*Оздоева Амина Магомедовна*

Ингушский государственный университет, Республика Ингушетия, Россия

ozdoamina@mail.ru

Научный руководитель: *Цороева Марем Иссаевна*

Ингушский государственный университет, Республика Ингушетия, Россия

**Безопасность цифровых платежей: современные угрозы и методы защиты**

Аннотация: в статье рассматриваются современные угрозы безопасности, нацеленные на цифровые платежные системы, включая фишинг, вредоносное ПО, атаки "человек посередине", атаки на мобильные устройства и криптовалютные кошельки, а также социальную инженерию. Проанализированы эффективные методы защиты, такие как многофакторная аутентификация, токенизация, шифрование данных, мониторинг транзакций, обучение пользователей и соблюдение стандартов безопасности. Подчеркивается необходимость комплексного подхода, сочетающего технологические инновации, организационные меры, правовое регулирование и сотрудничество между участниками рынка, для обеспечения безопасности пользователей, стабильности финансовой системы и развития цифровой экономики. Особое внимание уделено необходимости постоянной адаптации к новым угрозам и инновациям в сфере кибербезопасности.

Ключевые слова: киберпреступность, финансовая безопасность, платежные системы, информационная безопасность, киберриски, цифровая экономика, безопасность транзакций, методы защиты информации.

В эпоху стремительной цифровизации экономики и общества, цифровые платежно-расчетные системы трансформировались из удобного дополнения в жизненно важную инфраструктуру. Они стали неотъемлемым компонентом торговли, сферы услуг, государственных финансов и повседневных операций миллионов людей по всему миру. Удобство, скорость, доступность и снижение транзакционных издержек сделали цифровые платежи предпочтительным способом осуществления финансовых операций. Однако, эта цифровая революция привела к экспоненциальному росту киберпреступности, нацеленной на уязвимости и лазейки в цифровых платежных системах. Следовательно, обеспечение безопасности цифровых платежей стало приоритетной задачей для всех заинтересованных сторон: правительств, финансовых институтов, поставщиков платежных услуг и конечных потребителей. В данной статье мы проведем углубленный анализ современных угроз, нацеленных на цифровые платежные системы, подробно рассмотрим эффективные методы защиты и подчеркнем важность комплексного подхода для обеспечения безопасности пользователей и поддержания стабильности и доверия к финансовой инфраструктуре [1].

Киберпреступность в сфере цифровых платежей постоянно эволюционирует, становясь все более сложной, изощренной и целенаправленной. Злоумышленники используют широкий спектр инструментов и техник для кражи данных, обмана пользователей и подрыва доверия к цифровым платежным системам. Для эффективной борьбы с этими угрозами необходимо четкое понимание их природы и механизмов:

•  Фишинговые атаки: социальная инженерия в действии: Фишинг остается одним из наиболее распространенных и эффективных методов, используемых киберпреступниками. Мошенники маскируются под легитимные организации (банки, платежные системы, интернет-магазины) и отправляют поддельные электронные письма, сообщения в социальных сетях или SMS, содержащие ссылки на фальшивые веб-сайты. Эти веб-сайты обычно выглядят как настоящие и предназначены для обмана пользователей с целью раскрытия их учетных данных, таких как логины, пароли, номера кредитных карт, CVV-коды и личная информация. Фишинговые атаки часто используют методы социальной инженерии, играя на страхе, срочности или жадности жертвы.

•  Вредоносное ПО (Malware): скрытые угрозы на устройствах пользователей: Вредоносное программное обеспечение, такое как вирусы, трояны, шпионские программы и программы-вымогатели, представляет серьезную угрозу для цифровых платежей. Злоумышленники могут распространять вредоносное ПО через электронную почту, зараженные веб-сайты, поддельные приложения или уязвимости в программном обеспечении. После установки на компьютер или мобильное устройство пользователя, вредоносное ПО может перехватывать платежную информацию, красть данные учетных записей, осуществлять несанкционированные транзакции, блокировать доступ к устройству и требовать выкуп.

