Научная статья
https://doi.org/10.24412/2220-2404-2024-12-7
УДК 336.711

КИБЕРПРЕСТУПНОСТЬ В БАНКОВСКОЙ СФЕРЕ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Долотова Н.П.
Тамбовский государственный технический университет

Аннотация. *В статье рассмотрены теоретические вопросы формирования кибермошенничества в банковской сфере: сущность, классификация и основные виды киберпреступлений. Проанализированы инциденты нарушения информационной безопасности при осуществлении банковских операций и методы противодействия им. Кибермошенничество в банковской сфере достаточно сложное и многоаспектное понятие, которое набирает обороты особенно сегодня и представляет собой использование различных технологий и методов для совершения незаконных действий с целью получения доступа к финансовым средствам, данным или другим активам клиентов и банков.*

Основной целью написания статьи является выявление основных проблем и описание мер по повышению эффективности методов противодействия киберпреступлениям в банковской сфере. В соответствии с целью, поставлены следующие задачи: изучить сущность кибермошенничества в банковской сфере, выявить основные проблемы обеспечения кибербезопасности в банковской сфере, изучить меры по повышению эффективности методов противодействия киберпреступлениям в банковской сфере, изучить меры по повышению эффективности методов противодействия киберпреступлениям в банковской сфере.

Ключевые слова: *банк, кибермошенничество, кибербезопасность, кибератака, цифровизация, онлайн-банкинг, банковская система, информационные системы.*

CYBERCRIME IN THE BANKING SECTOR IN THE RUSSIAN FEDERATION

Natalia P. Dolotova
Tambov State Technical University

Abstract. *The article discusses the theoretical issues of the formation of cybercrime in the banking sector: the essence, classification and main types of cybercrime. The incidents of information security violations during banking operations and methods of countering them are analyzed. Cyber fraud in the banking sector is a rather complex and multidimensional concept that is gaining momentum especially today and represents the use of various technologies and methods to commit illegal actions in order to gain access to financial funds, data or other assets of customers and banks.*

The main purpose of this article is to identify the main problems and describe measures to improve the effectiveness of methods of countering cybercrime in the banking sector. In accordance with the goal, the following tasks are set: to study the essence of cyberbullying in the banking sector, to identify the main problems of ensuring cybersecurity in the banking sector, to study measures to improve the effectiveness of methods of countering cybercrime in the banking sector, to study measures to improve the effectiveness of methods of countering cybercrime in the banking sector.

Keywords: *banking, cyberbullying, cybersecurity, cyberattack, digitalization, online banking, banking system, information systems.*

Введение.

Кибермошенничество в банковской сфере представляет собой использование различных технологий и методов для совершения незаконных действий с целью получения доступа к финансовым средствам, данным или другим активам клиентов и банков

Киберпреступность – это одно из основных направлений преступности, которое набирает огромные обороты. Преимущественный рост киберпреступлений наблюдается в двадцать первом веке вместе с повсеместным внедрением компьютерных технологий в жизнь общества.

Для понимания проблем, которые снижают уровень кибербезопасности в банковской

сфере, и для выявления направлений совершенствования мер противодействия киберпреступности в банковской сфере следует проанализировать современное состояние киберпреступности в банковской сфере: инциденты нарушения информационной безопасности при осуществлении банковских операций и методы противодействия им, рассмотреть современные мошеннические практики, используемые в банковской сфере.

Обсуждение.

Обеспечение кибербезопасности в банковской сфере требует комплексного подхода. Необходимость постоянного мониторинга и адаптации к новым угрозам, развитие быстрого реагирования, систематизация и создание стандартов обеспечения безопасности, постоянное обновление шифрования.

Рассмотрим динамику инцидентов нарушения информационной безопасности при осуществлении банковских операций в России за период с 2019 по 2023 год. Целью проведения анализа является выявление тенденций, оценка влияния различных форм противодействия киберпреступности в банковской сфере. Особое внимание при этом будет уделено анализу операций без согласия клиентов, доле социальной инженерии в данных операциях, доле возмещенных средств, каналам осуществления мошеннических практик, видам и векторам современных мошеннических практик. Реализация рисков и их влияние на финансовые процессы позволяют оценить эффективность банковского киберпространства[1].

Результаты.

В таблице 1 представлена информация об общей картине операции без согласия клиентов за период с 2020 по 2023 годы. Источником послужила информация, размещенная на официальном сайте ЦБ РФ.

Таблица 1 – Операции без согласия клиентов (ОБС): общая картина за период с 2019 по 2023 год [2].

