

**Х.У.Рахимова,**  
доцент Банковско-финансовой академии

**Ш.Р.Тохирхужаев,**  
магистрант Банковско-финансовой академии

**З.О.Омонов,**  
магистрант Банковско-финансовой академии

## **ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ И ПРЕСЕЧЕНИЕ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ В БАНКОВСКОЙ СФЕРЕ**

**Аннотация.** В данной статье затронуты основные аспекты защиты информации в банковской сфере, а также особенности организации политики Центрального банка в данной области. Дана оценка современной системе защиты информации в банковской сфере. Особое внимание уделено инструментам, способам и механизмам защиты информации в банковском секторе. Кроме того, рассмотрены вопросы повышения эффективности политики Центрального банка в области защиты информации и пресечения мошеннических операций в банковском секторе.

**Ключевые слова:** киберугрозы, кибербезопасность, информационная безопасность, политика информационной безопасности, риск банковского сектора, киберустойчивость.

**Annotation.** This article touches upon the main aspects of information security in the banking sector, as well as the specifics of organizing the Central Bank's policy in this area. The assessment of the modern information security system in the banking sector is given. Particular attention is paid to tools, methods and mechanisms for protecting information in the banking sector. In addition, issues of increasing the efficiency of the Central Bank's policy in the field of information protection and suppression of fraudulent transactions in the banking sector were considered.

**Key words:** cyber threats, cyber security, information security, information security policy, banking sector risk, cyber resilience.

**Аннотация.** Ушбу мақолада банк секторида ахборот хавфсизлигини таъминлашнинг асосий жиҳатлари, шунингдек, Марказий банкнинг ушбу соҳадаги сиёсатини ташкил этишнинг ўзига хос томонлари кўриб чиқилди. Банк соҳасида замонавий ахборот хавфсизлик тизими баҳо берилган. Банк соҳасида ахборотни ҳимоя қилиш воситалари, усуллари ва механизмларига алоҳида эътибор қаратилмоқда. Бундан ташқари, Марказий банкнинг ахборотни ҳимоя қилиш ва банк соҳасида фирибгарлик операцияларига чек қўйиш соҳасидаги сиёсати самарадорлигини ошириш масалалари кўриб чиқилган.

**Калит сўзлар:** кибертаҳдидлар, киберхавфсизлик, ахборот хавфсизлиги, ахборот хавфсизлиги сиёсати, банк сектори хавфи, кибер барқарорлик.

Сегодня мир стремится приобрести цифровой облик, но вместе с этим в этом мире вопрос информационной безопасности набирает новые обороты и занимает центральное место в социально-экономической жизни общества.

Совершенствование экономической индустрии, широкое использование разнообразных информационных технологий ведёт к распространению компьютерных и коммуникационных сетей, а это в свою очередь, создаёт условия для несанкционированного проникновения в них. Проблема преступности в информационной сфере в разы превышает другие виды преступности и, вопрос совершенствования борьбы с данным видом преступлений во всех странах мира вызывает необходимость уделения большего внимания и сил общественности, а также ресурсов. Информационная безопасность – это обеспечение сохранности ценных данных и информации, защита информации от несанкционированного использования и корректировок, сохранение информационной тайны и надёжность технической работы компьютеров и компьютерных сетей.

Как объект особого внимания в сфере информационной безопасности информационная база банковской системы стоит на особом учёте, т.к. это сфера больше других сфер подвергается мошенническим и хакерским операциям.

Сегодня в результате проведения цифровых трансформаций в банковском деле появляются новые, удобные банковские продукты для клиентов, в частности доступ к виртуальным помощникам и чат-ботам, расширения безналичных расчётов по пластиковым картам, расширения систем бесконтактных платежей, интегрированные выписки для клиентов по имеющим счетам нескольких банков, пользование услугами искусственного интеллекта с использованием биометрических параметров клиентов. Но следует отметить, что с появлением новых видов услуг и обеспечением максимальных удобств для потребителей платёжных услуг появляются новые виды мошеннических операций, увеличивается их объём. В частности, расширение дистанционного банковского обслуживания, увеличение объёма рынка бесконтактных платежей, использование в обороте цифровых валют, P2P сервисов и развитие электронной коммерции растёт мошеннические операции, что по оценкам зарубежных экспертов, ежегодные финансовые потери от этих операциях составляют многие миллиарды долларов. В странах с развитой информационной технологией эта проблема носит достаточно острый характер, и вопрос обеспечения информационной безопасности превращается в злободневную задачу соответствующих структур, государства и общества.

Информационная преступность это противоправные действия в информационной сфере, нарушающие установленные законом права личности, организации и государства и, наносящие им моральный вред и материальный ущерб.<sup>1</sup>

В обеспечении информационной безопасности банковской сферы большая роль принадлежит Центральному банку страны, он соответствующими

---

<sup>1</sup> [https://dic.academic.ru/dic.nsf/fin\\_enc/23429](https://dic.academic.ru/dic.nsf/fin_enc/23429)

техническими, юридическими инструментами и механизмами выполняет на него возложенную функцию.

