“MOLIYA, PUL VA KREDIT”
mahalliy va xalqaro miqyosidagi ilmiy-ommabop elektron jurnal
2025-yil, iyul-avgust. №6-son
www.info@mpkuz.uz
https://mpkjournal.com/index.php/MPK


# АНАЛИЗ РИСКОВ, СВЯЗАННЫХ С ЦИФРОВИЗАЦИЕЙ КАЗНАЧЕЙСКОЙ ДЕЯТЕЛЬНОСТИ

# G‘AZNACHILIK FAOLIYATINI RAQAMLASHTIRILISHI BILAN BOG‘LIQ RISKLAR TAHLILI

**[1]Сагдиев Равшан Сайфуллаевич**

*[1]PhD, Ташкентский государственный экономический университет, самостоятельный исследователь.* ***ORCID:*** *0009-0005-1716-3783*
***E-mail:*** *ravshanbek_0071@mali.ru*

**Аннотация Annotatsiya**

***Рус.*** - Цифровизация казначейской деятельности представляет собой важный шаг в модернизации государственного управления и финансовых процессов. Однако внедрение новых технологий сопряжено с рядом рисков и угроз, таких как кибератаки, утечка данных, технические сбои и правовые несоответствия. В рамках исследования рассмотрены основные угрозы, связанные с цифровизацией казначейства, а также предложены меры по их минимизации, включая усиление защиты данных, улучшение IT-инфраструктуры, соблюдение юридических стандартов и обучение персонала. Использованы методы системного анализа и сравнительного исследования зарубежного опыта для выработки рекомендаций по оптимизации казначейской системы.

***Uzb.*** - Ushbu maqolada g‘aznachilik faoliyatini raqamlashtirish jarayoni davlat boshqaruvi va moliyaviy jarayonlarni modernizatsiya qilishning muhim bosqichi sifatida yoritiladi. Biroq, yangi texnologiyalarning joriy etilishi kiberhujumlar, texnik nosozliklar hamda huquqiy nomuvofiqliklar kabi bir qator xavf va tahdidlar bilan bog‘liq. Tadqiqotda g‘aznachilikni raqamlashtirish bilan bog‘liq asosiy tahdidlar o‘rganilib, ularni minimallashtirish bo‘yicha chora-tadbirlar, jumladan, ma’lumotlar himoyasini kuchaytirish, IT-infratuzilmani takomillashtirish, qonunchilik standartlariga rioya etish va xodimlarni tayyorlash masalalari taklif etiladi.

**Ключевые слова: Kalit so‘zlar:**

❖ *цифровизация, казначейство, риски, киберугрозы, защита данных, IT-инфраструктура, юридическое соответствие, управление рисками.*

❖ *raqamlashtirish, xazina, xatarlar, kibertahdidlar, ma’lumotlarni himoya qilish, IT infratuzilmasi, qonuniy muvofiqlik, risklarni boshqarish.*

## Введение.

Цифровизация казначейской деятельности становится важнейшей частью трансформации финансовых процессов в организациях и государственных структурах по всему миру. Внедрение современных технологий позволяет существенно повысить эффективность управления денежными потоками, улучшить прозрачность финансовых операций и оптимизировать рабочие процессы. Автоматизация казначейских функций, таких как управление ликвидностью, мониторинг денежных потоков, обработка платежей и учет финансовых операций, открывает

новые возможности для повышения оперативности и снижения операционных затрат.

Однако, с развитием цифровых технологий возникают и новые риски, которые требуют внимательного подхода. Цифровизация делает системы казначейства более уязвимыми к внешним и внутренним угрозам, таким как кибератаки, сбои в системах, утечка данных и ошибки в автоматизированных процессах. Также важно учитывать юридические и регуляторные вызовы, которые возникают на фоне стремительных изменений в законодательных требованиях к цифровой безопасности и финансовым операциям.

В этой статье рассмотрим основные риски, связанные с цифровизацией казначейской деятельности, а также возможные способы их минимизации и управления для обеспечения безопасной и эффективной работы казначейских систем в условиях цифровой трансформации.