Год	Квартал	Количество операций без согласия клиентов, ед.	Объем операций без согласия клиентов, тыс. рублей	Доля социальной инженерии, %	Доля возмещенных средств (от объема), %
2020	1 квартал	169501	1830299,50	64,0	11,3
	2 квартал	192636	2177427,51	68,6	12,8
	3 квартал	182954	2716549,83	63,8	13,1
2021	1 квартал	237 737	2 873 356,49	56,2	7,3
	2 квартал	236 971	3 013 664,38	47,0	7,4
	3 квартал	256 198	3 206 473,23	41,0	7,7
2022	1 квартал	258 097	3 294 160,94	52,5	6,2
	2 квартал	211 263	2 848 614,92	44,8	5,0
	3 квартал	229 757	3 973 456,54	54,1	3,4
2023	1 квартал	252 111	4 549 282,42	50,5	4,3
	2 квартал	279 706	3 622 543,21	46,5	4,5
	3 квартал	288 784	3 591 091,15	31,6	5,5

Более наглядно отразим информацию из таблицы 1, касательно количества и объема операций без согласия клиентов за период с 2020 по 2023 год в виде диаграммы на рисунке 1.

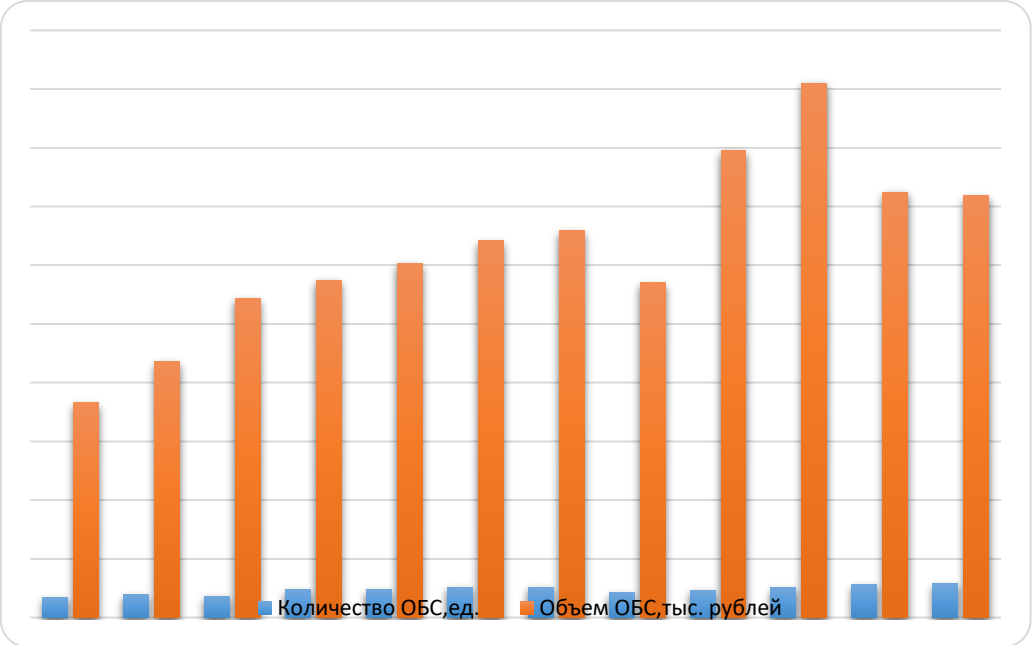

Рисунок 1 – Количественные характеристики операций без согласия клиентов за период с 2020 по 2023 год, ед. и тыс. руб.

Количество операций без согласия клиентов ежеквартально вплоть до 1 квартала 2022 года растет. Банк России основной причиной увеличения выделяет активное развития новых дистанционных платежных сервисов и роста объема денежных переводов с использованием электронных средств платежа (платежные карты и иные электронные средства платежа).

2020 год характеризуется пиком пандемии COVID-19, которая привела к резкому росту числа людей, работающих дома, совершающих покупки в Интернете и активно пользующихся цифровыми технологиями, что способствовало увеличению мошеннических практик в киберпространстве.

Одним из основных элементов формирования страны с развитой экономикой является ее экономическая политика государства, которая также включает в себя денежную политику. Правильная денежная политика является обязательным условием для достижения стабильного развития экономики. Практически, это составная часть инфраструктуры, достаточно важный, однако полностью не достаточный фактор экономического роста.

Во втором квартале 2022 года снизилось количество операций без согласия клиентов и достигло 211 263 ед., что на 25708 ед. меньше аналогичного показателя предшествующего года. Такая динамика объясняется снижением активности кибермошенников в отношении граждан с конца февраля и по апрель включительно.

Наибольшее число операций без согласия клиентов за рассматриваемый период времени пришлось на 1 квартал 2023 года. Банк России определяет основную причину, как: рост объема денежных переводов с использованием карт до 136,38 трлн. руб. Чтобы выявить, какие клиенты больше подвержены мошенническим практикам, обратимся к информации об операциях без согласия клиентов в разрезе физических и юридических лиц.

