УДК 004.8:004.9

Щерб'як М.Т., здобувач,
Ящук В.І., к.екон.н., доцент,
Шклярський Р.А., викладач
Львівський державний університет безпеки життєдіяльності

РОЗРОБЛЕННЯ КОНЦЕПТУАЛЬНОЇ МОДЕЛІ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ТОВ «ІНФО ПРОСТІР ПЛЮС» ВІД НЕСАНКЦІОНУВАНОГО ДОСТУПУ НА ОСНОВІ БАГАТОРІВНЕВОЇ АРХІТЕКТУРИ БЕЗПЕКИ

У сучасному цифровому середовищі корпоративні мережі перебувають під постійним впливом широкого спектра кіберзагроз, зокрема несанкціонованих спроб доступу, атак на автентифікаційні механізми, експлуатації мережевих вразливостей і маніпуляцій із конфігураційними параметрами систем. Стійкість інформаційної інфраструктури організації залежить від здатності вчасно протидіяти зовнішнім і внутрішнім ризикам, забезпечуючи захист на кожному рівні взаємодії користувачів і сервісів.

Для ТОВ «ІНФО ПРОСТІР ПЛЮС» важливою є побудова моделі, яка поєднує структуровані механізми контролю доступу, сегментацію мережевих ресурсів, інструменти моніторингу та автоматизоване реагування на інциденти. Багаторівнева архітектура безпеки дає змогу реалізувати комплексний підхід до захисту, у якому кожен рівень функціонує як автономна лінія оборони та взаємодіє з іншими для формування єдиної системи. Таке поєднання технічних засобів, політик конфіденційності й організаційних заходів створює умови для мінімізації ризиків несанкціонованого доступу та забезпечує стабільне функціонування ІТ-інфраструктури підприємства.

Несанкціонований доступ виникає внаслідок комп'ютерних атак, компрометації облікових даних, помилок користувачів або неправильно налаштованих компонентів мережі. Уразливість може з'являтися як на рівні фізичної інфраструктури, так і в логічній конфігурації систем, що зумовлює необхідність комплексного контролю.

Побудова концептуальної моделі системи захисту передбачає використання принципів «глибинної оборони». Першим рівнем виступає автентифікація користувачів, включно з багатофакторною перевіркою, біометричними ідентифікаторами, політиками складності паролів та обмеженням доступу на основі ролей. Другий рівень включає сегментацію корпоративної мережі. Розділення інфраструктури на логічні зони за допомогою VLAN, фільтрації трафіку на межах сегментів та виділення окремих контурів для критично важливих

ресурсів підвищує контрольованість інфраструктури та знижує ризик поширення атак. Третій рівень моделі ґрунтується на технологіях виявлення аномалій та вторгнень. IDS/IPS-системи аналізують мережевий трафік, визначають характерні відхилення та блокують підозрілу активність. SIEM-рішення забезпечують централізований збір логів, кореляцію подій, аналіз дій користувачів і пристроїв, формуючи цілісну картину стану безпеки. Четвертий рівень – системи управління конфігураціями, аудит інфраструктури та контроль цілісності. Регулярна перевірка прав доступу, журналів змін і конфігураційних файлів зменшує ризики, пов'язані з помилками адміністрування та непоміченими модифікаціями.

Важливу роль відіграє також організаційний компонент: розроблення регламентів, політик безпеки, проведення навчання для співробітників та підтримання культури відповідальної роботи з даними. У поєднанні з концепцією Zero Trust, яка передбачає постійну перевірку користувачів, пристроїв, місця розташування та контексту запиту, така архітектура створює високий рівень захищеності корпоративної мережі ТОВ «ІНФО ПРОСТІР ПЛЮС».

Багаторівнева архітектура безпеки забезпечує системну протидію несанкціонованому доступу та дозволяє охопити всі ключові складові корпоративної інфраструктури – від автентифікації до моніторингу й аналізу поведінкових патернів. Ефективність захисту визначається узгодженою роботою механізмів контролю доступу, сегментації мережі, моніторингу трафіку та кореляції подій, а також відповідністю політик безпеки сучасним стандартам кіберзахисту. Комплексна модель створює передумови для підвищення кіберстійкості підприємства, знижує ймовірність успішної компрометації критичних ресурсів і гарантує надійне функціонування інформаційних процесів. Реалізація інтегрованого підходу особливо важлива для ТОВ «ІНФО ПРОСТІР ПЛЮС», оскільки забезпечує захист бізнес-процесів, мінімізує ризики внутрішніх і зовнішніх загроз та відповідає сучасним вимогам корпоративної безпеки.

Список використаних джерел:

1. Ящук В. І. Методика забезпечення безпеки інформаційних систем та реагування на кіберінциденти кібербезпековими центрами // Scientific Collection «InterConf+». 2024. Vol. 45(201) : Proceedings of the 8th International Scientific and Practical Conference «International Scientific Discussion: Problems, Tasks and Prospects», May 19–20, 2024, Brighton, United Kingdom / comp. LLC SPC «InterConf». Brighton : A.C.M. Webb Publishing Co Ltd., 2024. P. 632–641. DOI: https://doi.org/10.51582/interconf.19-20.05.2024