**БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ПЛАТЕЖЕЙ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ**

**Дахкильгова Тамара Салингиреевна,** студент

**Цороева Марем Иссаевна,** *преподаватель*

**Ингушский Государственный Университет (г.Магас)**

*Аннотация: В статье рассматриваются актуальные вопросы безопасности мобильных платежей, анализируются существующие угрозы и уязвимости, а также предлагаются решения для повышения уровня защиты мобильных финансовых транзакций. Особое внимание уделяется анализу методов аутентификации, шифрования данных и мониторинга транзакций. Оцениваются перспективы развития технологий безопасности мобильных платежей, включая биометрическую аутентификацию и использование искусственного интеллекта для обнаружения мошеннических операций.*

*Ключевые слова: мобильные платежи, электронные платежные системы, безопасность, угрозы, уязвимости, аутентификация, шифрование, биометрия, искусственный интеллект, финансовые транзакции.*

Мобильные платежи становятся всё более популярным способом оплаты товаров и услуг. Удобство и доступность делают их привлекательными для потребителей, а развитие технологий и инфраструктуры способствует их широкому распространению. Однако рост популярности мобильных платежей привлекает и злоумышленников, стремящихся получить несанкционированный доступ к финансовым средствам пользователей.

Безопасность мобильных платежей является критически важным аспектом развития всей индустрии. Утечка данных, мошеннические транзакции и другие инциденты, связанные с безопасностью, могут подорвать доверие потребителей и привести к серьезным финансовым потерям.

Существует широкий спектр угроз и уязвимостей, которые могут быть использованы злоумышленниками для совершения мошеннических действий в сфере мобильных платежей:

Фишинг и смишинг: мошеннические сообщения, имитирующие официальные уведомления от банков или платежных систем, с целью получения учетных данных пользователей.

Вредоносное ПО: мобильные приложения, содержащие вирусы или трояны, которые могут перехватывать информацию о платежах или получать доступ к банковским счетам.

Атаки «человек посередине» (Man-in-the-Middle): перехват трафика между мобильным устройством и сервером платежной системы для кражи данных.

Незащищенные сети Wi-Fi: использование общедоступных сетей Wi-Fi без шифрования позволяет злоумышленникам перехватывать данные пользователей, включая платежную информацию.

Кража или потеря мобильного устройства: потеря или кража мобильного устройства, содержащего данные о платежных картах или доступ к мобильному банкингу, может привести к несанкционированному доступу к финансовым средствам.

Уязвимости в мобильных приложениях: недостаточная защита мобильных приложений может позволить злоумышленникам получать доступ к конфиденциальной информации или совершать мошеннические транзакции.

Для защиты мобильных платежей используются различные методы и технологии:

Аутентификация:

Двухфакторная аутентификация (2FA): использование двух различных факторов аутентификации (например, пароля и SMS-кода) для подтверждения личности пользователя.

Биометрическая аутентификация: использование уникальных биометрических данных (например, отпечатка пальца, распознавания лица) для идентификации пользователя.

Шифрование данных: использование криптографических алгоритмов для защиты данных, передаваемых между мобильным устройством и сервером платежной системы.

Токенизация: замена реальных данных платежных карт на уникальные токены, которые используются для совершения транзакций. Это позволяет защитить конфиденциальную информацию в случае утечки данных.

Мониторинг транзакций: использование систем мониторинга транзакций для выявления подозрительной активности и предотвращения мошеннических операций.

Безопасная передача данных: использование протоколов HTTPS для защиты данных при передаче через Интернет.

Развитие технологий безопасности мобильных платежей не стоит на месте. В будущем можно ожидать широкого распространения следующих технологий:

Улучшенная биометрическая аутентификация: использование более надежных и точных методов биометрической аутентификации, таких как распознавание вен на ладони или анализ поведения пользователя.

Искусственный интеллект и машинное обучение: использование алгоритмов машинного обучения для выявления аномалий в платежных операциях и предотвращения мошенничества.

Блокчейн-технологии: использование блокчейна для создания более безопасных и прозрачных платёжных систем.

Усиленная защита мобильных устройств: разработка новых методов защиты мобильных устройств от вредоносного ПО и несанкционированного доступа.

Безопасность мобильных платежей является сложной и многогранной проблемой, требующей постоянного внимания и совершенствования. Разработчики платёжных систем, банки и другие участники рынка должны постоянно работать над повышением уровня защиты мобильных финансовых транзакций, используя современные технологии и методы обеспечения безопасности. Только так можно обеспечить доверие потребителей и дальнейшее развитие индустрии мобильных платежей.

**Библиографический список:**

1. Андерсон, Р. (2008). Инженерия безопасности. Джон Уайли и сыновья.
2. Фергюсон Н., Шнайер Б. (2003). Практическая криптография. John Wiley & Sons.
3. Столлингс, У. (2017). Криптография и сетевая безопасность: принципы и практика. Пирсон.
4. Европейское банковское управление (EBA). (2015). Отчет EBA о безопасности интернет-платежей.
5. ENISA. (2016). Обзор угроз и руководство по передовым методам для мобильных платежей.