ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-10

КИБЕР УГРОЗЫ И БЕЗОПАСНОСТЬ ДАННЫХ В КОММЕРЧЕСКИХ БАНКАХ УЗБЕКИСТАНА.

Ибодуллаев Сардорбек Лазиз угли
sardorbekibodullayev3@gmail.com
Ташкентский Международный университет Химии

Аннотация: В современную эпоху цифровизации банковской системы обеспечение кибербезопасности становится одной из ключевых задач коммерческих банков Узбекистана. С ростом использования электронных платежных систем, интернет-банкинга и мобильных приложений увеличивается риск кибератак, направленных на кражу конфиденциальных данных клиентов и финансовых средств. В статье рассматриваются основные виды киберугроз, с которыми сталкиваются банки, включая фишинг, вредоносное программное обеспечение, DDoS-атаки и внутренние угрозы. Анализируются современные методы защиты информации, используемые коммерческими банками, а также роль государственных регуляторов и нормативных актов в обеспечении цифровой безопасности. Особое внимание уделено необходимости создания комплексной системы киберзащиты, повышения уровня цифровой грамотности сотрудников и внедрения инновационных технологий для минимизации рисков.

Ключевые слова: кибербезопасность, коммерческие банки, киберугрозы, защита данных, информационная безопасность, Узбекистан, цифровизация, интернет-банкинг, фишинг, DDoS-атаки.

Введение

В условиях стремительного развития цифровых технологий банковская сфера Узбекистана переживает глубокую трансформацию. Коммерческие банки активно внедряют инновационные решения, такие как интернет- и мобильный банкинг, автоматизированные платежные системы, дистанционное обслуживание клиентов и цифровые платформы. Эти изменения способствуют повышению эффективности банковских услуг и улучшению качества обслуживания клиентов. Однако вместе с цифровизацией банковской системы значительно возрастает и уровень киберугроз, направленных на получение несанкционированного доступа к финансовым и персональным данным клиентов. Киберпреступления в финансовой сфере становятся всё более изощрёнными, а их последствия могут привести не только к крупным финансовым потерям, но и к утрате доверия клиентов, что особенно опасно для коммерческих банков, работающих в конкурентной среде. В этой связи проблема обеспечения информационной и кибербезопасности приобретает стратегическое значение для устойчивого развития банковского сектора Узбекистана.

В последние годы в стране предпринимаются меры по совершенствованию правовой базы в области кибербезопасности, развитию национальной инфраструктуры защиты данных и повышению цифровой грамотности специалистов финансового сектора. Тем не менее, анализ показывает, что многие банки всё ещё сталкиваются с трудностями в реализации комплексных систем защиты информации и предотвращении современных кибератак. Целью данного исследования является анализ основных видов киберугроз, с которыми сталкиваются коммерческие банки Узбекистана, а также рассмотрение существующих методов и

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

инструментов обеспечения безопасности данных. На основе анализа предлагаются направления совершенствования системы киберзащиты в банковском секторе страны.

Методы и материалы исследования

В процессе исследования использованы аналитические, сравнительные и системные методы изучения проблем кибербезопасности в банковской системе Узбекистана. Основное внимание уделено анализу нормативно-правовых документов Республики Узбекистан, регулирующих вопросы информационной безопасности и защиты персональных данных, таких как Закон «О персональных данных», а также государственные программы по цифровизации финансового сектора. Материалы исследования включают данные Центрального банка Республики Узбекистан, отчёты коммерческих банков о внедрении систем информационной защиты, публикации в научных журналах и материалы международных организаций, занимающихся вопросами кибербезопасности. На основе этих источников проведён сравнительный анализ состояния киберзащиты в отечественных банках и мировых тенденций в области цифровой безопасности.

Для оценки эффективности существующих механизмов защиты информации применялись методы контент-анализа и экспертных оценок. Также использовались статистические данные о зарегистрированных киберинцидентах в финансовой сфере, позволяющие выявить наиболее уязвимые направления деятельности коммерческих банков. Результаты исследования основаны на обобщении практического опыта банковской системы Узбекистана, а также на анализе международных стандартов безопасности, таких как ISO/IEC 27001, что позволило определить актуальные направления совершенствования киберзащиты в финансовом секторе страны.

Результаты и обсуждение

Проведённый анализ показал, что коммерческие банки Узбекистана в последние годы активно развивают цифровые услуги, что, в свою очередь, повышает риски возникновения киберинцидентов. Среди наиболее распространённых угроз, с которыми сталкиваются банки, можно выделить фишинг, внедрение вредоносных программ, несанкционированный доступ к банковским системам, DDoS-атаки и внутренние угрозы со стороны сотрудников.

1. Фишинг и социальная инженерия. Этот вид киберугроз остаётся самым распространённым в банковском секторе. Мошенники используют поддельные сайты и электронные письма, имитирующие интерфейсы банков, чтобы получить личные данные клиентов. Несмотря на развитие систем двухфакторной аутентификации, многие пользователи становятся жертвами из-за недостаточной цифровой грамотности.

