

Безопасность современных платежных технологий.

Частухин В.Ю.; Слепенчук Р.А.; Жачко А.Н.

Дальневосточный федеральный университет

Школа естественных наук

Кафедра информационной безопасности

Ключевые слова: Платёжная система, Электронная коммерция, Транзакция, Атака на систему, Цифровая валюта.

Введение в проблему

На сегодняшний день лидирующую позицию в сфере экономических взаимодействий в мире занимают наличные платежи, однако в большом количестве развивающихся стран всё большее распространение получает электронная коммерция. Она представляет собой совокупность структур, которые позволяют совершать транзакции, не используя наличные деньги. Однако, в связи с ростом популярности систем, посредством которых осуществляются электронные платежи, вопрос о их защите встаёт весьма остро. На сегодняшний день первоочередная задача в сфере безопасности платёжных технологий — это защита информации и персональных данных пользователей. Что бы гарантировать защищённость, инфраструктура платёжных систем должна постоянно развиваться и совершенствоваться, что, однако, влечёт за собой возникновение новых проблем, которые тоже нуждаются в решении.

Популярность электронных платёжных систем обусловлена множеством факторов, в числе которых: высокая скорость транзакций, их низкая стоимость. Кроме того, итогом 2020 года, прошедшего под знаком пандемии, стал резкий рост использования альтернативных способов оплаты. В общем случае процесс совершения транзакции посредством платёжной системы может быть представлен как взаимодействие продавца, покупателя и некоторого посредника (оператора). Конкретные действия этих сторон зависят от типа системы, однако схема взаимодействия всегда представляет собой последовательность запросов и ответов. Очевидно, что такие системы уязвимы к различным типам атак, именно поэтому первоочерёдным является обеспечение защиты данных всех участников взаимодействия. В рамках построения непосредственно систем, в качестве наиболее популярных средств безопасности используются криптографические протоколы, которые дают возможность гарантировать целостность данных пользователей и их

конфиденциальность. Однако первым шагом в формировании надёжной защиты является формулировка требований к системам.

Выработка критериев безопасности платёжных систем необходимы как для компаний, которые их разрабатывают, так и для пользователей. Первые получают возможность создать гарантированно надёжную систему, а вторые – способность оценить безопасность той или иной системы. К основным критериям безопасности платёжных систем относятся: надёжность паролей, использование протоколов шифрования при соединении с вебсайтом, безопасность при авторизации и наличие требования подтверждения операции. Кроме перечисленного, целесообразно использовать информационные способы обеспечения безопасности, то есть информировать пользователей о совершаемой операции, во избежание мошенничества, а также предоставлять им инструкции и рекомендации по безопасности.

Несмотря на множество мер защиты, ни одну систему нельзя назвать в полной мере надёжной. Абсолютное большинство атак на системы электронных платежей совершается с использованием вредоносного программного обеспечения. Суть таких атак заключается в том, что сперва злоумышленники проникают в систему через фишинговые письма, рассылаемые по списку электронных адресов сотрудников организаций. Вредоносное ПО содержится во вложениях таких писем или же его необходимо загрузить с внешнего ресурса по ссылке. Затем, после открытия вредоносного файла, происходит скрытая загрузка и запуск ПО, которое предоставляет атакующей стороне удаленный доступ к компьютеру. После проникновения в первый компьютер злоумышленники проводят изучение доступного сегмента локальной сети, выявляют другие, представляющие интерес, компьютеры и серверы, проникают и закрепляются в них, а затем приступают к подготовке непосредственного хищения.

С каждым днем появляются новые угрозы безопасности электронных платежей, а инциденты ИБ, связанные с незарегистрированными транзакциями, не теряют актуальности. С ростом популярности безналичных платежей возникла закономерная угроза ИБ в данной сфере. Именно электронная транзакция является наименее защищенной частью платёжной технологии. Еще в 2011 году правительство РФ разработало свод законов, которые служат для контроля цифровых денег. Так федеральный закон №161-ФЗ «О национальной платёжной системе» позволяет определить правила электронных переводов, обязанности операторов электронных средств при их участии в НПС РФ. Также данный закон регулирует роль ЦБ РФ в обработке электронных финансовых операций. №161-ФЗ дополняется федеральным законом №173-ФЗ, на их основе выпускаются положения ЦБ РФ, например положение от 23 декабря 2020 года №747-П и положение

№382-П от 9 июня 2012 года. Кроме того, 31 июля 2020 года был подписан закон №259-ФЗ "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации", который вводит понятие цифровой валюты (криптовалюты), регулирует выпуск цифровых финансовых активов (ЦФА) и цифровой валюты (ЦВ) и их оборот в РФ. Данный федеральный закон вступил в силу с 1 января 2021 года, он призван урегулировать новую для страны область – обращение цифровой валюты.

Заключение

С каждым годом число электронных платёжных систем, участвующих в национальной системе, становится все больше, старые же совершенствуются и модернизируются. Вместе с тем обнаруживаются новые уязвимости, требующие совершенствования механизмов защиты. Однако именно финансовые организации обладают достаточным уровнем мотивации и ресурсов, чтобы гарантировать наиболее надёжную и современную защиту средствами информационной безопасности. Тем не менее, существует необходимость контролировать процессы электронного финансового взаимодействия со стороны государства. В соответствии с политикой и для обеспечения безопасности государства, граждан и их финансов, выпускаются и дополняются законы, позволяющие регулировать взаимоотношения между государством, банками и пользователями.