УДК 004.056

Н. КАРАПЕТЬЯНЦ

Национальный исследовательский ядерный университет «МИФИ», Москва

МОДЕЛЬ УГРОЗ И МОДЕЛЬ НАРУШИТЕЛЕЙ ДЛЯ ИНФРАСТРУКТУРЫ КРИПТОВАЛЮТНЫХ ПЛАТЕЖНЫХ СИСТЕМ

В материалах доклада представлено описание специфики разработки моделей угроз и нарушителей с учетом особенностей обеспечения информационной безопасности инфраструктуры криптовалютных платежных систем. Предложена модель угроз, включающая компрометацию криптовалютных кошельков, обход механизмов отслеживания транзакций и утечку пользовательских данных, а также разработана модель нарушителя, охватывающая киберпреступников, внутренние субъекты и операторов криптовалютных платформ.

Использование криптовалют в качестве средства платежа в рамках трансграничных расчетов по внешнеторговым договорам подтверждает актуальность разработки класса решений для обеспечения безопасности инфраструктуры криптовалютных платежей [1]. В отличие от традиционной платежной системы, инфраструктура криптовалютных платежей обладает архитектурными особенностями, которые необходимо учитывать при разработке моделей угроз и нарушителей. Специфика инфраструктуры криптовалютных платежных систем заключается в неразрывной архитектурной интеграции четырех функций: биллинг, процессинг, блокчейн-аналитика, комплаенс. В традиционной системе эти функции обычно реализованы независимо друг от друга многими посредниками платежной системы. Поэтому основной задачей данного исследования является разработка модели угроз и модели нарушителя для инфраструктуры криптовалютных платежных систем с учетом их особенностей.

Можно выделить следующие угрозы, связанные с архитектурными особенностями криптовалютной платежной системы: угроза компрометации криптовалютных кошельков, угроза обхода механизма отслеживания транзакций [2], угроза утечки данных пользователей. Угроза компрометации криптовалютных кошельков связана с утечкой, кражей, блокировкой приватных ключей, без которых платежные операции с криптовалютой невозможны. Если приватные ключи хранятся в холодном кошельке, то их могут только похитить. Что касается горячего кошелька, то доступ к ним может быть заблокирован как на

кастодиальных, так и на некастодиальных платформах. Угроза обхода механизма отслеживания криптовалютных транзакций может привести к проведению транзакций, средства которых могут быть связаны с незаконной деятельностью. Реализация данной угрозы может привести к штрафу со стороны регулятора, а в худшем случае к блокировке и отзыву лицензии. Реализация угрозы утечки данных пользователей может привести к их деанонимизации, что, несомненно, приведет к подрыву доверия со стороны большинства пользователей системы. Доверие пользователей в сети криптовалют имеет первостепенное значение, обеспечивая безопасность и устойчивость экосистемы.

Учитывая особенности архитектуры криптовалютной платежной системы, можно выделить следующих нарушителей: киберпреступники, внутренний нарушитель, а также платформы, осуществляющие операции с криптовалютой. Мотивация киберпреступников связана как с финансовой выгодой (кража криптовалюты), так и с возможностью произвести отмывание криптовалют, связанных с незаконной деятельностью. Внутренним нарушителем может быть любой сотрудник, чья деятельность напрямую связана с функционированием компонентов инфраструктуры криптовалютной платежной системы: от первой линии поддержки до системного администратора сетевой инфраструктуры [3]. Платформы, осуществляющие операции с криптовалютой, такие как биржи, сервисы обмена валют, сервисы хранения и управления криптовалютными кошельками могут заблокировать доступ к ресурсам в соответствии с законодательством той страны, в которой находятся, в рамках обеспечения борьбы с отмыванием денежных средств и финансированием терроризма.

В рамках работы были предложены модель угроз и модель нарушителя для инфраструктуры криптовалютной платежной системы. Результаты исследования могут быть использованы для улучшения существующих или разработки новых систем обеспечения безопасности данного класса систем.

Список литературы

1. Крылова Л.В. Возможность использования цифровых валют для трансграничных платежей в условиях санкций //Финансы: теория и практика. – 2024. – Т. 28. – №. 2. – С. 101–111.

2. Basynya E.A., Karapetyants N., Karapetyants M. Bitcoin Transaction Analysis System //Programming and Computer Software. – 2024. – Т. 50. – №. Suppl 2. – С. S104–S112.

3. Басыня Е.А., Сафронов А.В. Метод формирования децентрализованного реестра событий информационной инфраструктуры предприятия //Вестник УрФО. Безопасность в информационной сфере. – 2019. – №. 4 (34). – С. 35–44.