2. Вредоносное программное обеспечение. Банковские системы часто подвергаются атакам с использованием вирусов, троянов и шпионских программ, целью которых является кража паролей и финансовых данных. В 2023–2024 годах специалисты зафиксировали увеличение числа атак на мобильные приложения, что требует от банков постоянного обновления систем защиты.

3. DDoS-атаки и перегрузка серверов. Эти атаки направлены на вывод из строя интернет-сервисов банка и создают значительные проблемы для клиентов, особенно во время массовых платежей. Некоторые крупные банки страны уже внедрили системы фильтрации и распределения трафика, что позволяет минимизировать риск временной недоступности сервисов.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-10

4. Внутренние угрозы. Особое внимание заслуживает проблема несанкционированных действий сотрудников, имеющих доступ к конфиденциальной информации. В ряде случаев утечка данных происходила по вине персонала из-за отсутствия строгого контроля и обучения основам информационной безопасности.

Для противодействия этим угрозам коммерческие банки Узбекистана внедряют современные решения: системы мониторинга сетевого трафика, антивирусные комплексы, межсетевые экраны нового поколения, а также автоматизированные системы обнаружения вторжений. Кроме того, создаются внутренние службы кибербезопасности и проводится регулярное обучение сотрудников.

Таблица 1. Основные виды киберугроз в коммерческих банках Узбекистана и их последствия

№	Вид киберугрозы	Частота возникновения	Основные последствия	Методы защиты
1	Фишинг и социальная инженерия	Высокая	Кража данных клиентов	Двухфакторная аутентификация, фильтрация писем
2	Вредоносное ПО (вирусы, трояны)	Средняя	Потеря конфиденциальной информации	Антивирусные системы, регулярное обновление
3	DDoS-атаки	Средняя	Нарушение работы онлайн-сервисов	Системы фильтрации и защиты серверов
4	Внутренние угрозы	Низкая	Утечка данных изнутри организации	Контроль доступа, обучение персонала
5	Кража учётных данных	Высокая	Неавторизованные операции	Шифрование и мониторинг активности

Важно отметить, что Центральный банк Республики Узбекистан играет значительную роль в формировании единой политики кибербезопасности. Он издаёт нормативные документы, регулирующие защиту данных, и координирует деятельность коммерческих банков в области цифровой безопасности. Анализ международного опыта показал, что эффективная защита банковских данных возможна только при комплексном подходе, включающем технические, организационные и правовые меры. В этой связи необходимо совершенствовать законодательную базу, развивать национальные центры мониторинга киберинцидентов и активно внедрять международные стандарты информационной безопасности. Таким образом, результаты исследования свидетельствуют о том, что, несмотря на достигнутый прогресс, уровень защиты данных в коммерческих банках Узбекистана требует дальнейшего совершенствования и постоянного обновления технологий в соответствии с глобальными вызовами киберпространства.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-10

Заключение

В условиях активной цифровизации банковской системы Узбекистана обеспечение кибербезопасности становится неотъемлемой частью устойчивого развития финансового сектора. Проведённое исследование показало, что коммерческие банки сталкиваются с широким спектром киберугроз, включая фишинг, вредоносные программы, DDoS-атаки и внутренние утечки информации. Эти угрозы представляют серьёзную опасность не только для финансовой стабильности организаций, но и для доверия клиентов к банковской системе в целом. Результаты анализа подтверждают необходимость системного подхода к обеспечению защиты данных, который должен включать технические, организационные и нормативно-правовые меры. К числу наиболее эффективных направлений относятся: внедрение современных технологий шифрования и мониторинга сетей, развитие центров кибербезопасности, регулярное обучение сотрудников, а также укрепление сотрудничества между банками и государственными структурами.

Особое значение имеет повышение цифровой культуры пользователей и специалистов банковского сектора. Только комплексная работа по укреплению киберустойчивости позволит минимизировать риски и обеспечить надёжную защиту информации в условиях стремительного развития финансовых технологий. Таким образом, обеспечение кибербезопасности в коммерческих банках Узбекистана должно рассматриваться как стратегический приоритет, направленный на укрепление доверия клиентов, повышение конкурентоспособности и интеграцию национальной банковской системы в международное цифровое пространство.

Список литературы

1. Закон Республики Узбекистан «О персональных данных» — №ЗРУ-547 от 2 июля 2019 года.
2. Центральный банк Республики Узбекистан. Отчёт о состоянии и развитии банковского сектора за 2024 год. — Ташкент, 2025.
3. Постановление Президента Республики Узбекистан №ПП–3832 от 14 июля 2018 года «О мерах по развитию цифровой экономики и электронного правительства».
4. Cybersecurity in Banking and Financial Services. — International Monetary Fund Report, 2023.
5. Алимов Ш., Рахмонов Д. Информационная безопасность в финансовом секторе Узбекистана: проблемы и решения. — Журнал «Банк и Финансы», №2, 2024.
6. ISO/IEC 27001:2022 Information Security Management Systems. — International Organization for Standardization, Geneva, 2022.
7. Ахмедова М. Цифровая трансформация банков Узбекистана и проблемы кибербезопасности. — Ташкентский финансовый институт, Научные труды, 2024.