•  Атаки "человек посередине" (Man-in-the-Middle): перехват и манипуляция данными: Этот тип атаки подразумевает, что злоумышленник перехватывает связь между пользователем и платежной системой, например, между компьютером пользователя и сервером онлайн-банка. Перехватывая данные, злоумышленник может их изменять, например, подменяя номер счета получателя платежа, увеличивая сумму транзакции или крадя учетные данные пользователя.

•  Брутфорс-атаки: взлом методом перебора: Брутфорс-атаки – это метод, при котором злоумышленник пытается угадать пароль пользователя путем перебора всех возможных комбинаций. Эффективность брутфорс-атак значительно снижается при использовании сложных и уникальных паролей, а также при внедрении механизмов блокировки учетной записи после нескольких неудачных попыток входа.

•  Атаки на мобильные устройства: уязвимость портативных платформ: Мобильные устройства стали основным инструментом для осуществления цифровых платежей, что делает их привлекательной целью для киберпреступников. Угрозы включают кражу устройств, установку вредоносного ПО на мобильные телефоны (например, через поддельные приложения), перехват SMS-сообщений с кодами двухфакторной аутентификации (SIM-свопинг), а также использование уязвимостей в мобильных операционных системах.

•  Социальная инженерия: игра на человеческом факторе: Социальная инженерия – это метод манипулирования людьми для получения конфиденциальной информации или выполнения определенных действий. Злоумышленники могут представляться сотрудниками банка, технической поддержки, правоохранительных органов или даже друзьями и родственниками, чтобы убедить пользователя предоставить свои учетные данные, перевести деньги или установить вредоносное ПО.

•  Атаки на API и инфраструктуру платежных систем: проникновение вглубь системы: Недостатки в безопасности API (интерфейсов программирования приложений) и других компонентов инфраструктуры платежных систем могут быть использованы для компрометации системы, кражи данных, подмены транзакций или нарушения работоспособности.

•  Внутренние угрозы: злоупотребления и халатность: Злоупотребления со стороны сотрудников платежных систем или финансовых учреждений, имеющих доступ к конфиденциальной информации, также представляют серьезную угрозу. Это может включать кражу данных, мошеннические транзакции, передачу информации третьим лицам или небрежное отношение к мерам безопасности.

•  Скимминг: устаревающая, но все еще актуальная угроза: Скимминг – это кража данных с магнитных полос банковских карт при использовании поддельных устройств (скиммеров), установленных на банкоматах или POS-терминалах. Хотя эта угроза снижается с распространением EMV-чипов (которые сложнее подделать), скиммеры все еще используются в некоторых регионах.

•  Атаки на криптовалютные кошельки и биржи: высокая ценность, высокая опасность: Криптовалюты, обладающие высокой ценностью и анонимностью, стали привлекательной целью для киберпреступников. Угрозы включают кражу криптовалюты из кошельков пользователей (путем взлома, фишинга или вредоносного ПО), взлом криптовалютных бирж для хищения средств, а также манипуляции с ценами на криптовалюты [2].

Учитывая разнообразие и сложность современных угроз, эффективная защита цифровых платежных систем требует применения комплексного и многоуровневого подхода, который включает в себя технологические инновации, организационные меры, образовательные кампании и законодательное регулирование.

Многофакторная аутентификация (MFA) требует от пользователя предоставления нескольких способов подтверждения личности перед получением доступа к платежной системе или совершением транзакции. Это может включать комбинацию пароля, SMS-кода, биометрических данных (отпечатка пальца, распознавания лица) или аппаратных токенов. MFA значительно усложняет задачу для злоумышленников, даже если им удастся украсть или угадать пароль пользователя.

Токенизация заменяет реальные номера банковских карт или другие конфиденциальные данные уникальными цифровыми идентификаторами (токенами), которые не имеют ценности для злоумышленников. Токены могут использоваться для совершения транзакций, не раскрывая реальные данные [3].

Шифрование – это преобразование данных в нечитаемый формат с использованием криптографических алгоритмов. Шифрование следует использовать для защиты конфиденциальной информации при передаче по сети (например, с использованием протокола HTTPS) и при хранении на серверах.

Установка и регулярное обновление антивирусного программного обеспечения и брандмауэров на компьютерах и мобильных устройствах пользователей помогает защитить их от вредоносного ПО и несанкционированного доступа.

