**Міністерство освіти і науки України**
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

# *ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ*

Матеріали
II наукової онлайн-конференції

## (Суми, 02 липня 2024)

Суми
Сумський державний університет
2024

004.056.5:336(082)
В43

**Головний редактор**
доц., к.е.н., ***Койбічук Віталія***, завідувачка кафедри економічної кібернетики, Сумський державний університет
.

*Затверджено Вченою Радою Сумського державного університету (протокол № 1, 29.08.2024)*

S62 Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 02 липня 2024. Збірник матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2024. – 72 с.

Матеріали наукової онлайн-конференції "Виклики кібербезпеки індустрії фінансових послуг" присвячені пошуку системного вирішення проблем у сфері протидії кібеззагрозам у сфері фінансових послуг, підвищенню рівня кіберзахисту об'єктів критичної інфраструктури.

Видання розраховане на науковців, викладачів, студентів вищих навчальних закладів, аспірантів, докторантів та інших зацікавлених осіб.

004.056.5:336(082)

# ЗМІСТ

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

## СЕКЦІЯ 2 КІБЕРЗАГРОЗИ У СФЕРІ ФІНАНСОВИХ ПОСЛУГ

# ІДЕНТИФІКАЦІЯ ТА УПЕРЕДЖЕННЯ КІБЕРШАХРАЙСТВ В ЕЛЕКТРОННОМУ БАНКІНГУ: ДОСВІД ЄС

# IDENTIFICATION AND PREVENTION OF CYBER FRAUD IN ELECTRONIC BANKING: EU EXPERIENCE

***Віталія Койбічук**, к.е.н., доцентка,*
*Сумський державний університет, Україна*

Сучасний світ став гіперз'єднаним, й кіберзлочинці становлять значну загрозу внутрішній безпеці кожній країні, особливо країнам, які мають високий рівень розвитку економіки та цифрової грамотності. За даними Міжнародного союзу електрозв'язку (ITU), станом на 2023 рік у 175 країнах світу існують національні центри кібербезпеки (НЦКБ), задачею яких є підвищення обізнаності про кібербезпеку, реагування на кіберінциденти моніторинг кіберзагроз, співпраця з іншими країнами.

В глобальному просторі Міжнародні агеніції та дослідницькі компанії публікують у відкритому доступі інформацію щодо типів, видів кіберзагроз та надслідками, що пов'язані у разі їхнього настання, та відповідно необхідністю упередження кібервзломів. Таку статистичну звітність можна спостерігати у базах даних Євростат, Статистика, Світовий банк, статистика ОЕСД. Приватні аналітичні компанії, діяльність яких безпосередньо стосується питань кібербезпеки (наприклад e-Governance Academy, Surfshark VPN service, The Fletcher School, Kaggle та ряд інших), науково-дослідницькі інститути в межах реалізації своїх наукових грантів публікують у відкритому доступі інформацію (проте її не так вже й багато, що обумовлюється об'єктивними причинами), що пов'язана з проблемами кібербезпеки, методологічиними підходоми до її визначення та оцінювання.

Зокрема, в країнах Європи з 2004 року Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (The European Union Agency for Cybersecurity, ENISA) опікується питаннями щодо високого загального рівня кібербезпеки. Агентство ENISA сприяє кіберполітиці ЄС, підвищує надійність продуктів, послуг і процесів інформаційно-комунікаційних технологій за допомогою схем сертифікації кібербезпеки. Законадавча база ЄС дуже потужна та спрямована на формування безпечного інформаційного простору для суб'єктів економіко-політичної діяльності та охоплює різні сфери діяльності держав (освітньо-наукову, соціальну, медичну, страхову). Зокрема дослідження "Cybersecurity Assessments", що було проведено за 2018-2022 роки ENISA (ENISA, January 2024), описує різні способи оцінки кібербезпеки

ІКТ-рішень, таких як стандарти, національні та приватні схеми та методології сертифікації.

Проте не зважаючи на потужну нормативну базу ЄС щодо протидії кіберзлочинам, стан ландшафту загроз кібербезпеці, уразливостей та інцидентів кібербезпеки залишається надзвичайно широким. Прямими загразоми були й залишаються: програми-вимагачі; шкідливе програмне забезпечення; соціальна інженерія; загрози для даних; загрози доступності: відмова в обслуговуванні; загроза доступності: Інтернет-загрози; маніпулювання інформацією та втручання; атаки на ланцюги поставок (ENISA Threat Landscape 2023).

Відліковою точкою для виявлення шахрайств в електронному банкінку є перевірка дотриманню стандартного набору правил Європейського банківського управління (European Banking Authority, EBA) для регулювання та нагляду за банківською діяльністю у всіх країнах ЄС, адже саме банківська система є найбільш вразливою для використання великої кількості різноманітних витонтчених шахрайських схем із залученням всіх учасників фінансових операцій: клієнтів банку (фізичних чи юридичних осіб), співробітників банків, економічних агентів (підприємства, фірми), держава.

Європейська система центральних банків (ЄСЦБ) містить:

- Європейський центральний банк;
- Національні центробанки з усіх 27 держав-членів Євросоюзу.

Окремо виділяють Євросистему, що об'єднує основні банківські структури 20 країн-членів ЄС, які перейшли на валюту євро. Євросистема та ЄСЦБ співіснуватимуть доти, доки є країни-члени Євросоюзу за межами єврозони.

Європейський центральний банк (ЄЦБ) є ядром ЄСЦБ і Євросистеми. Він був створений 1 червня 1998 року. ЄЦБ є незалежним у здійсненні своїх повноважень і є юридичною особою відповідно до міжнародного публічного права. Штаб-квартира знаходиться у Франкфурті-на-Майні, Німеччина.