## Обзор использованной литературы.

Цифровизация казначейской деятельности привлекла внимание множества исследователей, так как она оказывает значительное влияние на эффективность управления финансовыми потоками и улучшение прозрачности. В то же время, внедрение цифровых технологий сопровождается рядом рисков, таких как киберугрозы, технические сбои, юридические проблемы и необходимость квалифицированного персонала для работы с новыми системами. В рамках этого обзора рассмотрены основные работы, посвящённые анализу рисков цифровизации казначейства, а также подходам к их минимизации и управлению. Эти исследования подчеркивают как преимущества, так и вызовы, с которыми сталкиваются организации в процессе цифровой трансформации.

Цифровизация казначейской деятельности и её риски стали предметом интенсивных исследований в последние десятилетия, особенно в контексте глобальных изменений в финансовом секторе. В ряде работ подчёркивается, что внедрение информационных технологий в управление финансовыми потоками способствует повышению эффективности и прозрачности, но в то же время увеличивает уязвимость систем от внешних угроз и ошибок в программном обеспечении [1].

Одним из важных направлений в этом контексте является исследование киберугроз и безопасности данных в цифровых казначействах. Например, в работе Джонсона и соавторов [2] рассматриваются конкретные случаи утечек данных и методы защиты от них, что подчеркивает важность обеспечения безопасности на всех уровнях цифровых финансовых систем.

Технические сбои и зависимость от внешних поставщиков также занимают значительное место в исследованиях. В частности, Смит [3] акцентирует внимание на важности резервирования и устойчивости IT-инфраструктуры для минимизации рисков сбоев в работе казначейства, которые могут привести к задержкам в обработке финансовых операций и потере данных. Это подчеркивает необходимость создания надежных систем и алгоритмов для защиты от возможных ошибок.

Кроме того, важным аспектом цифровизации является правовое регулирование. Фелпс [4] акцентирует внимание на юридических рисках, связанных с глобальными изменениями законодательства, которые касаются обработки персональных данных и финансовых операций в цифровых системах. Эти изменения требуют от организаций постоянного обновления их

практик и адаптации к новым нормативным требованиям.

Особое место в исследованиях занимает подготовка кадров для работы с цифровыми инструментами. В частности, работы Харриса и соавторов [5] показывают, что успешная цифровизация казначейства невозможна без достаточной подготовки специалистов, а использование новых технологий требует развития компетенций в области информационной безопасности и финансов, что способствует снижению человеческого фактора ошибок.

В работах российских авторов, таких как Иванова и Петрова [8], рассматриваются специфические риски цифровизации казначейства в условиях российской юридической и технической инфраструктуры. Исследования подчеркивают, что успешное внедрение технологий требует не только высоких технологических стандартов, но и умения адаптироваться к постоянно меняющимся регуляторным требованиям, что является актуальной задачей для российских организаций.

Кузнецов и Воронцов [9] в своих исследованиях выделяют проблемы интеграции цифровых платформ в казначейские системы стран СНГ и их воздействие на внутренние процессы управления финансами в государственных и частных структурах. В этом контексте они подчеркивают необходимость создания комплексных решений для оптимизации работы с цифровыми платформами в казначейской деятельности.

Несмотря на все риски, учёные сходятся во мнении, что преимущества цифровизации значительные, и решения по её внедрению должны быть комплексными. Работы Бенсона и Кларка [6], а также исследования Чанг и Тана [7] подчеркивают, что для успешной цифровизации необходимо проводить комплексное управление рисками, включая регулярные обновления программного обеспечения, мониторинг системы безопасности и создание эффективных систем защиты данных.

## Методология исследования.

В исследовании использовался логико-структурный анализ теоретических и эмпирических данных, а также методы системного анализа для выявления факторов, влияющих на риски цифровизации казначейской деятельности. Основной целью работы было изучение влияния цифровых технологий на казначейские процессы, выявление угроз (кибератаки, утечка данных, сбои) и предложение решений для их минимизации. Применялись методы анализа и синтеза для обобщения существующих подходов, выявления ключевых проблем и преимуществ цифровизации. Также был использован метод сравнительного анализа для выработки рекомендаций по оптимизации казначейской системы в условиях цифровизации.

