ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

1. Forbes Kazakhstan // Объём безналичных транзакций в Казахстане превысил показатель ВВП // https://forbes.kz/economy/exchange/obyem_tranzaktsiy_v_kazahstane_prevyisil_pokazatel_vvp/
2. DKNWORLDNEWS // Как обеспечивается кибербезопасность в банковском секторе Казахстана? // https://dknews.kz/ru/finansy/260462-kak-obespechivaetsya-kiberbezopasnost-v-bankovskom
3. Национальный банк Республики Казахстан // Вопросы дальнейшей цифровизации финансовой инфраструктуры обсудили участники финрынка Казахстана // https://nationalbank.kz/ru/news/informacionnye-soobshcheniya/16350
4. DKNWORLDNEWS // Казахстан запускает Open API и Open Banking: новая эра в финансовой индустрии // https://dknews.kz/ru/finansy/313915-kazahstan-zapuskaet-open-api-i-open-banking-novaya

МЕЖДУНАРОДНАЯ БОРЬБА С КИБЕРМОШЕННИЧЕСТВОМ В БАНКОВСКОМ СЕКТОРЕ

Нурбекова Инкар Нуржановна
inkaran@bk.ru
Студентка ОП Финансы, Евразийский национальный университет им. Л.Н. Гумилева
Астана, Казахстан
Научный руководитель- к.э.н., профессор Жоламанова М.Т.

Кибермошенничество является серьезной проблемой в международном банковском секторе, представляющей серьезную угрозу для финансовых учреждений и их клиентов. Финансовые потери от мошенничества высоки: только в 2021 году общие убытки составили 5,8 млрд долларов США, а на каждый доллар, потерянный в результате мошенничества, банки несут расходы в размере 4 долларов США [1].

Мошенничество является постоянной проблемой, которая может нанести ущерб репутации банка, и мошенники продолжают находить новые и творческие способы обворовать банки и их клиентов. Кроме того, меняющаяся глобальная банковская среда с увеличением объемов цифровых платежей и сокращением филиальной сети создает новые проблемы в борьбе с кибермошенничеством. Обеспокоенность риском кибербезопасности возросла по сравнению с предыдущим годом: более 80% банкиров оценили риск кибербезопасности как «чрезвычайно важный». Риск кибербезопасности является основным внутренним риском в финансовом секторе, и руководители ИТ и безопасности должны принять меры для решения проблем кибербезопасности. Наиболее серьезной проблемой риска мошенничества в международном банковском секторе являются кибератаки, при этом передовые технологии необходимы для борьбы с киберпреступниками и должны быть частью первой линии защиты. Однако киберпреступники представляют собой серьезную проблему в борьбе с мошенничеством в международном банковском секторе, используя те же векторы атак, что и менее способные субъекты угроз, такие как фишинг и программы-вымогатели, но обладающие большими техническими возможностями и финансированием. Помимо кибератак, отмывание денег также представляет значительный риск, который может поставить под угрозу целостность рынка финансовых услуг в международном банковском секторе, поскольку банки, уличенные в отмывании денег, сталкиваются с юридическими и нормативными санкциями, а также репутационным ущербом и потерей репутации. Для борьбы с этими рисками банкам необходимо усовершенствовать свои стратегии обнаружения и предотвращения финансового мошенничества для борьбы с мошенничеством в цифровых пространствах. Глобальное исследование банковского мошенничества направлено на получение всестороннего представления на то, как банки структурируют свои команды и используют ресурсы для оптимизации своих усилий по управлению рисками мошенничества [2].

Борьба с кибермошенничеством в банковском секторе является непрерывным и многоструктурным процессом, который в зависимости от степени развития цифровизации в стране, имеет стратегии и методы по снижению мошенничества. Для подробного рассмотрения разнообразий используемых стратегии и методов снижению мошенничества, мы изучили опыт США и Россия, которые имеют практику управления кибермошенничеством.

Банковский сектор США в настоящее время сталкивается с множеством тенденций кибермошенничества, при этом основной проблемой является мошенничество с поддельными банковскими веб-сайтами [3]. Киберпреступность и кража денег по телефону также вызывают растущую обеспокоенность в банковской сфере, причем масштабы киберпреступности достигают таких масштабов, что ее можно рассматривать как угрозу национальной безопасности. К сожалению, только 25% случаев кибермошенничества в банковском секторе США раскрываются, что подчеркивает необходимость принятия более эффективных мер для решения этой проблемы. Законодательство в этой сфере не успевает за новыми угрозами в сфере высоких технологий и схемами хищения денег, что делает отрасль уязвимой для атак.

