НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ

ЗБІРНИК МАТЕРІАЛІВ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «ШТУЧНИЙ ІНТЕЛЕКТ І БЕЗПЕКА»

19-21 листопада 2024 р.

Київ–2024

УДК 004(8+056+413.4)
ББК 32.813
Ш-94

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 12 від 28 листопада 2024 р.)

Ш-94 **Штучний інтелект і безпека,** науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Інституту проблем реєстрації інформації Національної академії наук України : матеріали, 19-21 листопада 2024 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, ІПРІ НАН України, 2024. 115 с.

SH-94 **Artificial intelligence and security**, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine, Institute for Information Recording of the National Academy of Sciences of Ukraine : materials, November 19-21, 2024. Kyiv: PIMEE NAS of Ukraine, IPRI NAS of Ukraine, 2024. 115 p.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
(м. Київ)
Інститут проблем реєстрації інформації
(м. Київ)

ПРОГРАМНИЙ КОМІТЕТ

Мохор Володимир Володимирович
член-кореспондент НАН України, доктор технічних наук, професор,
директор Інституту, голова програмного комітету

Чемерис Олександр Анатолійович
доктор технічних наук, старший науковий співробітник
заступник директора з наукової роботи

Чьочь Вікторія Володимирівна
кандидат технічних наук,
заступник директора з науково-технічної роботи

Артемчук Володимир Олександрвич
доктор технічних наук, старший науковий співробітник
заступник директора з науково-організаційної роботи

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Артемчук Володимир Олександрвич
доктор технічних наук, старший науковий співробітник
заступник директора з науково-організаційної роботи

Клименко Тетяна Михайлівна
Завідувачка науково-організаційного відділу

Цуркан Оксана Володимирівна
молодший науковий співробітник

Я.Ю. Дорогий, В.В. Цуркан, І.О. Бердиченко, О.О. Дорога-Іванюк

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ БАНКІВСЬКОЇ СФЕРИ

Анотація. Захист критичної інфраструктури банківської сфери є важливою умовою стабільності та безпеки фінансової системи України. Військові дії, підвищення кіберзагроз і складні економічні умови вимагають інноваційних підходів до захисту. Штучний інтелект (ШІ) є одним із найбільш перспективних інструментів, що дозволяє не лише швидко реагувати на загрози, але й передбачати нові вразливості. Впровадження ШІ допомагає установам банківської сфери краще справлятися з кіберзагрозами, знижуючи ризики та підвищуючи надійність інфраструктури.

Вступ. Критична інфраструктура (КІ) банківської сфери є основою економічної безпеки України, від стабільності якої залежить функціонування фінансових операцій, збереження заощаджень громадян і довіра до банківської системи. Останні роки, особливо в умовах війни, відзначаються різким збільшенням кібератак, спрямованих на банківську інфраструктуру України. Атаки мають на меті як безпосереднє завдання шкоди, так і дестабілізацію економічної системи. З огляду на це, критично важливим є впровадження інноваційних рішень, зокрема штучного інтелекту, для моніторингу, виявлення загроз і швидкого реагування на потенційні ризики.

Захист критичної інфраструктури банківської сфери. Захист КІ банківської сфери вимагає комплексного підходу. Ключові компоненти цієї інфраструктури включають платіжні системи, канали передачі фінансових даних, бази даних клієнтів, та системи онлайн-банкінгу. Відмова цих систем може призвести до фінансових втрат і зниження довіри клієнтів до банківської сфери. В умовах війни значно посилилися загрози з боку кіберзлочинців, які використовують більш витончені методи атаки, що ускладнює їх виявлення та нейтралізацію.

Особливу роль у захисті банківської інфраструктури відіграє Національний банк України (НБУ), який, відповідно до законодавства, здійснює регулювання та нагляд за станом критичної інфраструктури банківської сфери [1]. НБУ розробляє нормативно-правові акти, контролює виконання вимог кібербезпеки банками та координує заходи з захисту їх КІ у разі кризових ситуацій [2, 3].

НБУ забезпечує функціонування системи кіберзахисту в банківській системі України, серед іншого організовано обмін інформацією про кіберзагрози, кібератаки та кіберінциденти з банками України; визначено особливості кіберзахисту об'єктів критичної інформаційної інфраструктури банківської системи України; відбувається сприяння розвитку та вдосконаленню систем, комплексів та засобів забезпечення кіберзахисту в банківській системі України.

В НБУ, з метою поєднання та координації зусиль суб'єктів кіберзахисту створено та функціонує Центру кіберзахисту [4]. Основними технічними інструментами Центру кіберзахисту є MISP-NBU і портал Центру кіберзахисту. Центр кіберзахисту забезпечує реалізацію інформаційного обміну, функціонування CSIRT-NBU, і відповідно, координацію дій з питань кіберзахисту в банківській системі.

