Вопросы безопасности электронных платежных систем являются сложной задачей для финансового сектора и регуляторов. Существуют две серьезные проблемы – несанкционированные списания средств с банковских карт или счетов юридических лиц и общая гарантия сохранности платежей, совершаемых через небанковские системы переводы платежей. Поэтому нужно понимать как работает банковская система

Как работает ЭПС

- Под термином «электронная платежная система» (ЭПС) понимается система расчетов, при которой платежи проводятся по интернет-каналам, традиционной обработки платежных поручений не происходит.
- Под это определение попадают:
- расчеты посредством банковских карт традиционных систем Visa, MasterCard, «Мир». Здесь при абсолютной гарантии защиты трансакций возникает проблема несанкционированных списаний в результате перехвата трафика или получения номеров карт;
- программы межбанковских расчетов по электронным каналам связи, в том числе быстрых платежей, осуществляемых банками по номерам телефонов;
- расчеты через электронные кошельки (Яндекс.Деньги и другие);
- расчеты через инфраструктуру мобильных операторов и другие современные решения.

- Для осуществления платежей посредством банковских карт международные системы переводов применяют собственные меры ИБ межкарточных переводов, корреспондирующие с требованиями Банка России. Для иных операторов безбумажных платежей, совершающих более 6 миллионов переводов в год, работает программа сертификации Qualified Security Assessor (QSA).

- В России работают представительства нескольких организаций, имеющих право на выдачу сертификата, и он будет предоставлен, если оператор соответствует следующим требованиям:
- его деятельность соответствует международному стандарту Payment Card Industry Data Security Standard (PCI DSS);
- оператор сервиса платежей получил сертификат на соответствие международным требованиям к менеджменту ИБ кредитных организаций в сфере разработки, внедрения и сопровождения программных средств ISO/IEC 27001:2005;
- оператор работает с использованием электронно-цифровой подписи (ЭП);
- шифрование осуществляется разрешенными средствами криптографической защиты, разработанными организациями, имеющими лицензии на право осуществления деятельности по предоставлению, техническому обслуживанию криптографических средств.

Как работает проверка платежей

На самом деле описать все критерии проверки будет сложно — их 288. Сама процедура довольно длительная, потому что затрагивает проверку ряда сложных технических моментов. Полностью список критериев, разбитый на 12 групп, выглядит следующим образом:

- Защита вычислительной сети.
- Конфигурация компонентов информационной инфраструктуры.
- Защита хранимых данных о держателях карт.
- Защита передаваемых данных о держателях карт.
- Антивирусная защита информационной инфраструктуры.
- Разработка и поддержка информационных систем.
- Управление доступом к данным о держателях карт.
- Механизмы аутентификации.
- Физическая защита информационной инфраструктуры.
- Протоколирование событий и действий.
- Контроль защищенности информационной инфраструктуры.
- Управление информационной безопасностью.