УДК 336(477)
Бабенко-Левада В.Г.[1], Цимбал А.С.[2]
[1]канд. економ. наук, доц. НУ «Запорізька політехніка»
[2]студ. НУ «Запорізька політехніка»

КІБЕРШАХРАЙСТВО У ФІНАНСОВОМУ СЕКТОРІ

Ураховуючи трансформаційний вплив цифрової революції на фінансовий сектор, важливість забезпечення кібербезпеки стає надзвичайно великою. Фінансові установи щодня опрацьовують величезний обсяг конфіденційної інформації, що робить їх головною мішенню для кіберзлочинців.

Кібершахрайство – це новий, відмінний від звичайного шахрайства вид кримінального правопорушення, який у результаті еволюції та впливу технологій вчинюється з використанням нових, раніше не досліджених методів, хоча за складом нагадує звичайне шахрайство. [1]

Серед основних форм кіберзлочинності можна виокремити наступні: поширення шкідливого програмного забезпечення, крадіжка номерів кредитних карт та банківських рахунків, вторгнення у системи за допомогою зламаних паролів, порушення прав на інтелектуальну власність. Кіберзлочинці можуть використовувати різноманітні техніки, такі як взлом або обхід захисту, для незаконного доступу до інтелектуальної власності. Це може призвести до значних фінансових втрат для власників прав на інтелектуальну власність, а також до порушення їхнього авторського контролю та репутації.

Серед негативних наслідків кіберзлочинності у фінансовому секторі можна виділити значні фінансові втрати для компаній та їх клієнтів. Кіберзлочинці, які отримують несанкціонований доступ до конфіденційної інформації, такої як банківські реквізити або особисті дані, можуть використовувати цю інформацію для викрадення грошей або здійснення ідентифікаційного шахрайства. Крім того, такі атаки можуть призвести до порушення конфіденційності та приватності клієнтів, що може пошкодити репутацію фінансової

установи. Для попередження цих негативних наслідків необхідно вдосконалювати системи кібербезпеки та реагувати на інциденти швидко і ефективно.

З точки зору науковців про цілеспрямованість розробки заходів проти кібершахрайства, можуть впроваджуватися різними установами та особами. Ці заходи включають:

Залучення технічних експертів або спеціалізованих компаній для підвищення рівня кібербезпеки у державних органах та приватних компаніях. Експерти можуть ускладнити роботу зловмисників, впроваджуючи необхідні захисні алгоритми, в тому числі організаційні, та надаючи інструкції працівникам, що працюють з відповідними системами та мережами.

Слідкування за попередженнями щодо кіберзагроз на офіційних ресурсах Держспецзв'язку та CERT-UA для осіб, які перебувають у зоні ризику. Там публікуються офіційні повідомлення про можливі загрози та поради з їх уникнення.

Якщо особа стала жертвою кібератаки, важливо повідомити про це тих, на кого ця атака може вплинути - співробітників, клієнтів, контрагентів, родичів або друзів.

У разі кібератаки обов'язково повідомляти про це офіційні органи забезпечення кібербезпеки України, CERT-UA та кіберполіцію. Це допоможе притягнути винних до відповідальності та негайно вжити заходів щодо блокування та нейтралізації шкідливих веб-ресурсів.[2]

Щоб уникнути кібершахрайства, потрібно постійно контролювати та покращувати заходи безпеки. Це включає посилення моніторингу мережі та систем для виявлення загроз, регулярне оновлення програмного та апаратного забезпечення для запобігання вразливостям, а також аналіз і вдосконалення правил безпеки. Навчання персоналу про потенційні загрози та методи захисту є також важливим. Крім того, співпраця з іншими гравцями на ринку дозволяє обмінюватися досвідом та інформацією про кращі практики у протидії кіберзлочинності. Такий підхід сприяє розробці більш ефективних стратегій безпеки та збереженню високого рівня кібербезпеки у фінансовому секторі.

Міжнародна співпраця відіграє ключову роль у протидії кіберзлочинності через глобальний характер цього явища. Вона сприяє обміну інформацією про кіберзагрози, спільним розслідуванням кіберзлочинів, розвитку міжнародних стандартів та політик у галузі кібербезпеки, підтримці країн з менш розвиненою кіберінфраструктурою та розвитку міжнародного права щодо кібербезпеки. Тільки через спільні зусилля країн можна створити більш безпечне та стійке цифрове середовище для всіх користувачів Інтернету.

Отже, у світі, де цифрові технології перетинаються з усіма аспектами нашого життя, фінансові установи стають особливим об'єктом інтересу для кіберзлочинців. Кібершахрайство у фінансовому секторі не лише призводить

до матеріальних збитків для компаній і клієнтів, але також підриває довіру до фінансових установ та може викликати серйозні наслідки для економіки загалом. У протидії цій загрозі необхідно посилювати заходи кібербезпеки, включаючи не лише технічні заходи, але й навчання персоналу та співпрацю зі спеціалізованими організаціями. Постійний моніторинг, актуалізація програмного та апаратного забезпечення, а також підвищення рівня обізнаності щодо кіберзагроз є важливими складовими успішної стратегії кібербезпеки. Лише спільними зусиллями фінансовий сектор зможе забезпечити свою захищеність від кібершахрайства та зберегти довіру клієнтів та інвесторів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Сайт Запорізької гімназії №40 Запорізької міської ради [Електронний ресурс]. Режим доступу: https://school40.zp.ua/content/kibershahraystvo

2. Ярема М., Борисенко А. Боротьба з кіберзлочинністю в умовах дії воєнного стану:Закон2149-IX. [Електронний ресурс]. Режим доступу: Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX | ЮРЛІГА (ligazakon.net)