А. Д. Вашкевич, Д. В. Латышева
Научный руководитель — кандидат экономических наук Е. С. Пономарёва
БГЭУ (Минск)

КИБЕРАТАКИ В БАНКОВСКОЙ СФЕРЕ

Кибератаки — негативное явление глобальной цифровизации, которое усугубилось после пандемии коронавируса и обострилось в связи с нестабильной геополитической обстановкой. При этом именно банковская сфера является наиболее привлекательной для преступников, так как здесь совершается множество транзакций с денежными средствами.

В банковской сфере основными видами кибератак с использованием компьютерной техники являются: кража данных платежных карточек и электронных платежных систем граждан, получение сведений о финансовых операциях и банковских счетах, атаки на системы дистанционного банковского обслуживания.

Согласно данным отчета ОАО «Банковский процессинговый центр», основная доля мошенничества в Республике Беларусь в 2022 г. приходилась на мошенничество с банковскими платежными карточками с применением методов социальной инженерии, которая позволяет с помощью психологических манипуляций, методов и технологий, направленных на получение конфиденциальной информации, заставить пользователей путем излишней доверчивости совершать ошибки [1]. Именно ее инструменты лежат в основе 97 % успешных атак с похищением денег у людей. В 2022 г. использовались следующие схемы: рассылка информационных сообщений от имени банков; схемы с оформлением кредита; рассылка фишинговых ссылок; звонки от псевдосотрудников правоохранительных органов.

По данным ОАО «Банковский процессинговый центр», в 2022 г. общее количество мошеннических операций уменьшилось на 2858 ед. и составило 17 739 ед. Мошенничество, связанное с перехватом счета (account takeover), увеличилось на 20 % по сравнению с 2021 г. и составило 40 % от общего числа преступлений, использование реквизитов карточек в мошеннических целях составляет 60 % и уменьшилось на 30 %, мошеннические операции с применением поддельных карточек не зафиксированы, а утерянными или украденными карточками воспользовались 11 раз. В то же время общая сумма успешных мошеннических операций в 2022 г. уменьшилась на 15 %, а средняя сумма одной мошеннической операции составила 42 дол. США, что соответствует аналогичному показателю прошлого года [2].

Основными жертвами кибератак в банковской сфере являются клиенты банков, которые мало осведомлены о цифровой безопасности. Для решения этих проблем предлагается внедрить сайт в сети Интернет, который позволит пострадавшему оперативно оповестить правоохранительные органы и простых граждан о мошеннических операциях. Аналогичная система функционирует в США под названием «Центр жалоб на интернет-преступления» (IC3) [3].

Также необходимо обеспечить кибербезопасность посредством повышения финансовой грамотности граждан, обучение их основам информационной безопасности, предупреждение населения и банков о возможных атаках, внедрение новых программ защиты, запуск новых продуктов страхования от киберугроз, обеспечение непрерывного обмена данными об информационных инцидентах на международном уровне и т.п.

Источники

1. Социальная инженерия в контексте информационной безопасности: понятие, виды, значение [Электронный ресурс] // Следственный комитет Республики Беларусь. — Режим доступа: https://sk.gov.by/ru/news-ru/view/sotsialnaja-inzhenerija-v-kontekste-informatsionnoj-bezopasnosti-ponjatie-vidy-znachenie-10991/. — Дата доступа: 25.03.2023.

2. Отчет о тенденциях и случаях мошенничества в сфере платежных инструментов и сервисов за 2022 год [Электронный ресурс] // Банковский процессинговый центр. — Режим доступа: https://npc.by/bankovskie-kartochki/protivodeystvie-moshennichestvu-v-sfere-tsifrovykh-tekhnologiy/analitika/otchet-o-tendentsiyakh-i-sluchayakh-moshennichestva-v-sfere-platezhnykh-instrumentov-i-servisov-za-2022/Годовой%20отчет%202022.pdf. — Дата доступа: 25.03.2023.

3. *Пейзак, А. В.* Противодействие киберпреступности в США / А. В. Пейзак // Общество, право, государственность: ретроспектива и перспектива. — 2022. — № 4 (12). — С. 54–59.