## Анализ и обсуждение результатов.

Цифровизация казначейской деятельности приносит значительные преимущества, такие как повышение эффективности, прозрачности и быстроты обработки финансовых операций. Однако она также сопровождается рядом рисков и угроз, которые могут серьёзно повлиять на финансовую устойчивость и безопасность работы казначейства. Ниже представлена информация о ключевых рисках и статистических данных, которые иллюстрируют масштабы угроз, с которыми сталкиваются финансовые организации в процессе цифровизации.

Одним из самых серьёзных рисков является киберугрозы и безопасность данных. Внедрение цифровых технологий повышает уязвимость казначейских систем перед кибератаками и утечками данных.

Согласно данным IBM, средняя стоимость утечки данных в финансовом секторе составляет 5,72 миллиона долларов США. Кроме того, по информации Verizon, 80% инцидентов с утечками данных связаны с атаками на третьих лиц, что подчеркивает риски взаимодействия с внешними поставщиками и партнёрами. Ожидается, что к 2025 году мировые затраты на борьбу с киберугрозами могут достичь 1 триллиона долларов США [10], что ещё раз подтверждает важность кибербезопасности для всех отраслей, включая финансовый сектор.

Технические сбои и зависимость от внешних поставщиков также представляют собой значительную угрозу для цифровых казначейств. Внедрение новых технологий увеличивает зависимость от поставщиков IT-услуг, что может повлиять на непрерывность работы казначейства. Согласно данным Gartner, около 30% крупных организаций сталкивались с техническими сбоями, которые приводили к приостановке операций. В отчёте PwC за 2022 год также отмечается, что 60% финансовых организаций пережили сбои в своих критических системах, что могло вызвать значительные финансовые и операционные потери [11].

Юридические и регуляторные риски также играют важную роль в процессе цифровизации. Необходимость соблюдать разнообразные законодательные требования, особенно в области защиты данных, увеличивает риски правовых нарушений. Исследование Accenture показало, что 38% финансовых учреждений испытывают трудности с соблюдением законодательства, особенно с учётом часто меняющихся нормативных норм в области защиты данных. Кроме того, согласно EY, более 50% банков в Европе сталкиваются с проблемами адаптации под новые нормативные требования, такие как GDPR и PSD2, что подчеркивает важность своевременного обновления системы в ответ на изменения законодательства.

Подготовка кадров и обучение также является важным аспектом успешной цифровизации. Недостаточная квалификация сотрудников в области информационной безопасности и финансовых технологий может привести к ошибкам, утечкам данных и другим инцидентам. По данным Deloitte, 40% организаций испытывают дефицит квалифицированных специалистов, что замедляет процесс цифровизации. Также 50% крупных организаций сталкиваются с дефицитом ресурсов для обучения сотрудников, что затрудняет внедрение новых технологий [13].

Одним из наиболее очевидных последствий цифровизации является возможность финансовых потерь из-за инцидентов. Проблемы с IT-системами, такие как сбои или утечки данных, могут привести к значительным финансовым убыткам для казначейства. Согласно исследованию KPMG, каждое второе финансовое учреждение понесло убытки из-за технических сбоев или утечек данных. В отчёте McKinsey за 2020 год указано, что 17% банков столкнулись с крупными сбоями, которые привели к потерям до 1% годового дохода [11].

Наконец, использование облачных технологий создаёт дополнительные риски, связанные с безопасностью данных и техническими сбоями. В 2022 году 90% финансовых учреждений использовали облачные технологии для обработки данных, и около 20% из них сталкивались с инцидентами, связанными с утратой данных в облаке. Проблемы с интеграцией облачных решений с существующими IT-системами были зафиксированы в 50% организаций [13].

Цифровизация казначейства приносит не только выгоды, но и риски. Главный из них – кибератаки и утечки данных, так как

новые технологии добавляют слабые места в защиту информации. Чтобы уменьшить эти риски, нужно установить многоуровневую защиту, например, шифрование и регулярное обновление программ. Сбои в технике и зависимость от поставщиков тоже угрожают работе казначейства. Поэтому важна автономная IT-инфраструктура и запасные системы для случаев поломки. Изменения в законах создают юридические риски, требуя постоянного контроля и адаптации к новым правилам, чтобы избежать наказаний и сохранить доверие клиентов.

Успешная цифровизация казначейства возможна только при чёткой стратегии управления рисками, которая включает защиту данных, резервирование систем, подготовку сотрудников и соблюдение законов.

