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

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Матеріали
наукової онлайн-конференції

(Суми, 07 вересня 2023)

Суми
Сумський державний університет
2023

004.056.5:336(082)
В43

Затверджено Вченою Радою Сумського державного університету (протокол № 2, 14.09.2023)

S62 Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 07 вересня 2023. Збірник матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2023. – 183 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

СЕКЦІЯ 3 ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В ПРОТИДІЇ КІБЕРЗАГРОЗАМ

КОНВЕРГЕНЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ТА ПРОТИДІЇ ФІНАНСОВИМ ЗЛОЧИНАМ

CONVERGENCE OF THE CYBER SECURITY SYSTEM AND COMBATING FINANCIAL CRIMES

***Альона Рапута**, студентка*
Сумський державний університет, Україна

На сьогоднішній день існує серйозна загроза людству у сфері фінансової безпеки з боку кібертероризму. Аналіз актуальності проблеми конвергенції системи кібербезпеки та протидії фінансовим злочинам спрямований на виявлення необхідності використання інновацій, змін, які можливі в ході виявлення взаємозв'язків між цими системами.

Фінансові злочини та зростаюча складність кібератак стали поширеною проблемою для фінансових установ по всьому світу. Впровадження засобів інформаційної безпеки в банківську інфраструктуру дозволяє захистити дані, ресурси та створити міцну основу для дотримання нормативних вимог. Стратегія безпеки даних має бути комплексною, охоплювати людей, процеси та технології, які, завдяки постійному розвитку науки, набувають нових форм та методів для боротьби з незаконними діями шахраїв у сфері фінансів.

Розробка надійної системи кібербезпеки дозволяє не тільки чітко бачити загрози, але й допомагає забезпечити дотримання нормативних вимог [1]. Щоб відповідати нормативним вимогам і протидіяти зростаючій кількості кіберзагроз і шахрайств, фінансова індустрія потребує інструментів, оснащених штучним інтелектом, а також багаторівневою системою захисту від кіберзагроз, яка підтримує швидке та масштабоване виявлення та вирішення проблем. Впровадження цих інструментів значно підвищить надійність захисту даних у сфері фінансів та допоможе протистояти кіберзагрозам, які на сьогоднішній день є актуальною проблемою у всіх сферах, а особливо у сфері фінансів.

Сфера фінансів - сфера обігу грошових і валютних цінностей, а також цінних паперів - найважливіший елемент економіки, який активно розвивається [2]. Дана сфера стала однією з найбільш привабливих для злочинної діяльності.

Злочинна діяльність у фінансовій сфері характеризується вчиненням комплексу протиправних дій, спрямованих на перешкоджання руху переважно грошових коштів або їх замінників [2].

Корисливим злочинам часто сприяє ситуація слабкого контролю за порядком роботи систем, слабкий захист систем від несанкціонованого доступу. Наприклад, недостатній захист від шахрайських дій банківських платіжних документів, недостатня якість їх виготовлення та захищеність [2].

Саме за таких умов ефективним рішенням буде конвергенція системи кібербезпеки та протидії фінансовим злочинам.

Адже в умовах, коли фінансова система держави є вразливою у сфері фінансової безпеки та має нерозвинену систему кіберзахисту – спокій і надійність не гарантовані.

В процесі вивчення теми кібербезпеки та протидії фінансовим злочинам були виявлені фактори, які варто враховувати при аналізі даної теми:

– Конфіденційність даних означає, що дані доступні лише уповноваженим особам.

– Цілісність даних означає впевненість у тому, що дані не будуть фальсифіковані або погіршені під час або після подання. Це переконання, що дані не були змінені навмисно чи ненавмисно.

– Доступність даних означає, що інформація доступна авторизованим користувачам у разі потреби. Щоб система продемонструвала доступність, вона повинна мати добре функціонуючі обчислювальні системи, засоби контролю безпеки та канали зв'язку.

– Глобальний індекс кібербезпеки (GCI), надійний орієнтир, який вимірює прихильність країн кібербезпеці в усьому світі.

– Індекс готовності мережі - має на меті виміряти ступінь готовності країн використовувати можливості інформаційних та комунікаційних технологій.

– Національний індекс кібербезпеки (NCSI) вимірює рівень готовності країни запобігати кіберзагрозам, а також готовність керувати кібер-інцидентами, злочинністю та масштабними кризами.