Использование алгоритмов машинного обучения и искусственного интеллекта для анализа транзакций в режиме реального времени позволяет выявлять подозрительные операции, такие как необычно крупные переводы, транзакции из необычных мест или транзакции с использованием скомпрометированных учетных записей.

Использование HTTPS и других безопасных протоколов для защиты данных, передаваемых между пользователем и платежной системой, предотвращает перехват и изменение информации злоумышленниками.

Установка последних обновлений операционных систем, приложений и платежных систем помогает закрыть уязвимости в безопасности, которые могут быть использованы злоумышленниками.

Проведение образовательных кампаний для повышения осведомленности пользователей о методах мошенничества, фишинга, социальной инженерии и других угрозах, а также о мерах предосторожности при использовании цифровых платежей, является важным элементом защиты. Пользователи должны знать, как распознавать подозрительные сообщения, как создавать надежные пароли, как защищать свои устройства и как сообщать о подозрительной активности.

Использование сложных, уникальных и регулярно меняющихся паролей для всех учетных записей, связанных с цифровыми платежами, является критически важным. Пароли должны быть достаточно длинными, содержать комбинацию букв, цифр и специальных символов, и не должны использоваться повторно на разных веб-сайтах.

Разработка и внедрение строгих политик безопасности и процедур для защиты платежных систем от внутренних и внешних угроз, включая контроль доступа, аудит безопасности, реагирование на инциденты и обучение персонала, необходимы для создания надежной системы защиты.

Соответствие международным стандартам безопасности, таким как PCI DSS (Payment Card Industry Data Security Standard), для защиты данных платежных карт, помогает организациям внедрить лучшие практики и обеспечить высокий уровень безопасности.

Обмен информацией об угрозах и методах противодействия между платежными системами, банками, правоохранительными органами, аналитическими центрами и другими заинтересованными сторонами позволяет оперативно реагировать на новые угрозы и разрабатывать эффективные стратегии защиты.

Использование страховых продуктов для компенсации убытков, связанных с киберпреступностью, может помочь организациям смягчить финансовые последствия атак и восстановить свою деятельность после инцидентов.

Внедрение технологий распознавания лиц, отпечатков пальцев или голоса для подтверждения личности пользователя обеспечивает более надежную аутентификацию, чем традиционные пароли.

Использование распределенного реестра (блокчейна) для хранения информации о транзакциях может повысить прозрачность, безопасность и надежность цифровых платежных систем, особенно в контексте криптовалют [4].

Разработка и принятие законов, направленных на борьбу с киберпреступностью, защиту прав потребителей в сфере цифровых платежей, установление ответственности за нарушение безопасности и создание механизмов сотрудничества между правоохранительными органами и частным сектором, являются важными шагами для создания безопасной и правовой среды для цифровых платежей.

Безопасность цифровых платежей является непрерывным и многогранным вызовом, требующим постоянного внимания, инноваций и сотрудничества. Современные угрозы становятся все более сложными и изощренными, требуя от всех участников рынка постоянного совершенствования методов защиты. Комплексный подход, сочетающий технологические инновации, организационные меры, образовательные кампании, правовое регулирование и активное сотрудничество, позволит эффективно противодействовать киберпреступности, защищать права потребителей, обеспечивать стабильность финансовой системы и содействовать развитию безопасной и процветающей цифровой экономики. Важно признать, что безопасность – это не статичное состояние, а динамичный процесс, требующий постоянной адаптации к новым угрозам и инновациям. Только при таком подходе мы сможем создать надежную и безопасную экосистему цифровых платежей, которая будет способствовать экономическому росту и улучшению качества жизни людей.

**Список использованной литературы**

1.Орлов С.Н., Татаринцев А.В. Экономическая безопасность электронных средств платежа // Экономико-правовые проблемы обеспечения экономической безопасности. Екатеринбург, 2021. С. 79-82.

2.Полякова А.А. Классификация электронных платежей систем // Экономика и социум. 2019. № 4. С. 613-615.

3.Ущекин С.Н. Безопасность электронных средств платежа // Актуальные проблемы теории и практики уголовного права и процесса в современных условиях. Донецк, 2023. С. 605-609.

4.Якимова М.А. Развитие применения электронных денег в современной России // E-Scio, 2022. № 3. С. 691-701.