УДК 327.56:004.056.5

Кривий Р.А., здобувач,
Ткачук Р.Л., д.т.н., професор,
Балацька В.С., д-р. філ., ст. викладач
Львівський державний університет безпеки життєдіяльності

КІБЕРБЕЗПЕКА БАНКІВСЬКОГО СЕКТОРУ: СУЧАСНІ ЗАГРОЗИ ТА РОЛЬ ШІ У ПРОТИДІЇ

Зростання кіберзагроз у фінансовому секторі підвищує потребу в постійному оновленні систем захисту банківської інформації. Українські банки загалом захищені від існуючих загроз, проте сучасні виклики, зокрема пов'язані із застосуванням ШІ, потребують впровадження передових технічних рішень та розвитку культури інформаційної безпеки. Сфера ІБ в Україні базується на національних законах («Про інформацію», «Про захист персональних даних», «Про електронні комунікації») та міжнародних стандартах GDPR і ISO/IEC 27001. Технічний захист реалізується через нормативні вимоги, організаційну інфраструктуру та матеріально-технічні засоби, ключову роль серед яких відіграють системи DLP. Основні технічні канали витоку – акустичні, радіотехнічні, оптичні, електричні та матеріально-речові – нейтралізуються комплексом інженерно-технічних заходів.

Банківська система є критичною складовою економіки, а її стійкість визначає рівень фінансової безпеки держави. Цифровізація фінансових послуг супроводжується збільшенням обсягів даних, що містять персональну інформацію клієнтів, комерційні відомості та банківську таємницю, підвищуючи вразливість до кібератак (фішинг, DDoS, атаки на платіжні системи), внутрішніх загроз та інформаційно-психологічного впливу на співробітників і клієнтів.

Опираючись на проведений аналіз, основні сучасні виклики можна узагальнити у вигляді наступних загроз:

– кіберзлочинність – фішинг, шкідливе програмне забезпечення, несанкціонований доступ до баз даних та крадіжку фінансових ресурсів;

– штучні загрози, створені із застосуванням ШІ, які дозволяють автоматизувати атаки, обходити традиційні системи безпеки та прогнозувати поведінку користувачів;

– внутрішні ризики, пов'язані з людським фактором та порушенням процедур доступу;

– інформаційні обмеження, які впливають на своєчасність виявлення загроз та реагування на них.

Ці чинники ускладнюють забезпечення конфіденційності, цілісності та доступності даних банківської системи, що робить її вразливою до матеріальних, репутаційних і стратегічних втрат.

Ефективні заходи захисту на наш погляд мають включати:

Технічні засоби: впровадження систем виявлення вторгнень (IDS/IPS), багатофакторної автентифікації (MFA), розширеного шифрування даних, а також систем захисту електронної пошти та контролю мобільних пристроїв.

Інноваційні підходи: використання ШІ та методів машинного навчання для прогнозування загроз, аналізу великих обсягів даних та автоматичного реагування на аномалії.

Організаційні заходи: навчання персоналу, розмежування доступу за принципом найменших привілеїв та регулярні кібервійськові тренування.

Криптографічний захист: застосування квантового шифрування для підвищення стійкості систем до сучасних атак.

Технологія блокчейн: впровадження децентралізованих реєстрів для забезпечення прозорості, незмінності та додаткового рівня захисту даних, що знижує ризики шахрайства та несанкціонованого втручання.

Комплексне поєднання технічних, організаційних і криптографічних заходів, а також активне використання ШІ дозволяє забезпечити високий рівень стійкості банківських інформаційних систем, знижує ризики матеріальних та репутаційних втрат і підвищує готовність до реагування на новітні кіберзагрози.

Список використаних джерел:

1. Про затвердження Положення про використання засобів криптографічного захисту інформації Національного банку України : Постанова від 14.04.2023р. № 49. URL: https://zakon.rada.gov.ua/laws/show/v0049500-2

2. Ткачук Р. Л., Полотай О. І., Балацька В. С., Брич Т. Б., Кухарська Н. П. Моделювання захисту операційних систем від реалізації кібератак з використанням критерію Пірсона. Вісник Львівського державного університету безпеки життєдіяльності : зб. наук. пр. Львів : ЛДУ БЖД, 2025. № 31. С. 117–125. DOI: https://doi.org/10.32447/20784643.31.2025.12

3. Балацька В.С., Ткачук Р.Л., Маслова Н.О. Еволюція КСЗІ та інтеграція блокчейн-технологій у кіберзахисті державних інформаційних системи України. Кібербезпека: освіта, наука, техніка. Спеціальний випуск : електронне фахове наукове видання Київ, 2025. № 2 (30). С. 316–332. DOI: https://doi.org/10.28925/2663-4023.2025.30.975