УДК 338

КИБЕРПРЕСТУПНОСТЬ В БАНКОВСКОЙ СФЕРЕ

Короткова И.С.,

студентка

НИУ «Белгородский государственный университет»

г.Белгород, Россия

Мельникова Н.С.

канд. экон. наук, доцент кафедры инновационной экономики и финансов Института экономики и управления, Белгородский государственный национальный исследовательский университет

НИУ «Белгородский государственный университет»

г.Белгород, Россия

Аннотация. Банковский сектор является одним из основных источников экономического состояния страны. Одной из современных проблем человечества стала киберпреступность. С ростом цифровизации, растет и уровень мошенничества в экономике. Развитие информационных технологий как положительно, так и отрицательно влияет на банковский сектор, так как с течением времени мошенники изобретают новые схемы взлома систем безопасности. В статье рассмотрены понятие и виды киберпреступлений в банковском секторе экономике, а также пути решения данной проблемы и снижения риска их совершения, меры защиты общества от киберпреступности. Уделяется внимание динамике совершенных операций без согласия клиентов.

Ключевые слова: банковская сфера, киберпреступность, ущерб, потери, кибератаки, информационные технологии, мошенничество, экономическая преступность, глобализация ,глобальная сеть Интернет.

CYBERCRIME IN BANKING

Korotkova I.S.
student
NRU "Belgorod State University"
Belgorod, Russia
Melnikova N.S.
PhD in Economics, Associate Professor, Department of Innovative Economics and Finance, Institute of Economics and Management, Belgorod State National Research University
Belgorod, Russia

Annotation. The banking sector is one of the main sources of the country's economic condition. Cybercrime has become one of the modern problems of mankind. With the growth of digitalization, the level of fraud in the economy is also growing. The development of information technology both positively and negatively affects the banking sector, as over time, fraudsters invent new schemes for hacking security systems. The article discusses the concept and types of cybercrime in the banking sector of the economy, as well as ways to solve this problem and reduce the risk of their commission, measures to protect society from cybercrime. Attention is paid to the dynamics of transactions performed without the consent of customers.

Key words: banking, cybercrime, damage, losses, cyber attacks, information technology, fraud, economic crime, globalization, the global Internet.

Сегодня почти каждый аспект современной жизни сопровождается информационными технологиями. Распространение компьютеров и доступность информационных и коммуникационных систем создали компьютерные вирусы и другие средства преступлений. Использование

компьютеров и информационно-коммуникационных систем позволяет использовать компьютерные вирусы и другие технические средства для доступа к базам данных, банковским счетам и автоматизированным системам управления для совершения преступлений.

Угрозы связанные с текущим этапом развития информационных технологий, можно отнести такие как: кража данных платежных карт, преднамеренная кража личной и коммерческой информации клиентов, умышленный вред информационным системам или средствам коммуникации. Список угроз связанных с причинения ущерба предприятиям и физическим лицам не является исчерпывающим, но неизбежно приводит к возможности киберпреступности. Так как возникает возможность совершать преступления анонимно и быстро разбогатеть за счет этого, данная проблема продолжает расти, и набирает растущее число сторонников.

Одной из сфер в которой набирает огромные масштабы киберпреступность – это банковское дело, так как оно широко использует информационные технологии. Тема является актуальной на сегодняшний день, так как необходимо искать и применять новые способы борьбы с киберпреступлениями.

Так что же такое киберпреступность и какие существуют виды кибепреступлений?

Кибепреступность – это преступления совершенные одним человеком или группой людей направленные на достижения личных корыстных целей в области информационных технологий. В большинстве случаев основной целью кибепреступности является получение прибыли незаконным способом.

Рассмотрим основные виды кибепреступлений, изображенные на рисунке 1.

Рис.1- Виды киберпреступлений [авторская методика].

Следует отметить, что в основном к киберпеступлениям относят 2 типа деятельности: мошенничество связанное с компьютерами (вирусы, хакерские атаки), либо деятельность с использованием компьютера для совершения преступных действий (распространение вредоносных программа, кража данных).

