

# МЕХАНИЗМЫ КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЫ ДАННЫХ В УСЛОВИЯХ ЦИФРОВОГО ТУРИЗМА

**Куймуратова Матлубахон Абдиманабовна**

Доктор философии (PhD) по экономике, доцент Наманганский  
государственный технический университет

**Жамолиддинова Мунисабону Мансуржонова**

Студент Наманганского государственного технического университета

**Аннотация:** В данной статье рассматриваются вопросы обеспечения кибербезопасности и защиты данных в условиях цифровизации туристической отрасли. Анализируются современные угрозы информационной безопасности, возникающие при использовании онлайн-платформ бронирования, электронных платежных систем, мобильных приложений и цифровых сервисов в туризме.

**Ключевые слова:** цифровой туризм, кибербезопасность, защита данных, информационная безопасность, персональные данные.

## CYBERSECURITY AND DATA PROTECTION MECHANISMS IN

**Kuymuratova Matlubakhon Abdimanabovna**

Doctor of Philosophy (PhD) in Economics, Associate Professor, Namangan  
State Technical University

**Jamoliddinova Munisabonu Mansurjonovna**

Student, Namangan State Technical University

**Abstract:** This article examines the issues of cybersecurity and data protection in the context of tourism digitalization. The study analyzes modern information security threats arising from the use of online booking platforms, electronic payment systems, mobile applications, and digital services in tourism.

**Keywords:** digital tourism, cybersecurity, data protection, information security, personal data.

**Введение.** В условиях стремительного развития цифровых технологий туристическая отрасль претерпевает существенные изменения, связанные с внедрением информационно-коммуникационных систем, онлайн-платформ бронирования, мобильных приложений, электронных платежных сервисов и облачных технологий. Цифровизация туристической индустрии способствует повышению качества обслуживания, расширению доступа к туристическим услугам, ускорению обмена информацией и оптимизации взаимодействия между поставщиками услуг и потребителями. Вместе с тем активное внедрение цифровых технологий сопровождается увеличением рисков, связанных с киберугрозами, утечкой конфиденциальной информации, несанкционированным доступом к персональным данным и мошенничеством в цифровой среде.

**Основная часть.** Развитие цифровых технологий в туристической отрасли привело к существенному изменению механизмов предоставления услуг, взаимодействия между субъектами рынка и способов обслуживания клиентов. В современных условиях цифровой туризм представляет собой систему, основанную на использовании информационно-коммуникационных технологий, мобильных приложений, облачных сервисов, онлайн-платформ бронирования, электронных платежных систем и интеллектуальных аналитических решений. Туристические компании, гостиницы, транспортные организации и сервисы онлайн-бронирования активно используют цифровые технологии для оптимизации процессов управления, персонализации туристических предложений и повышения качества обслуживания клиентов. Однако одновременно с этим усиливаются угрозы информационной безопасности, что делает вопросы киберзащиты одним из ключевых направлений развития туристической индустрии.

Кибербезопасность в сфере туризма представляет собой совокупность организационных, технических и правовых механизмов, направленных на обеспечение конфиденциальности, целостности и доступности информации.

Основной особенностью туристической отрасли является высокий уровень обработки персональных данных клиентов. Во время регистрации на цифровых платформах пользователь предоставляет паспортные сведения, контактные данные, информацию о банковских картах, маршрутах поездок, предпочтениях и финансовых операциях. Подобная информация становится объектом интереса злоумышленников, осуществляющих кибератаки, фишинг, вредоносные программы, несанкционированный доступ к учетным записям и мошеннические операции.

Наиболее распространенными угрозами в цифровом туризме являются кража персональных данных, взлом информационных систем, утечка конфиденциальной информации, фальшивые туристические сайты и электронное мошенничество. В частности, злоумышленники могут создавать поддельные страницы бронирования гостиниц и авиабилетов, имитируя интерфейс популярных платформ, что приводит к потере финансовых средств и компрометации личных данных пользователей. Также существенную угрозу представляют вирусные программы и атаки на базы данных туристических компаний, способные привести к остановке работы цифровых систем и финансовым потерям.

**Таблица 1. Основные киберугрозы в условиях цифрового туризма и механизмы защиты**

<b>№</b>	<b>Вид угрозы</b>	<b>Характеристика угрозы</b>	<b>Механизмы защиты</b>
1	Фишинговые атаки	Создание поддельных сайтов и писем для получения личных данных	Двухфакторная аутентификация, проверка URL, обучение пользователей
2	Утечка персональных данных	Несанкционированный доступ к клиентской	Шифрование данных, защита

		информации	серверов, контроль доступа
3	Вредоносное программное обеспечение	Заражение устройств вирусами и программами-шпионами	Антивирусные системы, регулярное обновление ПО
4	Кибермошенничество	Незаконные финансовые операции и поддельные бронирования	Использование защищённых платежных систем
5	Взлом информационных систем	Несанкционированное проникновение в базы данных	Firewall, резервное копирование, мониторинг безопасности

Анализ представленных угроз показывает, что обеспечение информационной безопасности в цифровом туризме требует комплексного подхода, объединяющего технологические, организационные и правовые меры защиты. Одним из наиболее эффективных механизмов обеспечения кибербезопасности является внедрение многоуровневой системы защиты данных. Такая система включает использование криптографических методов шифрования, межсетевых экранов, резервного копирования информации, систем обнаружения вторжений и регулярного аудита безопасности.

Особое значение приобретает защита персональных данных туристов. Большинство туристических сервисов работают на основе облачных технологий, что предполагает передачу информации между различными цифровыми платформами. В этой связи необходимо соблюдать международные стандарты информационной безопасности, обеспечивать прозрачность обработки данных и минимизировать риски утечки информации. Кроме того, туристические организации должны проводить регулярное обучение персонала вопросам цифровой безопасности, поскольку

человеческий фактор остается одной из наиболее распространенных причин киберинцидентов.

Дополнительным направлением обеспечения безопасности является внедрение искусственного интеллекта и аналитических систем мониторинга угроз, позволяющих выявлять подозрительную активность и предотвращать кибератаки в режиме реального времени. Использование технологий машинного обучения способствует анализу поведения пользователей и быстрому выявлению аномалий в работе цифровых сервисов. Это особенно важно для крупных туристических платформ, обрабатывающих значительные массивы данных и финансовых операций.

**Заключение.** Таким образом, цифровизация туризма открывает широкие возможности для повышения эффективности обслуживания и расширения спектра услуг, однако одновременно усиливает необходимость внедрения современных механизмов защиты информации. Формирование надежной системы кибербезопасности становится важнейшим условием устойчивого функционирования туристической отрасли в условиях глобальной цифровой трансформации.

#### СПИСОК ЛИТЕРАТУРЫ

1. Постановление Президента Республики Узбекистан № ПП–348 от 19 ноября 2025 года «О мерах по организации деятельности Комитета по туризму Республики Узбекистан и ускоренному развитию сферы туризма»
2. Закон Республики Узбекистан «О туризме» (ЗРУ–549 от 18 июля 2019 года)
3. Аникин И.В. Кибербезопасность: защита информации в цифровой среде. – Москва: Юрайт, 2023. – 312 с.
4. Козлов А.А., Петров С.В. Информационная безопасность в условиях цифровой экономики. – Санкт-Петербург: Питер, 2022. – 287 с.

5. Гаврилов Д.С. Цифровая трансформация туристической индустрии: современные подходы и технологии // Экономика и управление. – 2023. – №4. – С. 45–52.

6. Иванова Н.П. Информационные технологии в туризме. – Москва: Инфра-М, 2021. – 254 с.