Сегодня Центральный банк, как регулирующий орган банковской системы, разрабатывает политику и систему защиты банковской информации, которое в себя включает стратегию, нормативную базу (положения, стандарты, инструкции, правила, процедуры и ограничения) принятых как международными организациями, так и самим Центральным банком.

Политика Центрального банка в области обеспечения информационной безопасности кредитно-финансовой сфере должна опираться на совершенные методы, механизмы и инструменты. Под политикой дословно следует понимать совокупность механизмов и инструментов управленческих действий, направленных на обеспечение безопасности всех видов информационных систем в банке.

Важное место в политике обеспечения информационной безопасности банковской системы Центрального банка принадлежит нормативным документам, обеспечивающие правовое регулирование отношений в области проведения безопасных финансовых транзакций и операций.

Коммерческие банки, как важные элементы банковской системы обязаны реализовывать стратегию и руководствоваться принятыми документами для обеспечения безопасности информации банковской системы.

Политика Центрального банка в сфере обеспечения безопасности банковской информации должна включать следующие важные направления:

- развитие киберустойчивости кредитно-финансовой сферы страны;
- обеспечение эффективной системой мониторинга и контроля за показателями риска в финансовой системе;
- совершенствование системы реагирования и предотвращения компьютерных атак на объекты и субъекты финансово-кредитной системы;
- защита прав потребителей финансовых услуг и обеспечение их защиты от кибермошеннических атак;
- обеспечение инновационными технологиями в части контроля показателей риска реализации информационных угроз и обеспечение необходимого уровня информационной безопасности.

Надо признать тот факт, что правовые инструменты Центрального банка по обеспечению информационной безопасности вносят существенный вклад в систему защиты информации в банковской сфере, но вместе с ними, большое внимание заслуживают организационно-технические инструменты, которые присутствуют в банковских системах при организации проведения банковских операций или транзакций. К ним следует отнести инструменты системы идентификации, аутентификации и верификации, внутрисистемные защитные программы, системы мониторинга за безопасностью банковской деятельности и другие.

Важная роль в системе защиты информации в Республике Узбекистан принадлежит государственной унитарной предприятии (ГУП) «Центр кибербезопасности». На данный центр возложен ряд задач по обеспечению

защиты от возможных кибератак и стабильного функционирования объектов информатизации страны.

На регулярной основе центр проводит мониторинг всех событий и инцидентов информационного пространства Узбекистана и разрабатывает меры по кибербезопасности. Кроме того, центр недавно провел исследование по рейтинговой оценке состояния обеспечения информационной и кибербезопасности в органах государственного и хозяйственного управления, органах государственной власти на местах по итогам 3 квартала 2021 года. По итогам оценки были определены топ 10 организаций с высоким рейтингом и очень отраднo, что данный список лидирует Центральный банк Республики Узбекистан, с показателем рейтинга 96,9 баллов из 100<sup>2</sup>.

Несмотря на то, что со стороны Центрального банка в банковской системе создаются эффективные нормативно–технологические стандарты защиты информации, немаловажным остаётся фактор повышения цифровой и финансовой грамотности населения Узбекистана. Значимость данного фактора можно судить по тому, как этот фактор может существенно влиять на доверие к платёжным системам, торговым сайтам и вообще к дистанционным и цифровым финансовым услугам. При учащении мошеннических операций, пользователи финансовых услуг будут относиться с недоверием к платёжным системам, из-за обмана или заблуждения их мошенниками.

Результаты проведённых исследований в области информационной безопасности финансовых транзакций населения показывает, что имеются существенные моральные и финансовые ущербы от мошеннических операций. В частности, результаты анализа информационной безопасности по карточным платёжным системам расчёта, показывает, что в день мошенники только с сайта Olx.uz путём завладения СМС кода или Фишинговых сайтов крадут из счёта от 30-35 млн сум<sup>3</sup>. По оценке экспертов, специалистов количество мошеннических преступлений в Узбекистане увеличились в разы и это набирает новые обороты.

На сегодня часто встречающимися видами мошеннических операций выступают фишинг, СМС или звонки мошенников, кража личных данных.

Что такое фишинг? Фишинг - вид мошенничества через интернет. При этом виде мошенничества мошенники создают клонированные сайты банковских или платёжных компаний и через них получают данные карты. Хозяева карт пытаются купить товары или услуги через клонированный сайт, их приманивают мошенники через фиктивные объявления на акции или скидки на товары или услуги, жертвы нажимая на объявления переходят на клонированный сайт торгового агента и вводят свои карточные данные собственноручно.

