Євгеній Олександрович ПЕРЕПЕЛИЦЯ,
курсант навчальної групи Ф4-102
Харківського національного університету внутрішніх справ

КІБЕРБЕЗПЕКА У ФІНАНСОВІЙ СФЕРІ

Останнім часом питання кіберзлочинності набуло глобального масштабу, а збитки від діяльності кібернетичних шахраїв сягнули десятків мільярдів доларів [1]. Поміж найбільш вразливих до кібернетичних злочинних сфер суспільного життя відноситься сектор фінансової економіки. Кібербезпека в фінансовій сфері є дуже важливим питанням, оскільки фінансові установи та банки є ціллю для кіберзлочинців, які намагаються зламати безпекові системи, щоб отримати доступ до конфіденційної інформації та коштів. Незаконний доступ до фінансових даних може призвести до серйозних наслідків для фінансових установ та їх клієнтів.

Одним з основних завдань кібербезпеки у фінансовій сфері є захист від кібератак, які можуть спричинити значні збитки для банків та інші заклади фінансових послуг. Наприклад, хакери можуть спробувати здійснити шахрайство з використанням крадіжки особистих даних клієнтів, розповсюдження шкідливих програм, вимагання викупу в обмін на доступ до важливої інформації, інші атаки на фінансові системи.

Останнім часом розповсюдження набули такі види злочинів: кіберзлочинність у фінансово-банківській сфері; шахрайство з використанням платіжних карток та їх реквізитами; крадіжки коштів з банківських рахунків; заволодіння конфіденційною комп'ютерною інформацією про клієнтів тощо.

Шахраї все більше мріють заволодіти банківськими рахунками як звичайних громадян, так і великих компаній та організацій. Зі зростанням обсягів безготівкових розрахунків зростає і чисельність потерпілих від кібершахраїв. Чинниками, які сприяють зростанню кіберзлочинів, є зростання та підвищення ІТ-технологій, значна територія для скоєння кіберзлочин [1].

Програми, за допомогою яких шахраї відбирають гроші у населення і банків є безліч, наприклад віруси Gamker і Carberp. Це банківські віруси, які ще називають троянами для крадіжки інформації. Вірус-троян вражає або частино підстроюється під код системи та краде інформацію з онлайн-банкінгу у якому містяться публічні та приватні ключі, криптографічні утиліти та додатки, пов'язані з фінансами. Він здатний перехоплювати натискання

клавіш і зберігати комбінації в окремий файл. Програмні коди вірусу також зберігають знімок з екрана, розвинуті віруси вміщують у себе записи командного рядка, після чого посилає всі дані до шахраїв [2].

Існує кілька методів, які використовуються для підвищення кібербезпеки в фінансовій сфері:

1. Захист від кібератак: фінансові установи повинні застосовувати заходи безпеки, такі як двофакторна аутентифікація, захист від зламу паролів та фільтри для розпізнавання шкідливих програм.

2. Перевірка та моніторинг: важливо ретельно перевіряти фінансові транзакції, щоб виявити будь-які аномалії або підозрілу діяльність. Крім того, системи моніторингу допомагають виявляти та запобігати кібератакам.

3. Освіта: фінансові установи повинні надавати своїм працівникам та клієнтам інформацію про кібербезпеку та оновлювати їх знання щодо нових загроз та заходів безпеки.

4. Реагування на інциденти: важливо мати план дій для реагування на кібератаки та негайно реагувати на будь-які підозрілі події, які можуть стати загрозою для безпечного користування онлайн банкінгом.

5. Захист даних: фінансові установи повинні захищати конфіденційні дані своїх клієнтів шляхом шифрування, захисту від зламу.

Висновки. Явище кіберзлочинності має досить велику суспільну небезпечність. Про це свідчать такі явища як: стрімке зростання кількості вчинюваних кіберзлочинів; можливість завдання шкоди як фізичним, так і юридичним особам, і навіть державним структурам; досить складні способи захисту, і складність застосування найпростіших з них пересічними громадянами через неосвіченість у даній сфері тощо. Потрібно зауважити, що є способи підвищити рівень кібербезпеки як країни в цілому, так і кожної конкретної людини, а саме:

1. Вдосконалення прав осіб які користуються банкоматами та онлайн банкінгом і законів боротьби з кіберзлочинністю

2. Чітке розмежування компетенції та функцій правоохоронних органів

3. Покращення практичного досвіду працівників підрозділів кіберполіції України

4. Поліпшення методичного забезпечення розслідування кіберзлочинів

5. Налагодження співпраці зі службою безпеки банків та підприємств та судовою системою.

Список бібліографічних посилань

1. Проблеми українського суспільства: кіберзлочинність - PDF Free Download. Enjoy free comfortable tools to publish, exchange, and share any kind of documents online!. URL: https://docplayer.net /71413983-Problemi-ukrayinskogo-suspilstva-kiberzlochinnist.html (дата звернення: 10.04.2023).

2. Протидія кіберзлочинності в фінансово-банківській сфері - PDF Free Download. *Enjoy free comfortable tools to publish, exchange, and share any kind of documents online!*. URL: https://docplayer.net /48379249-Protidiya-kiberzlochinnosti-v-finansovo-bankivskiysferi.html (дата звернення: 10.04.2023).

Одержано 12.04.2023

Софія Дмитрівна ПЕРЕПЕЛІЦИНА,
курсантка навчальної групи Ф1-305
Харківського національного університету внутрішніх справ

ПРОБЛЕМИ ПРИТЯГНЕННЯ ДО КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА КОЛАБОРАЦІЙНУ ДІЯЛЬНІСТЬ

Сьогоднішні події в Україні стають все більш напруженими. Багато громадян, які знаходяться на тимчасово окупованій території перейшли на сторону країни-агресора. Саме тому постає питання про притягнення таких громадян до кримінальної відповідальності.

3 березня Верховною Радою України прийнятий і 15 березня 2022 р. набув чинності Закон № 2108-IX, яким включено до Кримінального кодексу України нову статтю 111-1 «Колабораційна діяльність», що охопила значну кількість складів кримінальних правопорушень щодо співпраці з державою-агресором [1].

Колабораційна діяльність — це публічне заперечення громадянином України здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України або публічні заклики громадянином України до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора, до співпраці з державою-агресором, збройними формуваннями та/або окупаційною