Наибольшим атакам подвержены физические лица, юридические лица хоть и менее подвержены атакам, но как и физические лица, остро реагируют на изменения внешних условий. Так, 2020-2021 годы характеризуются распространением пандемии и расширению онлайн-сервисов, что способствовало увеличению атак на системы, обеспечивающие удаленную работу. В 2022 году отмечается рост кибератак в связи с изменившейся внешнеполитической обстановкой, а также с тем, что многие отечественные предприятия не были готовы к подобному развитию ситуации.

Продвижение безналичных платежей и цифровой трансформации при сохранении безопасности банковских операций, продолжая совершенствовать правовую базу, механизмы и политику платежей

для создания благоприятных условий для содействия появлению новых бизнес-моделей, продуктов, удобных и безопасных услуг, отвечающих требованиям предприятий и частных лиц.

В последние два десятилетия международные взаимоотношения между различными государствами и движениями во всем мире претерпевают существенные изменения. Глобализация всё больше связывает существующие страны в единую систему, функционирование которой находится в зависимости от норм международного права. Для обеспечения соблюдения этих норм необходимы специальные меры. Одним из универсальных методов воздействия на нарушителей является лишение его специальных прав на мировой арене и вытекающее из этого принуждение к соблюдению норм международного права. В данном случае, принуждение выступает не в качестве насилия, а как средство осуществления международного права. Для легитимности такой меры воздействия, как принуждение, требовалась его узаконенная форма. Такой формой стали санкции.

Обратимся к наиболее типичным схемам кибермошенничества используемым кибермошенниками в период с 2019 по 2024 годы [2]:

1. Предоставление налоговых деклараций.
2. Мошенники похищают деньги и имущество под предлогом обновления банкнот Банка России.
3. Хакеры распространяют вирусные шаблоны документов, чтобы похитить средства компаний.
4. Злоумышленники стали похищать деньги без данных карты.
5. Мошенники представляются работодателями.
6. Утечка персональных данных.
7. Представляются сотрудниками операторов мобильной связи.

На рисунке 2 представлена информация о возрасте жертв, пострадавших от кибермошенничества за 2023 год в долевом соотношении. Источником послужила информация, размещенная на официальном сайте ЦБ РФ.

Наибольшая доля принадлежит возрастному интервалу от 25 до 44 лет. Банк России основной причиной выделяет, что именно данная категория вместе с категорией от 45 до 64 лет, является наиболее активными пользователями сервисов онлайн-банкинга. Также отмечается, что пострадавшими, в большей степени, выступают представительницы женского пола. Доля кибератак в банковской сфере, приходящихся на женщин, составляет 55,5%, причем данный перевес был достигнут за 1 год.

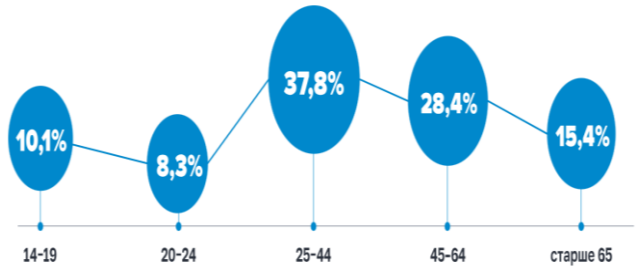

Рисунок 2 – Возраст пострадавших от кибермошенничества в долевом соотношении в 2023 году, % [3].

Наглядно представим меры борьбы с киберпреступностью в банковской сфере в таблице 2 [4].

Таблица 2 – Ключевые меры борьбы с киберугрозами в банковской сфере и способы их реализации.

Меры борьбы с киберугрозами	Способы реализации мер
1.Улучшение систем обнаружения и предотвращения	- Внедрение передовых систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS). - Построение гибких систем, способных адаптироваться к новым угрозам и технологическим изменениям
2.Шифрование данных	- Внедрение технологий управления ключами шифрования для обеспечения их надежности и безопасности. - Регулярное обновление шифрования для обнаружения уязвимостей и обеспечения соответствия стандартам безопасности.
3.Многофакторная аутентификация.	- Использование комбинации различных методов аутентификации, таких как пароль, биометрические данные или одноразовые коды
4.Регулярное обновление и патчинг	- Систематическое обновление программного обеспечения, операционных систем и приложений для устранения известных уязвимостей.

