УДК 004.056.5:005.334

Нарепеха Д.Ю., здобувач,
Полотай О.І., к.т.н., доцент,
Балацька В.С., д-р філ., ст. викладач
Львівський державний університет безпеки життєдіяльності

АНАЛІЗ ВИКОРИСТАННЯ МІТИГАЦІЇ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ НА ПІДПРИЄМСТВІ

Проблематика інформаційної безпеки значною мірою визначається характером ризиків та масштабом їх можливих наслідків. У невеликих локальних системах створення ефективної системи управління ризиками є відносно простішим завданням, ніж у розподілених системах, що зумовлено їх специфічними особливостями [2].

У сучасних умовах цифровізації економіки питання забезпечення інформаційної безпеки стає одним із ключових аспектів ефективного функціонування підприємства. Ризики інформаційної безпеки охоплюють широкий спектр загроз – від несанкціонованого доступу до корпоративних даних до збоїв у роботі інформаційних систем, витоків конфіденційної інформації чи кібератак. Такі ризики можуть призвести до значних фінансових втрат, зниження репутації, втрати клієнтів і порушення стабільності бізнес-процесів. Саме тому мітигація ризиків інформаційної безпеки є критично важливою складовою системи управління ризиками підприємства.

Мітігація (або митігування) ризиків - це термін, що походить від англійського слова mitigation, що означає "пом'якшення" або "пом'якшення наслідків". Прямий переклад з англійської вже частково описує суть мітигації ризиків – це зниження наслідків їх реалізації. Спочатку термін «мітігація» застосовувався щодо різноманітних катастроф і надзвичайних ситуацій (у розумінні способів зниження тяжкості їх наслідків), але останнім часом він нерідко використовується і в теорії управління ризиками. Особливо часто останнім часом цей термін застосовується в таких галузях як інформаційна та кібербезпека. Мітигація – це процес здійснення заходів, спрямованих на зменшення ймовірності настання ризикової події та/або зменшення тяжкості наслідків, якщо вона все ж станеться. Це proactive-стратегія, яка передбачає активні дії для попередження негативних наслідків, а не просто реагування на них після того, як вони сталися [2].

Процес мітигації ризиків інформаційної безпеки передбачає кілька основних етапів: ідентифікацію, оцінювання, розроблення заходів

реагування, реалізацію та постійний моніторинг. На етапі ідентифікації визначаються потенційні загрози, такі як фішингові атаки, шкідливе програмне забезпечення, помилки персоналу чи вразливості програмного забезпечення. Оцінювання ризиків дозволяє визначити ймовірність їх виникнення та рівень впливу на бізнес-процеси, що є основою для формування пріоритетів у захисті інформаційних активів.

Одним із практичних прикладів мітигації ризиків інформаційної безпеки у локальних комп'ютерних мережах підприємства є впровадження системи контролю доступу та сегментації мережі для зниження ризику несанкціонованого доступу до конфіденційних даних.

Наприклад, на підприємстві існує спільна локальна мережа, до якої підключені всі комп'ютери працівників різних відділів – бухгалтерії, відділу кадрів, технічного відділу тощо. У разі відсутності розмежування прав доступу, співробітники можуть потенційно отримати доступ до інформації, яка не стосується їхніх обов'язків, або ж зовнішній зловмисник, потрапивши до внутрішньої мережі, отримає змогу вільно пересуватися між сегментами системи.

Щоб мінімізувати цей ризик, підприємство впроваджує політику мітигації ризику шляхом сегментації мережі – кожен відділ отримує власний підмережевий сегмент із чітко визначеними правилами взаємодії між ними. Доступ до критично важливих ресурсів, наприклад до бази даних бухгалтерії, надається лише авторизованим користувачам із багатофакторною аутентифікацією. Додатково застосовується система моніторингу та журналювання подій, яка дозволяє відстежувати спроби несанкціонованого доступу.

Завдяки таким заходам ризик компрометації даних зменшується: навіть якщо зловмисник отримає доступ до однієї з ділянок мережі, він не зможе легко проникнути до інших частин системи або отримати доступ до конфіденційної інформації. Такий підхід демонструє ефективну мітигацію ризику шляхом технічного, організаційного та процедурного посилення системи інформаційної безпеки.

Список використаних джерел:

1. Мітигація ризиків. URL: https:// https://qamania.org/blog/risk-mitigation//

2. Тичина Ю., Ящук В., Полотай О. Модель системи управління інцидентами інформаційної безпеки. Зб. тез доп. V Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів "Інформаційна безпека та інформаційні технології". (м. Львів, 30 листопада 2022 р.). Львів : ЛДУБЖД, 2022. С. 108–111.