Далее, рассмотрим динамику объема операций без согласия клиентов за 2020-2022 год в млн. рублей, представленную на рисунке 2.

Рис.2- Объем операций без согласия клиентов за 2020-2022 год в млн. рублей [6].

Также рассмотрим динамику количества операций без согласия клиентов за 2020-2022 год в тыс. рублей (рисунок 3).

Рис.3- Динамика количества операций без согласия клиентов за 2020-2022 год в тыс. рублей [6].

Исходя из рисунков 2 и 3, можно сделать вывод о том, что в 2021 году количество и объем операций без согласия клиентов увеличились по сравнению с 2020 годом на 33,8 и 38,8% соответственно на фоне активного развития новых дистанционных платежных сервисов и роста объема денежных переводов с использованием электронных средств платежа (платежные карты и иные электронные средства платежа).Благодаря расширению комплекса мер, которые банки принимают для противодействия мошенничеству, количество операций без согласия клиентов в отчетный период снизилось на 15,31% по сравнению с 2021 годом.

Главным инструментом воздействия на людей злоумышленниками является метод социальной инженерии. Это такой прием, при котором человек под психологическим воздействием добровольно переводит денежные средства или раскрывает банковские сведения, позволяющие злоумышленникам совершить хищение. Доля таких операций снизилась с 61,8 до 49,4%. По оценке Банка России, в 2021 году наблюдался рост

средней суммы одного хищения, совершенного с использованием приемов и методов социальной инженерии, что в том числе привело к увеличению общего размера ущерба по операциям без согласия клиентов. В 2021 году клиентам кредитных организаций возвратили 6,8% (920,5 млн руб.) от всего объема операций по переводу денежных средств, совершенных без согласия клиентов (в 2020 году данный показатель составил 11,3%, или 1 105,3 млн руб.).

В Российской Федерации хакерские группы, такие как «Cobalt», «MoneyTaker» и «Lazarus», являются основным источником кражи средств. В настоящее время эти группы представляют опасность для банковского сообщества не только в Российской Федерации, но и на международном уровне, нарушая работу каждой банковской системы с целью захвата финансовых активов.

Какие же меры следует предпринять по борьбе с мошенничеством в банковском секторе?

Основными методами противодействия с хакерскими атаками должны являться:

- активный мониторинг и своевременное обновление систем защиты в банковских учреждениях;
- непрерывное обновление защиты кредитными и финансовыми учреждениями и возможное сотрудничество с поставщиками антивирусного программного обеспечения,
- сотрудничество с национальными и международными организациями, предоставляющими помощь в предотвращении и борьбе с киберугрозами;
- создать специализированные отделы для предотвращения и борьбы с киберпреступностью в организациях;
- использование сложных и безопасных паролей;

— повышение финансовой грамотности населения.

Подведя итог, следует сказать, что главной проблемой киберпреступности в банковском секторе- это низкая обнаруживаемость, которая неэффективна в долгосрочной перспективе, отсутствие возможности быстро устранять угрозы, быстрая идентификация нарушителей и улучшение правовой базы по борьбе с киберпреступностью.

Библиографический список:

1. Батюкова В. Е. Состояние киберпреступности в банковской сфере //Государственная служба и кадры. – 2021. – №. 3. – С. 77-79.
2. Богданов А. В. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу //Криминологический журнал. – 2020. – №. 1. – С. 15-20.
3. Кутовой Я. С. Актуальные проблемы киберпреступности в банковской сфере //Modern Science. – 2019. – №. 10-3. – С. 170-174.
4. Лакомов А. С. Киберпреступность: современные тенденции //Академическая мысль. – 2019. – №. 2 (7). – С. 53-56.
5. Юсупова О. А. Киберпреступность в банковской сфере: современное состояние и способы защиты //Научный электронный журнал Меридиан. – 2020. – №. 9. – С. 57-59.
6. Официальный сайт Центрального Банка. – Режим доступа: https://cbr.ru/analytics/ib/review_1q_2q_2020/

Оригинальность 83%