	- Автоматизация процессов патчинга для обеспечения своевременного обновления систем.
5.Обучение сотрудников и повышение их осведомленности.	- Проведение регулярных тренингов по кибербезопасности для всех сотрудников банка для повышения их осведомленности о методах социальной инженерии, фишинге и других типах кибератак.
6.Инцидентное реагирование и восстановление после сбоя.	- Разработка и регулярное тестирование планов реагирования на инциденты, чтобы обеспечить быстрое восстановление после кибератак. -Постоянный мониторинг и анализ информации о киберугрозах для быстрого реагирования на новые угрозы и атаки.
7.Сотрудничество и обмен информацией.	- Участие в национальных и международных программах по обмену информацией о киберугрозах для получения актуальных данных о новых видах атак и методах их нейтрализации. - Сотрудничество с правоохранительными органами и другими финансовыми учреждениями для обмена опытом и координации действий по борьбе с киберпреступностью.

Заключение.

Таким образом, тема кибермошенничества в банковской сфере особенно актуальна сегодня по многим причинам, основные из которых связаны с технологическим развитием, увеличением числа онлайн-транзакций, постоянной модификацией и совершенствованием кибератак. Кибермошенничество наносит ущерб не только отдельным клиентам, но и банкам в целом, подрывая доверие общественности к финансовым учреждениям. Отмечается, что с развитием технологий и переходом банков к предоставлению услуг через интернет, включая мобильный и онлайн-банкинг, количество точек взаимодействия с клиентами увеличилось, что хоть и облегчило жизнь пользователей, но также повысило риск совершения кибератак. Кроме того, киберпреступники могут действовать из любой точки мира, что не только осложняет реагирование правоохранительных органов, но и создает общемировую угрозу.

История развития кибермошенничества в банковской сфере свидетельствует о постоянной эволюции методов и технологий, используемых мошенниками, с развитием цифровизации банковских услуг, мошенники адаптировались и стали использовать все более изощренные методы киберпреступлений.

Зависимость киберпреступлений от экономической ситуации в стране подчеркивает важность кибербезопасности и необходимость адаптации к новым вызовам и угрозам в киберпространстве.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Литература:

1. Сабельникова Г.С. Киберпреступность в банковской сфере. Тенденции и особенности расследования [Электронный ресурс] // Современная наука. 2020. – №1.

2. Противодействие мошенническим практикам [Электронный ресурс] // Официальный сайт Банка России. – Режим доступа: https://www.cbr.ru/information_security/pmp/?CF.Search=&CF.Date.Time=Custom&CF.Date.DateFrom=01.2019&CF.Date.DateTo=01.2024. – Загл. с экрана.

3. Кибермошенничество: портрет пострадавшего [Электронный ресурс] // Официальный сайт Банка России. – Режим доступа: https://cbr.ru/statistics/information_security/cyber_portrait//. – Загл. с экрана.

4. Шкодинский, С.В. Цифровая трансформация банковских бизнес-моделей и проблемы обеспечения кибербезопасности [Электронный ресурс] / С.В. Шкодинский, Ю.А. Крупнов, О.М. Толмачев // Вестник евразийской науки. – 2023. – Т. 15. – № 3.

5. Токарев, В.С. Факторы, влияющие на цифровизацию банковской деятельности, и их особенности / В.С. Токарев // Известия Санкт- Петербургского государственного экономического университета. – 2021 - №1. – С. 185-190.

References:

1. Sabelnikova G.S. Cybercrime in the banking sector. Trends and features of the investigation [Electronic resource] // Modern science. 2020. – No.1.

2. Countering fraudulent practices [Electronic resource] // Official website of the Bank of Russia. – Access mode: https://www.cbr.ru/information_security/pmp/?CF.Search=&CF.Date.Time=Custom&CF.Date .DateFrom=01.2019&CF.Date.DateTo=01.2024. – Blank

3. Cyberbullying: portrait of the victim [Electronic resource] // Official website of the Bank of Russia. – Access mode: https://cbr.ru/statistics/information_security/cyber_portrait //. – Cover from the screen.

4. Shkodinsky, S.V. Digital transformation of banking business models and problems of cybersecurity [Electronic resource] / S.V. Shkodinsky, Yu.A. Krupnov, O.M. Tolmachev // Bulletin of Eurasian Science. – 2023. – vol. 15. – No. 3.from the screen.

5. Tokarev, V.S. Factors influencing the digitalization of banking activities and their features / V.S. Tokarev // Izvestiya St. Petersburg State University of Economics. – 2021 - No. 1. – pp. 185-190.

Информация об авторе:

Долотова Наталия Павловна, кандидат экономических наук, доцент кафедры «Экономика» Федерального государственного бюджетного образовательного учреждения высшего образования «Тамбовский государственный технический университет", nazarchuk.natali@mail.ru

Natalia P. Dolotova, PhD in Economics, Associate Professor of the Department of Economics of the Federal State Budgetary Educational Institution of Higher Education «Tambov State Technical University».