ЄЦБ Європейський центральний банк має три органи, які приймають рішення, а також керують ЄСЦБ та Євросистемою:

1. Рада керівників ЄЦБ – головний орган, який приймає рішення. Він формулює грошово-кредитну політику зони євро та приймає керівні принципи, необхідні для виконання завдань.

2. Виконавча рада – оперативний орган ЄЦБ та Євросистеми, який реалізує грошово-кредитну політику зони євро відповідно до рішень Ради керуючих та керує поточною діяльністю Європейського центробанку. До його складу входять президент, віце-президент та ще чотири члени.

3. Генеральна рада створена як третій директивний орган ЄЦБ. Це перехідний орган, який існуватиме доти, доки всі держави-члени ЄС не перейдуть на євро, після чого його розпустять.

Є також наглядова рада, створена після того, як на ЄЦБ було покладено конкретні завдання щодо пруденційного нагляду за кредитними організаціями в рамках Єдиного наглядового механізму (ЄЕС) з метою сприяння надійності та стабільності банківської системи.

16 січня 2023 року набула чинності Директива (ЄС) 2022/2555 (NIS2, 2023), яка замінила Директиву (ЄС) 2016/1148. Агентство Європейського Союзу з кібербезпеки (The European Union Agency for Cybersecurity, ENISA) вважає, що NIS2 покращує існуючий стан кібербезпеки в ЄС за допомогою:

– створення необхідної структури управління кіберкризою (CyCLONe) (Європейська мережа організації зв'язку з кіберкризами – це мережа співпраці національних органів держав-членів, які відповідають за управління кіберкризами (мережа була запущена в 2020 році та офіційно оформлена 16 січня 2023 року з набранням чинності NIS2, стаття 16);

– підвищення рівня гармонізації щодо вимог безпеки та зобов'язань щодо звітності, а також генерація нових ідей за допомогою експертних оцінок для покращення співпраці та обміну знаннями між державами-членами;

– заохочення держав-членів до впровадження нових сфер інтересів, таких як ланцюг постачання, управління вразливістю, основний Інтернет та кібергігієна в їхні національні стратегії кібербезпеки.

– охоплення більшої частки економіки та суспільства шляхом включення більшої кількості секторів, що означає, що більше суб'єктів зобов'язані вживати заходів для підвищення рівня кібербезпеки.

Таким чином, алгоритм виявлення шахрайств в електронному банкінгу країн ЄС містить десять базових кроків.

Крок 1. Збір та моніторинг даних: збір та моніторинг транзакцій та активностей клієнтів в реальному часі.

Крок 2. Використання системи аналітики для відстеження звичайних та незвичайних фінансових операцій.

Крок 3. Використання алгоритмів машинного навчання та штучного інтелекту для аналізу та класифікації транзакцій та активностей клієнтів.

Крок 4. Виявлення незвичайних патернів або аномалій, що можуть вказувати на шахрайську діяльність.

Крок 5. Введення правил та обмежень: встановлення правил і обмежень для фінансових транзакцій, які можуть бути підозрілими (наприклад, великі перекази на незвичайні рахунки).

Крок 6. Використання системи оцінки ризику для класифікації та відстеження транзакцій за їхнім рівнем підозрілості.

Крок 7. Міжнародне співробітництво: обмін інформацією з іншими фінансовими установами та правоохоронними органами в ЄС та інших країнах для виявлення міжнародних шахраїв.

Крок 8. Повідомлення та дії: створення системи повідомлень та сповіщень для виявлення та реагування на підозрілу активність.

Крок 9. Заборона або блокування підозрілих транзакцій та рахунків.

Крок 10. Постійне вдосконалення алгоритмів та стратегій виявлення шахрайства на основі набутого досвіду та нових загроз.

Слід також зазначити, що кожний банк чи фінансова установа в ЄС може мати власну стратегію та технологічні рішення для боротьби з шахрайством, які відповідають їхнім потребам та ресурсам.

Окремо для ідентифікації та оцінювання ризиків, запобігання кібершахрайств в електронному банкінгу ENISA рекомендує застосовувати комплексну систему методів. Зокрема, в звіті ENISA Cyber Insurance – Models and methods and the use of AI, (2024) розглядуються класичні актурні підходи, моделі зараження, теоретико-ігрові аспекти, статистичні методи, стохастичне моделювання ризиків, методи навчання під наглядом, неконтрольоване навчання, навчання з підкріпленням, машинне навчання та штучний інтелект, моделювання частоти та серйозності втрат за допомогою нейронних мереж, регресійних лісів, узагальнених лінійних змішаних моделей. При цьому в звіті підкреслюється важливість проблеми збору відповідних даних достатньої якості та деталізації, також необхідність розробки та вдосконалення існуючих підходів до моделювання протидії кіберзлочинам, розробки моделей динамічної стратегічної взаємодії, що включають реалістичні моделі мережі.

***Список використаних джерел***

1. Cybersecurity Assessments: European Union Agency for Cybersecurity, January 2024. URL : https://www.enisa.europa.eu/publications/cybersecurity-market-assessments

2. ENISA serves as the CyCLONe Secretariat boosting cooperation among national Cyber Crises Liaison Organisations. URL : https://www.enisa.europa.eu/topics/incident-response/cyclone

3. ENISA Threat Landscape 2023. URL : https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

4. European Banking Authority. URL : https://www.eba.europa.eu/homepage

5. Cyber Insurance – Models and methods and the use of AI: European Union Agency for Cybersecurity, February 2024. Retrieved from https://www.enisa.europa.eu/publications/cyber-insurance-models-and-methods-and-the-use-of-ai