Для успешной цифровизации казначейской деятельности необходимо учитывать широкий спектр рисков и угроз, которые могут повлиять на её функционирование. Системы цифрового казначейства подвергаются различным видам внешних и внутренних угроз, включая кибератаки, технические сбои, юридические риски, а также недостаточную подготовленность персонала. Важно не только выявить эти риски, но и разработать эффективные меры для их минимизации. В следующей таблице представлены основные риски и угрозы, с которыми могут столкнуться казначейства при цифровизации, а также рекомендации по их управлению и предотвращению.

**Таблица 1**

**Риски и угрозы при цифровизации казначейства***

| *Тип риска* | *Описание угрозы* | *Меры минимизации риска* |
|---|---|---|
| *Киберугрозы и утечка данных* | *Угроза несанкционированного доступа, утечек данных, кибератак (например, фишинг, вирусы)* | *Внедрение многоуровневых систем защиты данных, использование шифрования, регулярные обновления ПО, обучение сотрудников* |
| *Технические сбои* | *Сбой в работе IT-систем, зависимость от внешних поставщиков технологий, отказ оборудования* | *Создание резервных систем, использование альтернативных платформ, регулярное тестирование инфраструктуры, планирование восстановительных мероприятий* |
| *Юридические риски* | *Нарушение законодательства в области обработки персональных данных, финансовых операций, международных стандартов* | *Регулярный мониторинг изменений в законодательстве, внедрение юридических консультаций, соблюдение стандартов защиты данных и финансовых операций* |
| *Низкий уровень подготовки кадров* | *Недостаточные знания специалистов для работы с цифровыми системами, что может привести к ошибкам или уязвимостям* | *Регулярное обучение сотрудников, повышение квалификации, внедрение внутренней мотивации и аттестации специалистов* |
| *Риски нарушения внутренней целостности* | *Внутренние угрозы, такие как ошибки сотрудников или преднамеренные действия, приводящие к утечке информации или ошибкам в процессе* | *Разработка внутренних политик безопасности, контроль доступа, внедрение системы аудита и мониторинга действий сотрудников* |
| *Зависимость от внешних факторов* | *Проблемы с подключением к внешним платформам или поставщикам услуг, сбои в связи, ошибки со стороны поставщиков* | *Заключение соглашений с несколькими поставщиками, внедрение резервных каналов связи, регулярное тестирование внешних сервисов* |
| *Операционные риски* | *Нарушения в процессе интеграции цифровых систем, ошибки в настройках, проблемы с совместимостью* | *Тщательное тестирование интеграционных решений, проведение пилотных запусков, использование стандартных протоколов и платформ* |

** Подготовленно автором.*

Представленная таблица-1 иллюстрирует ключевые риски и угрозы, с которыми сталкиваются казначейства при цифровизации своих процессов. Наиболее заметным риском является угроза кибератак и утечек данных, что требует внедрения многоуровневых систем защиты и регулярных обновлений программного обеспечения для обеспечения безопасности финансовых и персональных данных. Технические сбои и зависимость от внешних поставщиков также представляют собой значительную угрозу, что делает важным наличие резервных систем и альтернативных платформ для обеспечения бесперебойной работы. Юридические риски, связанные с изменениями в законодательстве, подчеркивают необходимость постоянного мониторинга и адаптации к новым требованиям, что позволяет избежать санкций и правовых последствий.

Невозможность казначейства функционировать без должной подготовки кадров также подтверждает необходимость систематического обучения сотрудников, что помогает минимизировать риски ошибок и уязвимостей. Внутренние угрозы, такие как ошибки или преднамеренные действия сотрудников, могут быть снижены с помощью разработки четких внутренних политик безопасности и системы контроля доступа. Наконец, риски, связанные с операциями и зависимостью от внешних факторов, требуют дополнительного внимания к интеграции и тестированию цифровых платформ, а также заключения соглашений с несколькими поставщиками для обеспечения устойчивости.

В целом, таблица-2 подчеркивает важность комплексного подхода к управлению рисками, который включает как технические меры, так и внимание к правовым, кадровым и внутренним аспектам цифровизации.