Окрім зазначених вище заходів та нормативно-правового регулювання, важливим елементом є використання інноваційних технологій. ШІ надає можливість аналізувати великі обсяги даних у режимі реального часу, виявляти аномалії та передбачати можливі загрози ще до їх реалізації. Для прикладу, алгоритми машинного навчання можуть виявляти невластиву поведінку користувачів у системах банківського обслуговування, яка може сигналізувати про потенційну атаку. Використання таких технологій дозволяє установам банківської сфери швидше реагувати на загрози, зменшуючи можливість витоку конфіденційної інформації та втрати фінансів.

Інтеграція ШІ стає невід’ємною частиною міжнародної співпраці у кібербезпеці та сфері захисту критичної інфраструктури, зокрема для захисту критичної банківської інфраструктури. Банківські установи України отримують підтримку від міжнародних партнерів, які надають сучасні технологічні рішення на основі ШІ, а також консультації і методології, що допомагають протидіяти новітнім кібератакам та захищати КІ. Співпраця з такими установами, як Європейське агентство з кібербезпеки (ENISA), сприяє інтеграції штучного інтелекту в українські системи захисту, дозволяючи відповідати найвищим стандартам, наприклад, ISO/IEC 27001 [5]. ШІ дозволяє покращити не лише автоматизований моніторинг загроз, а й підвищувати ефективність обміну інформацією з міжнародними партнерами для швидшої реакції на нові загрози.

Штучний інтелект також стає важливим інструментом для навчання та обізнаності співробітників банків щодо кіберзагроз та захисту КІ. НБУ, як секторальний орган захисту критичної інфраструктури банківської сфери [3], рекомендує банкам проводити регулярні тренінги, які включають моделювання кіберзагроз із використанням ШІ. Це дає змогу співробітникам краще зрозуміти потенційні інсайдерські загрози та способи їх виявлення. ШІ може автоматизувати моніторинг дій користувачів у банківських системах, допомагаючи виявляти підозрілу активність у режимі реального часу, що є особливо актуальним в умовах зростання кількості інцидентів у період військових конфліктів. Також слід відзначити, що НБУ в умовах війни веде активну роботу щодо підвищення координації між різними департаментами всередині самого регулятора та в банківській сфері в цілому. Це допомагає уникати дублювання заходів захисту та забезпечувати єдність підходів до захисту критичної інфраструктури. В цьому напрямку, важливою ініціативою є створення централізованих команд з управління кібербезпекою та захисту критичної інфраструктури, що складаються з фахівців різних профілів.

Такі команди можуть проводити оцінку ризиків і здійснювати аналіз наявних проблем КІ для своєчасної розробки стратегій реагування.

Висновки. Використання штучного інтелекту для захисту критичної інфраструктури банківської сфери в умовах війни та підвищеної кіберзагрози є важливим кроком до забезпечення фінансової стабільності країни. Інтеграція ШІ у систему кібербезпеки дозволяє банкам автоматизувати процеси виявлення загроз, оптимізувати управління ризиками та швидко реагувати на інциденти. Це не лише підвищує надійність інфраструктури, а й сприяє збереженню довіри клієнтів до банківської системи.

Однак, навіть найсучасніші технології не можуть повністю захистити від порушення критичної інфраструктури без комплексного підходу. Необхідне поєднання нормативного регулювання, впровадження передових технологій, освітніх програм і міжнародного співробітництва. Військові виклики зумовлюють необхідність розширення інноваційних заходів безпеки та створення стратегій, що дозволять банківській інфраструктурі України оперативно адаптуватися до нових кіберзагроз та викликів захисту критичної інфраструктури. Такий підхід передбачає постійний моніторинг ефективності впроваджених заходів, оновлення захисних технологій і покращення професійної підготовки кадрів.

1. Про Національний банк України: Закон України від 20 травня 1999 року № 679-XIV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/679-14 (дата звернення: 02 листопада 2024).

2. Про основні засади забезпечення кібербезпеки України: Закон України, 5 жовтня 2017 року, № 2163-VIII / Верховна Рада України (онлайн) URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 02 листопада 2024).

3. Про критичну інфраструктуру: Закон України, 16 листопада 2021 року, № 1882-IX / Верховна Рада України (онлайн) URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 02 листопада 2024).

4. Національний банк України. Кіберкоманда реагування на інциденти (CSIRT). URL: https://csirt.bank.gov.ua/ (дата звернення: 08.11.2024).

5. ISO/IEC 27001:2013 Information security management systems — Requirements / International Organization for Standardization. URL: https://www.iso.org/standard/27001 (дата звернення: 02 листопада 2024).