Сложность проблемы усугубляется тем, что злоумышленники действуют превентивно и на несколько шагов опережают тех, кто им противостоит. Чтобы избежать обнаружения, мошенники теперь используют другие каналы, такие как мессенджеры, для рассылки сообщений с призывом проголосовать за кого-то в конкурсе красоты или создают фейковые объявления о продаже товаров на сайтах объявлений. Кроме того, продажа поддельных товаров на сайтах объявлений стала популярной схемой обмана в банковском секторе США. Интересно, что методы фишинга стали менее эффективными, поскольку у людей выработался иммунитет к подозрительным электронным письмам; следовательно, мошенники сейчас изучают альтернативы фишингу. Банковскому сектору США необходимо больше инвестировать в меры кибербезопасности, чтобы противостоять этим новым тенденциям и защитить клиентов от финансового ущерба.

Банковский сектор США сталкивается с целым рядом киберугроз, и власти приняли ряд мер регулирования для противодействия этим преступлениям. Правительство создало различные центры, такие как FinCERT, для мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере. Кроме того, созданы специальные подразделения по расследованию преступлений, связанных с высокими технологиями. Однако противодействие киберпреступности требует многогранного подхода, включающего конкретные методические разработки и устойчивые решения. В одном исследовании освещаются проблемы и угрозы, которые цифровая экономика создает для устойчивости национальной банковской системы, и подчеркивается необходимость конкретной методической разработки по борьбе с кибермошенничеством в банковском секторе. Также стоит отметить, что США находятся в авангарде создания кибероружия высокого уровня, такого как Stuxnet, а это означает, что банки страны потенциально уязвимы для подобных атак. Фактически, некоторые сообщения предполагают, что банки США уже стали объектами атак киберпреступников. Таким образом, крайне важно иметь нормативные меры для выявления и противодействия кибермошенничеству в банковском секторе [4]. Кроме того, крайне важно защитить граждан, которые зачастую являются основными жертвами этих преступлений и наименее защищены от воздействия мошенников.

Говоря об опыте в России в последние годы кибермошенничество, стало серьезной проблемой для российского банковского сектора. В результате банки начали применять новые подходы к борьбе с социальной инженерией, а операторы связи делятся опытом борьбы с телефонным мошенничеством в банковском секторе. Обсуждаются законодательные инициативы по борьбе с кибермошенничеством, такие как введение новой процедуры возврата украденных средств и периода обдумывания для клиентов, подвергшихся атаке. Максимальная сумма украденного за один раз достигала 500 млн рублей, а 83% граждан России хотя бы раз сталкивались с попытками кибермошенничества [5].

Клиенты банков являются основными жертвами кибермошенничества в российском банковском секторе, причем телефонное мошенничество является особенно распространенной

формой атак. В 2022 году объем денежных потерь граждан России от телефонного мошенничества составил 14,2 млрд рублей . Для противодействия этой мошеннической деятельности банки принимают различные меры, такие как внедрение нового метода подтверждения транзакций, внедрение систем антифрод-мониторинга, отключение ДБО за дропы. Кроме того, операторы мобильной связи обмениваются информацией о физических лицах, которые предоставляют мошенникам доступ к услугам оператора для звонков граждан, внесены изменения в закон «О национальной платежной системе». Кибермошенничество в российском банковском секторе становится все более частым: в 90% случаев злоумышленники нацелены на кредитные средства. Мошеннические звонки через мессенджеры также являются проблемой, несмотря на снижение с начала года. Целевые атаки мошенников могут длиться более месяца, также существует проблема подмены номеров нумерации небольших операторов мобильной связи [6]. Крупнейшие российские банки создают единую для всего рынка систему антифрод-мониторинга, а единый онлайн-ресурс будет автоматически отслеживать подозрительные звонки и транзакции и предупреждать о них.

Российский банковский сектор предпринял значительные шаги для решения проблемы кибермошенничества и повышения своей информационной безопасности. В свете растущего числа киберугроз банки были вынуждены разрабатывать новые стратегии обнаружения и предотвращения мошеннических действий. Одним из способов реагирования сектора является переход на внутренние модули безопасности для ИТ-систем, как указано в политике Центрального банка в отношении защиты информации и кибербезопасности [7].

Регулятор также намерен стимулировать банки к усилению защиты клиентов от вымогательства со стороны мошенников, учитывая, что ущерб от кибермошенников может быть значительным. Эксперты положительно оценили законодательные меры, принятые для борьбы с кибермошенничеством, в том числе недавние поправки к закону «О национальной платежной системе», которые направлены на повышение безопасности и снижение риска мошеннической деятельности. Кроме того, в статье, посвященной проблеме кибермошенничества в банковском секторе, освещаются эффективные способы выявления и борьбы с этими преступлениями, подчеркивается необходимость большего внимания к уязвимостям информационной инфраструктуры и превентивных мер по предотвращению кибератак.