**Таблица 2**

**Мероприятия для улучшения устойчивости цифровых казначейских систем***

| *Направление* | *Мероприятия для повышения устойчивости* | *Цель и ожидаемый эффект* |
|---|---|---|
| *Усиление безопасности данных* | *- Внедрение многоуровневых систем защиты данных (шифрование, аутентификация)* | *Защита данных от несанкционированного доступа, предотвращение утечек* |
| | *- Регулярные обновления программного обеспечения и операционных систем* | *Повышение защиты от уязвимостей и эксплойтов* |
| *Устойчивость IT-инфраструктуры* | *- Создание резервных копий данных и разработка планов восстановления после сбоев* | *Обеспечение непрерывности операций при сбоях и катастрофах* |
| | *- Развитие автономных систем и минимизация зависимости от внешних поставщиков* | *Устранение рисков, связанных с отказом внешних поставщиков* |
| *Юридическое соответствие* | *- Постоянный мониторинг изменений в законодательстве и стандартах безопасности* | *Соблюдение нормативных требований и избегание юридических последствий* |
| | *- Регулярное проведение юридических аудитов и проверок соответствия нормам* | *Обеспечение защиты от санкций и штрафов* |
| *Обучение и повышение квалификации кадров* | *- Проведение регулярных тренингов по информационной безопасности и цифровым инструментам* | *Повышение компетентности сотрудников для эффективной работы с новыми технологиями* |
| | *- Внедрение систем сертификации для сотрудников, работающих с чувствительной информацией* | *Снижение рисков человеческих ошибок и утечек данных* |

| | | |
|---|---|---|
| *Интеграция и тестирование систем* | *- Разработка и тестирование протоколов интеграции новых цифровых платформ с существующими системами* | *Обеспечение совместимости и минимизация рисков ошибок в интеграции* |
| | *- Проведение пилотных запусков и стресс-тестов на стадии внедрения новых технологий* | *Оценка устойчивости новых систем в условиях реального использования* |
| *Контроль и мониторинг* | *- Внедрение систем мониторинга для постоянного отслеживания состояния безопасности* | *Быстрое выявление угроз и минимизация возможных потерь* |
| | *- Разработка процедур для немедленного реагирования на инциденты безопасности* | *Обеспечение быстрой реакции на угрозы безопасности и их предотвращение* |

**Подготовленно автором.*

Представленная таблица содержит ряд мероприятий, направленных на улучшение устойчивости цифровых казначейских систем в условиях цифровизации. Наибольшее внимание уделяется обеспечению безопасности данных, с акцентом на многоуровневые системы защиты, регулярные обновления программного обеспечения и использование современных методов аутентификации и шифрования. Эти меры направлены на минимизацию рисков утечек данных и предотвращение кибератак.

Важной составляющей является развитие устойчивости IT-инфраструктуры. Это включает в себя создание резервных копий данных, разработку планов восстановления после сбоев и сокращение зависимости от внешних поставщиков, что помогает предотвратить критические потери при технических сбоях и внешних угрозах.

Также значительное внимание уделяется юридическому соответствию, с целью соблюдения нормативных актов и стандартов безопасности. Регулярный мониторинг изменений в законодательстве и проведение юридических аудитов позволяет минимизировать риски правовых последствий и санкций.

Не менее важным аспектом является обучение и повышение квалификации кадров. Регулярные тренинги по информационной безопасности и сертификация сотрудников помогают снизить риски, связанные с человеческим фактором, и повысить компетентность персонала в работе с новыми технологиями.

Интеграция и тестирование новых цифровых решений с существующими системами также являются ключевыми факторами для предотвращения ошибок и сбоев. Пилотные запуск и стресс-тесты позволяют заранее выявить возможные уязвимости и снизить риски при полном внедрении.

Наконец, контроль и мониторинг на всех этапах цифровизации позволяют оперативно реагировать на угрозы и инциденты безопасности, что минимизирует возможные потери и способствует более эффективному управлению рисками.

## Заключение и предложения.

Цифровизация казначейской деятельности приносит значительные преимущества в виде повышения эффективности, прозрачности и ускорения финансовых операций. Однако внедрение цифровых технологий также сопряжено с рядом рисков и угроз, таких как кибератаки, утечка данных, технические сбои, юридические несоответствия и недостаточная подготовленность кадров. Важно понимать, что успешная цифровизация невозможна без комплексного подхода к управлению этими рисками, что требует сочетания

технологий, процессов и квалифицированных кадров.

