act (DORA);
- довіра клієнтів, система управління інформаційною безпекою допомагає підприємствам забезпечити конфіденційність, цілісність і доступність конфіденційних даних клієнтів. Це зміцнює довіру та може призвести до підвищення лояльності та задоволеності клієнтів;
- економія коштів, система управління інформаційною безпекою може допомогти підприємствам уникнути фінансових втрат і пов'язаних з ними витрат на відновлення [2].

Таким чином, управління ризиками та інформаційна безпека повинні бути включені до стратегічного планування та операційних процесів організації разом з іншими важливими аспектами управління.

З кожним роком збільшується кількість кібератак, які спрямовані на втручання в IT-інфраструктуру підприємства з метою завдати їй шкоди або отримати секретні дані. Для злочинців підприємства є найбільш вигідними цілями ніж приватні особи, так як вони можуть задати шкоди їх репутації, отримати конфіденційну інформацію про діяльність або технологію виробництва. Тому IT-безпека підприємства повинна включати в себе захист комп'ютерних систем, мереж і даних від різноманітних загроз, що виникають у цифровому середовищі. Це включає захист від несанкціонованого доступу, маніпулювання або крадіжки конфіденційної інформації, а також від збитків, які можуть бути спричинені кібератаками.

Тільки підприємства, які серйозно ставляться до управління ризиками та інформаційної безпеки, можуть адаптуватися до швидко мінливого цифрового середовища та забезпечити свою довгострокову конкурентоспроможність.

Список використаних джерел

1. ISO/IEC 27001:2022. *ISO*. 2022. URL: https://www.iso.org/standard/27001

2. Brandenburg G. The Role and Implementation of an Information Security Management System in Modern Enterprises. *CTRL Disrupt | Creating Resilient Enterprises*. URL: https://ctrl-disrupt.nl/en/-insights-news/the-role-and-implementation-of-an-information-security-management-system-in-modern-enterprises