Рост кибермошенничества в России побудил власти создать несколько центров по борьбе с ним. Например, в составе ведомства созданы дополнительные специальные подразделения по выявлению и расследованию преступлений, связанных с высокими технологиями. За борьбу с киберпреступностью отвечает Управление «К» МВД. Кроме того, правительство России создало две системы обнаружения, предотвращения и ликвидации последствий компьютерных атак на российские информационные ресурсы. Первая — ГосСОПКА — Государственная система обнаружения, предотвращения и ликвидации последствий компьютерных атак на российские информационные ресурсы. Второй — FinCERT — Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере [4].

Хотя в тексте не содержится никакой информации о технологических решениях для обнаружения и предотвращения кибермошенничества, эти центры можно считать самостоятельными технологическими решениями. Они представляют собой согласованные усилия по предотвращению кибермошенничества за счет использования технологий и специализированного персонала.

В свете этих событий становится ясно, что российский банковский сектор серьезно относится к предотвращению кибермошенничества и внедряет лучшие практики для защиты своих клиентов и учреждений. Исходя из международного опыта в борьбе с кибермошенничеством в банковском секторе, можно выявить основные рекомендации для предотвращения кибермошенничества в Казахстане.

1. Государственным органам и юридическим лицам, осуществляющим масштабную работу с персональными данными необходимо:

- Усилить контроль за безопасным использованием корпоративных локальных сетей и беспроводной связи.
- Усилить контроль по установке обязательных необходимых антивирусных программ, а также внедрить четкую систему отслеживания установки протоколов защиты на официальных сайтах организаций. Для этого ввести правовое регулирование и обозначить ответственность за нарушение или просрочку установки необходимых программ для сохранения безопасности.

2. Для банков:

- Инвестировать в передовые технологии безопасности: использовать системы аутентификации нового поколения, такие как биометрия, многофакторная аутентификация (MFA) и анализ поведения пользователя.
- Проводить регулярные тренинги для сотрудников по вопросам кибербезопасности: обучать сотрудников тому, как распознавать и реагировать на попытки кибермошенничества. [8]

Таким образом, международный опыт в борьбе с кибермошенничеством в банковском секторе показывает, что эта проблема требует комплексного подхода и постоянного обновления мер безопасности. Страны и банки активно обмениваются информацией о методах атак и совершенствуют свои системы защиты. Однако, угроза кибермошенничества по-прежнему остается высокой, и требует дальнейшего совершенствования международного сотрудничества, разработки новых технологий и повышения осведомленности общественности о методах защиты от киберугроз.

Список использованных источников:

1. Landy Wingard, Fraud Management in Banking: Detection, Prevention & More. global.hitachi-solutions.com/blog/fraud-prevention-in-banks/
2. KPMG Global, Global Banking Fraud Survey kpmg.com
3. Picus, Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022. www.picussecurity.com
4. Kurmanova L, Galimova G, Development of Digital Services and Information Security of Banks https://dl.acm.org/doi/abs/10.1145/3487757.3490911
5. Ассоциация банков России, Способы борьбы с кибермошенничеством https://asros.ru/news/asros/v-assotsiatsii-bankov-rossii-obsudili-sposoby-borby-s-kibermoshennichestvom/
6. Дементьева М.А.1, Лихачева В.В.1, Козырев Т.Г., Киберпреступления в банковской сфере Российской Федерации: способы выявления и противодействия https://elibrary.ru/download/elibrary_39191641_34198434.pdf
7. Тумеркин И.Ш., Кибератаки в банковском секторе - подход к обеспечению безопасности ит-инфраструктур коммерческих банков https://cyberleninka.ru/article/n/kiberataki-v-bankovskom-sektore-podhod-k-obespecheniyu-bezopasnosti-it-infrastruktur-kommercheskih-bankov
8. Серік Айнұр, Правовые основы предотвращения кибермошенничества: состояние и перспективы развития

УДК 330.442.001.36

ЦИФРОВИЗАЦИЯ КАК СРЕДСТВО РАЗВИТИЯ БИЗНЕСА В РЕСПУБЛИКИ КАЗАХСТАН

Нұрмаш Жастілек Русланұлы, Рахатов Нурбол
zastilek33@gmail.com
студент Университета Туран Астана, г. Астана, Республика Казахстан
Научный руководитель – Рахметалиева С.А.