Цифровизация казначейской деятельности требует комплексного подхода к управлению рисками и угрозами, которые могут возникнуть в процессе внедрения новых технологий. Снижение этих рисков необходимо для обеспечения безопасности данных, стабильности IT-инфраструктуры и соблюдения юридических норм. Для эффективного управления рисками важно учитывать несколько ключевых направлений: защиту данных, устойчивость инфраструктуры, соблюдение законодательства, обучение персонала, интеграцию новых технологий и создание системы управления рисками.

Во-первых, укрепление защиты данных включает в себя внедрение современных методов шифрования и многофакторной аутентификации для всех пользователей, что позволяет значительно повысить уровень безопасности.

Во-вторых, построение устойчивой IT-инфраструктуры требует разработки и внедрения резервных систем и механизмов автоматического восстановления данных. Важно выбирать надежных внешних поставщиков IT-услуг и заключать с ними соглашения о резервировании, чтобы минимизировать риски, связанные с зависимостью от внешних факторов.

В-третьих, регулярное соблюдение юридических требований необходимо для того, чтобы система всегда оставалась в рамках актуального законодательства. Создание команды, которая будет отвечать за мониторинг изменений в законодательстве и стандартах, позволит своевременно адаптировать систему к новым требованиям.

В-четвёртых, обучение и сертификация персонала играют ключевую роль в снижении рисков, связанных с человеческим фактором. Регулярное проведение тренингов по новым технологиям и информационной безопасности обеспечит персонал необходимыми знаниями для работы с цифровыми системами.

В-пятых, создание комплексной системы управления рисками включает в себя разработку внутренней политики управления рисками, которая будет включать регулярные обновления и мониторинг всех процессов. Использование автоматизированных систем для мониторинга финансовых операций, безопасности данных и соблюдения юридических норм позволит эффективно управлять рисками и повысить оперативность реагирования на инциденты.

Наконец, интеграция новых технологий с существующими системами требует проведения пилотных запусков и тестирования новых платформ перед их полномасштабным внедрением. Разработка стандартов для интеграции новых цифровых решений поможет избежать ошибок и обеспечит совместимость с текущими системами.

***Список использованной литературы:***

*1. Johnson, M., et al. (2021). Data Security Threats in Digital Financial Systems. Journal of Financial Security, 34(2), 87-102.*

*2. Smith, T. (2019). Technical Failure Risks in Digital Treasury Systems. International Journal of Financial Technology, 25(3), 56-69.*

*3. Phelps, S. (2020). Legal Risks and Treasury Digitalization. Legal Aspects of Financial Technology, 12(4), 143-158.*

*4. Harris, R., et al. (2018). Training Specialists for Digital Tools in Treasury Operations. Journal of Treasury Management, 27(1), 33-46.*

*5. Benson, A., & Clark, L. (2022). Risk Management in Treasury Digitalization. Financial Risk Management Review, 14(2), 112-128.*

*6. Chang, L., & Tan, V. (2020). Treasury Digitalization Strategies: Analyzing Benefits and Risks. Journal of Corporate Finance, 31(3), 208-222.*

*7. Johnson, B., et al. (2021). Treasury Software: From Automation to Data Protection. Financial Systems Review, 18(5), 67-81.*

*8. Иванов, А. и Петров, С. (2021). Цифровизация казначейства в России: риски и вызовы. Российский журнал финансовых технологий, 10(2), 55-72.*

*9. Кузнецов, И. и Воронцов, В. (2020). Интеграция цифровых платформ в казначейскую деятельность стран СНГ. Финансовая безопасность, 14(3), 124-139.*

*10. Gartner. Critical Infrastructure and Technology Risks in the Finance Sector. 2021.*

*11. PwC. Financial Services Technology Risk Survey. 2022.*

*12. EY. Digital Banking and Regulatory Challenges. 2021.*

*13. McKinsey. Impact of System Failures on Banks. 2020.*

*14. Forrester. Integration of Cloud Platforms in Financial Services. 2021.*