обсягів, що унеможливлює ефективне регулювання процесів, які відбуваються на ньому.

Список використаних джерел

1. Артамонова А. А. Біржовий ринок деривативів: світовий досвід та українські реалії // Молодий вчений. 2016. № 4. С. 8–11.

2. Хома І. Б., Угринюк О. Г. Сучасний стан та перспектива розвитку ринку похідних цінних паперів в Україні // Молодий вчений. 2017. № 5. С. 769–774.

3. Офіційний сайт Національної комісії з цінних паперів та фондового ринку України. URL: http:www.nssmc.gov.ua

СУТНІСТЬ ТА ОСОБЛИВОСТІ КІБЕРШАХРАЙСТВ У ФІНАНСОВІЙ СФЕРІ ЯК ОБ'ЄКТІВ СТАТИСТИЧНОГО ДОСЛІДЖЕННЯ

Криклій Олена Анатоліївна,
кандидат економічних наук, доцент,
доцент кафедри фінансів,
банківської справи та страхування,
Сумський державний університет

Сектор банківських та фінансових послуг є найбільш привабливим для кібершахрайств через можливість отримання зловмисниками значних фінансових та нефінансових вигід. Попри значну увагу фінансових установ до запобігання кібершахрайствам, втрати від них є досить значними та будуть зростати, зважаючи на те, що ландшафт кіберзагроз постійно розвивається, приводячи до складнішої кіберекосистеми. Це, насамперед, обумовлено розвитком цифрової інфраструктури, впровадженням нових технологій (блокчейну, криптовалют та штучного інтелекту) в діяльність фінансових посередників). Проблема посилюватиметься тим, що фінансові інформаційні системи ставатимуть все більш взаємопов'язаними, бізнес-процеси – більш автоматизованими, при цьому вже наявна інфраструктура інформаційних та комунікаційних технологій не була розроблена з пріоритетом кібербезпеки, що потребуватиме її адаптації до нових умов діяльності.

Зважаючи на це, розроблення концепції та обґрунтування теоретико-методологічних засад статистичного забезпечення дослідження кібер-шахрайств у фінансовій сфері є важливим науковим та прикладним завданням. Отже, необхідним є уточнення сутності й особливостей кібершахрайств у фінансовій сфері як об'єктів статистичного дослідження.

У найбільш загальному вигляді під кібершахрайством у фінансовій сфері слід розуміти злочини, об'єктом яких є окрема фінансова установа або фінансова система в цілому, що здійснюються за допомогою комп'ютерно-інформаційних технологій та мереж або спрямовані на них, і мають негативні

наслідки, які загрожуватимуть стабільності фінансової системи в цілому або її окремих учасників. Серед таких наслідків виокремлюють включаючи:

– фінансові (прямі) наслідки: збитки, пов'язані зі втратою, витоком або недоступністю інформації, знищенням та подальшим відновленням інформації; збитки від дезорганізації діяльності фінансових установ та втрат, пов'язаних із невиконанням ними своїх зобов'язань;

– нефінансові (непрямі) наслідки: репутаційні втрати та втрата довіри до бренду, втрати від реалізації юридичного ризику через санкції з боку клієнтів, контрагентів та регулятора.

Для збирання й систематизації даних про різні види кібершахрайств, їх структуру та динаміку необхідно систематизувати їх рівні та види, за якими має відбуватись накопичення інформації для подальшої обробки та систематизації (табл. 1, узагальнено автором).

Таблиця 1

Рівні, об'єкти та види кібершахрайств у фінансовій сфері

Рівні	Об'єкти	Види кібершахрайств
Фізичний рівень	Фізичні носії інформації у складі: систем зберігання даних; резервного копіювання; автоматизованих робочих місць. Знімні носії інформації. Канали зв'язку. Монітори. Приміщення, будівлі, споруди. Технічні засоби	Розкрадання / крадіжка
		Знищення / руйнування / диверсії
		Несанкціонований фізичний доступ
		Витік інформації
Мережевий рівень	Комунікаційне обладнання	Атаки «відмова в обслуговуванні»
		Підміна довіреного об'єкта мережі та передача за каналами зв'язку повідомлень від його імені з присвоєнням прав доступу
		Порушення штатних режимів роботи мережевого обладнання
		Упровадження апаратних закладок
Рівень мережевих додатків і сервісів	Мережеві додатки та сервіси	Упровадження шкідливого ПЗ
		Аналіз трафіка
		Атаки «відмова в обслуговуванні»
		Використання спеціалізованих програм
		Порушення штатних режимів роботи мережевих додатків
		Сканування мережі, спрямоване на виявлення відкритих портів та служб, відкритих з'єднань
Рівень операційних систем	Файли даних з персональними даними, банківською та комерційною таємницями. Загальносистемні програмні засоби. Інформація, необхідна для ідентифікації, автентифікації та (або) авторизації. Файли даних з відкритою інформацією	Крадіжка / втрата паролів
		Копіювання
		Модифікація / видалення
		Порушення штатних режимів роботи операційних систем
		Поширення шкідливих програм
		Неправильна (неповна) конфігурація систем захисту інформації
		Несанкціонований логічний доступ до систем з використанням програмного забезпечення