При случае использования мошенниками СМС или звонков, мошенники представляются сотрудниками банка и войдя в доверия жертв получают их

---

<sup>2</sup> <https://csec.uz/uz/news/mahalliy-yangiliklar/top10-3chorak-2021-rating/>

<sup>3</sup> <https://kun.uz/ru/news/2020/11/01/voruyut-do-35-millionov-sumov-v-den-v-uzbekistane-poyavilis-novyey-vidy-moshennichestva>

данные, а затем мошенники используют данные для перевода, для оплаты или для получения онлайн кредита.

Кража личных данных сопровождается несанкционированным доступом к информационным базам жертв, к личным перепискам, а также при овладении данными карт в физическом виде (запоминания или копирование мошенниками номеров карт, их срока действия, CVV кода и других данных)

Согласно данным, предоставленным главным управлением уголовного розыска МВД за период 2020 года число таких преступлений по статье мошенничество составило 3881шт. Как отмечается экспертами, причиной столь бурного роста мошенничества в сфере интернет банкинга является низкая финансовая грамотность населения и не совершенная система защиты от мошенничества онлайн транзакций<sup>4</sup>.

Для повышения безопасности и обеспечения возможности расширения дистанционных банковских услуг в сферу банковского бизнеса активно внедряют такие физические показатели клиента, как отпечатки пальцев, голос, лицо, сетчатка глаз и другие). Всё это служит одним из современных механизмов и способов защиты банковской информации, информации о клиентах, о транзакциях, о финансовых ресурсах и другое.

Но несмотря на эти способы защиты информации, на сегодня актуальной задачей остаётся определение Интернет сайтов, служащие для проведения мошеннических операций в кредитно-финансовой сфере и своевременный запрет к ним потребителей финансовых услуг. Это требует закрепления за Центральным банком юридических полномочий по блокированию интернет сайтов, в частности, фишинговых сайтов, незаконно открытых сайтов, предоставляющие финансовые услуги, сайтов, используемых для распространения информации о финансовых пирамидах, привлекающих средства и имущество физических и юридических лиц, сайтов, связанных с экспансией вредных компьютерных программ.

Многие страны в своих концепциях развития финансовой сферы, с позиции безопасности предусмотрели введение и использование блокчейн технологий для осуществления финансово-транзакционных операций. Блокчейн технологии со стороны экспертов были оценены, как достаточно безопасная и прогрессивная технология.

Кроме того, в политике Центрального банка по обеспечению информационной безопасности в банковской сфере занимает мероприятия по созданию эффективной системы мониторинга за степенью риска информационных угроз и обеспечение надлежащего уровня информационной безопасности.

Как показывает международная практика для повышения эффективности деятельности Центрального банка в этом направлении необходимо проводить следующие важные работы:

---

<sup>4</sup> <https://kun.uz/ru/news/2020/11/01/voruyut-do-35-millionov-sumov-v-den-v-uzbekistane-poyavilis-novyve-vidy-moshennichstva>

-мониторинг и контроль за уровнем киберриска в финансовых организациях и субъектах платежных систем;

-развитие культуры использования информационных ресурсов и соблюдение киберсанитарии в кредитно-финансовой сфере;

-повышения надзора за информационной безопасностью при использовании инновационных технологий;

-развитие международного сотрудничества в области защиты информации в деятельности платёжных систем и предотвращения мошеннических операций.

-совершенствовать систему защиты через мобильные приложения и установления лимитов по операциям.

Вместе с этим важно создание реестра платёжных инструментов мошенников, которыми пользуются для вывода средств для дальнейшей блокировки. Расширение внедрения технологий 3D secure для осуществления онлайн операций, обеспечение мониторинга за конкретными платёжными инструментами, привязанных к единому владельцу/пользователю.

Делая заключение по данной статье, следует отметить следующие важные моменты:

- банковская система является высоко рискованной сферой и в связи с этим она нуждается в высокой защите информации;

-политика Центрального банка в области информационной защиты должна находиться в постоянном совершенствовании;

- информационная безопасность в платёжных системах должна в себя включать современные инструменты, способы и механизмы защиты информации;

- важно развитие цифровой и финансовой грамотности населения;

-совершенствование системы защиты информации за счёт эффективного международного сотрудничества по пресечению мошеннических операций в платёжных системах.

## **СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ**

1. Безопасность банковской деятельности: учебник для вузов / В. А. Гамза, И. Б. Ткачук, И. М. Жилкин. — 3-е изд., перераб. и доп. — М. : Издательство Юрайт, 2015. – 513 с.

2. Глобальные исследования по вопросам мошенничества. Издательство КППМГ налоги и консультирования. 2019 -28стр.

3. Воронцова С. В. Преступления в сфере электронных расчетов и платежей. Правовые и организационно-тактические основы противодействия. – М.: Юркомпани, 2015. – 336 с

4. Семеко Г.В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия

5. <http://www.cbu.uz/>

6. <https://tace.uz/company/>