– Рівень цифрової трансформації (DDL) – це процес повної заміни ручних, традиційних і застарілих способів ведення бізнесу новітніми цифровими альтернативами.

– Індекс злочинності є потужним, але простим для розуміння рейтингом злочинності.

В процесі аналізу теми «Конвергенція системи кібербезпеки та протидії фінансовим злочинам» був проведений канонічний аналіз для виявлення залежності між вищезазначеними факторами.

Канонічний аналіз – це багатовимірний метод аналізу, який передбачає визначення зв'язків між групами змінних у наборі даних. Основною метою

канонічного аналізу є знаходження максимальних кореляцій між групами змінних [3].

Канонічний аналіз даних був проведений за допомогою програми STATISTICA.

	Canonical Analysis Summary (Convergensy.sta) Canonical R: .95472 Chi²(7)=170.94 p=0.0000	
N=76	Left Set	Right Set
No. of variables	1	7
Variance extracted	100.000%	43.6225%
Total redundancy	91.1491%	39.7615%
Variables: 1	DDL	PSI
2		GEI
3		EDB
4		CI
5		CPI
6		GTI
7		FCI

Рисунок 1. Результати канонічного аналізу

На рисунку 1 наведено результати аналізу впливу фактору «Рівень цифрової трансформації» на фактори протидії фінансовій злочинності в країнах.

Як видно, отримане значення канонічного R = 0,95472 є високим, що свідчить про наявність сильного взаємозв'язку між факторами, які характеризують рівень цифрової трансформації та боротьбу з фінансовою злочинністю.

Критерій Пірсона, який складає 170,94, і рівень значущості якого не перевищує 0,05 (p = 0,0000), підтверджує статистичну значущість коефіцієнта кореляції. Значення надлишковості для лівого набору, який являє собою фактор - «Рівень цифрової трансформації», становить 91,1491%. Це свідчить про те, що фактори правої вибірки, які описують боротьбу з фінансовими злочинами, на 91,149% пояснюють мінливість індексу рівня цифрової трансформації, що свідчить про високе значення впливу. Процес боротьби з фінансовим шахрайством в країні залежить від кіберзахисту фінансових систем, оскільки індекс цифрової трансформації на рівні 39,761% описує мінливість факторів, що характеризують боротьбу з фінансовими шахрайствами у країнах.

Отримане значення є високим, і це вказує на те, що система кібербезпеки (індекс рівня цифрової трансформації) має сильний вплив на боротьбу з фінансовим шахрайством.

Таким чином, у процесі аналізу впливу факторів кібербезпеки було виділено один показник, який має сильний вплив на фактори, що

характеризують боротьбу з фінансовою злочинністю, це «рівень цифрової трансформації».

Отже, важливість кібербезпеки зростає. Насправді, наше суспільство є більш технологічно залежним, ніж будь-коли, і немає жодних ознак того, що ця тенденція сповільниться.

Однією з переваг конвергенції кібербезпеки та запобігання фінансовим злочинам є захист мереж і даних від несанкціонованого доступу. Фінансові дані потребують надійного захисту від злочинного використання, яке є серйозною загрозою для функціонування та існування фінансових систем. Тому важливо захистити дані від несанкціонованого доступу, і саме один із показників, який був виявлений у ході дослідження, а саме – «Рівень цифрової трансформації», може допомогти покращити ситуацію, яка складається на сьогоднішній день у сфері фінансів. Для покращення рівня безпеки фінансових установ, попередження протизаконних дій у сфері фінансів потрібно провести процес трансформації та заміни застарілих, ручних способів захисту та збереження інформації на більш новітні цифрові альтернативи.

Список літератури

1. Проект Закону України від 19.06.2015 № 2126а. Про основні засади забезпечення кібербезпеки України. URL: https://ips.ligazakon.net/document/JH1N268A?an=13

2. Задубінний А. В. 2021. Стратегія кібербезпеки України: цілі та пріоритети. URL: https://armyinform.com.ua/2021/08/27/strategiya-kiberbezpeky-ukrayiny-czili-ta-priorytety/

3. Пасько Н. О. 2023. Кібербезпека як ключовий фінтех-тренд року: що варто знати про загрози та захист. URL: https://fintechinsider.com.ua/kiberbezpeka-yak-klyuchovyj-finteh-trend-roku-shho-varto-znaty-pro-zagrozy-ta-zahyst/