Продовження табл. 1

Рівні	Об’єкти	Види кібершахрайств
Рівень систем управління базами даних	Бази даних інформаційних систем. Інформація, необхідна для ідентифікації, автентифікації і (або) авторизації	Копіювання
		Модифікація
		Неправильна (неповна) конфігурація систем захисту інформації
		Модифікація / видалення
		Порушення штатних режимів роботи систем управління базами даних
		Підміна ідентифікаторів користувача
		Несанкціонований логічний доступ до систем управління базами даних
		Поширення шкідливих програм
		Крадіжка паролів
Рівень технологічних процесів та програм	Програмне забезпечення для обробки персональних даних, банківської та комерційної таємниці, відкритої інформації. Платіжні картки. Інформація, необхідна для ідентифікації, автентифікації та (або) авторизації. Паперові документи	Модифікація / видалення
		Розповсюдження / передача
		Друк документів
		Крадіжка документів та карток
		Крадіжка паролів
Рівень бізнес-процесів	Дані обмеженого доступу Персонал	Саботаж
		Халатність та помилки
		Шкідництво

Базовою методикою ідентифікації кібершахрайств у фінансовій сфері є аналіз причинно-наслідкових зв’язків зовнішніх та внутрішніх загроз, реалізація яких може призвести до певних відхилень від цільових параметрів діяльності банку та цільового перебігу бізнес-процесів. Наслідком цього стають фінансові втрати, погіршення репутації, втрати транзакцій та клієнтів, санкції наглядових органів та юридична відповідальність (табл. 2, узагальнено автором).

Таблиця 2

Наслідки кібершахрайств у фінансовій сфері

	Характеристика	Вид	Характеристика	Підвиди
Фінансові	Вимірюються у грошовому еквіваленті, безпосередньо впливають на фінансовий результат діяльності фінансового посередника	Очікувані	Сума втрат, що повторюються (виникають із частотою не рідше одного разу на календарний рік) та перебувають у діапазоні оцінки грошового еквівалента очікуваних фінансових втрат	Структуруються за масштабами втрат та визначаються в кожному фінансовому посереднику індивідуально
		Неочікувані	Максимальні потенційні втрати внаслідок суттєвих недоліків (помилок) системи внутрішнього контролю або надзвичайних зовнішніх подій, що перебувають у діапазоні оцінки грошового еквівалента неочікуваних фінансових втрат	

Продовження табл. 2

	Характеристика	Вид	Характеристика	Підвиди
Нефінансові	Безпосередньо не впливають на фінансовий результат діяльності, але можуть призвести до несприятливих наслідків для фінансового посередника	Очікувані	Значущість очікуваного нефінансового впливу на горизонті одного календарного року	Втрата іміджу або репутації фінансового посередника: – втрата транзакцій; – втрата клієнта; – втрата груп клієнтів або портфеля; – санкції та стягнення
		Неочікувані	Максимальний потенційний нефінансовий вплив внаслідок суттєвих недоліків (помилок) системи внутрішнього контролю або надзвичайних зовнішніх подій	

З метою статистичного дослідження кібершахрайств у фінансовій сфері необхідною є розробка системи ключових індикаторів, що охоплює такі типи:

1) синхронні індикатори – показники, що характеризують зафіксовані втрати та включають показники реалізації помилок або нереалізованих втрат (наприклад, сума втрат за успішними шахрайськими операціями з платіжними картками, сума неуспішних шахрайських операцій з платіжними картками);

2) казуальні індикатори – показники, пов’язані з первинною причиною події реалізації кібершахрайства (наприклад, частка часу недоступності інформаційної системи / ресурсу банку / фінансової установи);

3) індикатори ефективності контролю – показники поточного моніторингу виконання контролів (наприклад, сума коштів, витрачена при укладанні контрактів з провайдерами).

Граничні значення ключових індикаторів мають визначатись як на основі історичних даних (емпіричний підхід), так і на експертних оцінках співробітників фінансових установ.