

УДК 004.056

Голда Антон, Стадник Марія, к.т.н., доц.

Тернопільський національний технічний університет імені Івана Пулюя

МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ ІНТЕРНЕТ-БАНКІНГУ

Golda Anton, Stadnyk Mariia, Ph.D., Assoc. Prof.

METHODS AND MEANS OF ENSURING INFORMATION SECURITY IN INTERNET BANKING SYSTEMS

Інтернет-банкінг в сучасному світі є не тільки зручним інструментом для фінансових операцій, але і об'єктом зростаючого інтересу для кіберзлочинців. Тому забезпечення інформаційної безпеки у цьому сегменті є надзвичайно важливим завданням для банків та їхніх клієнтів.

Одним з ключових методів є використання криптографічних технологій. Шифрування даних під час їх передачі забезпечує конфіденційність і унеможливає несанкціонований доступ. Технології SSL/TLS використовуються для захисту від перехоплення чутливої інформації, такої як паролі та особисті дані, під час онлайн-сесій.

Двофакторна аутентифікація є ще однією ефективною мірою безпеки. Окрім звичайного пароля, користувач також підтверджує свою особу, отримуючи, наприклад, одноразовий код на мобільний телефон, також можливе забезпечення додаткової безпеки за допомогою ідентифікації за відбитком пальця, обличчям та інших фізіологічних показників.

Банки активно використовують системи виявлення аномальної активності. Ці системи аналізують звичайну поведінку користувачів та швидко реагують на будь-які незвичайні транзакції чи входи.

Оновлення програмного забезпечення та регулярні патчі важливі для закриття вразливостей. Це означає, що банки повинні постійно вдосконалювати свої системи, щоб утримувати кіберзлочинців на відстані.

Не потрібно забувати і про освіту клієнтів. Банки здійснюють інформаційні кампанії, навчаючи користувачів розпізнавати шахрайство та вживати заходи безпеки в онлайн-середовищі.

Загалом, поєднання технологічних і організаційних заходів дозволяє забезпечити ефективний рівень інформаційної безпеки в інтернет-банкінгу, створюючи надійне середовище для фінансових операцій.

Безпека в інтернет-банкінгу також вимагає постійного моніторингу та реагування на нові загрози. Активна співпраця зі спеціалізованими службами та обмін інформацією про кіберзагрози стає необхідністю. Важливим є розробка стратегій відновлення після інцидентів та регулярне проведення тестів на проникнення для виявлення слабких місць у системах. Ці заходи, поєднані з постійним вдосконаленням технічних і організаційних аспектів, створюють стійкість і надійність в інтернет-банкінгових системах.

Постійне оновлення алгоритмів машинного навчання дозволяє вдосконалювати системи виявлення та запобігання. Застосування технологій блокчейн також може відігравати ключову роль у забезпеченні безпеки та незмінності транзакцій, зменшуючи ризик фінансових маніпуляцій та шахрайства. Такий комплексний підхід забезпечує сталу безпеку в інтернет-банкінгу та зміцнює віру клієнтів у сучасні фінансові технології.

Література:

1. Брижко В. М. Електронний банкінг у контексті захисту персональних даних / В. М. Брижко, Ю. К. Базанов, М. Я. Швець. – К. : НДЦПІ АПРН України, 2008. – 140 с.

2. Кулініч О. А. Інтернет-банкінг в Україні як складова розвитку мережної інфраструктури / О. А. Кулініч // Економічна стратегія і перспективи розвитку сфери торгівлі та послуг : зб. наук. пр. – Х. : ХДУХТ, 2011. – Вип. 2 (14). – С. 421–429.