Рекомендации по информационной безопасности

При разработке и реализации мер по обеспечению информационной безопасности участникам обмена рекомендуется применять положения международного стандарта ISO/IEC 27002:2013 Information technology. Security techniques. Codes of practice for information security controls.

1. В документах Клиентов, определяющих порядок обеспечения защиты информации при обмене электронными сообщениями, необходимо определять состав и порядок применения организационных мер защиты информации и использования технических средств защиты информации.

1.1. Документы должны учитывать следующие процессы (направлений) защиты информации:

обеспечение защиты информации при управлении доступом;

обеспечение защиты вычислительных сетей;

контроль целостности и защищенности информационной инфраструктуры;

защита от вредоносного кода;

предотвращение утечек информации;

управление инцидентами информационной безопасности;

защита среды виртуализации;

защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств.

1.2. В документах необходимо указать информацию, определяющую:

технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры;

состав и правила применения технологических мер защиты информации, используемых для контроля целостности и подтверждения подлинности электронных сообщений на этапах их формирования (подготовки), обработки, передачи и хранения, в том числе порядок

применения средств криптографической защиты информации (далее – СКЗИ) и управления ключевой информацией СКЗИ;

план действий, направленных на обеспечение непрерывности и восстановление деятельности, связанной с обменом электронными сообщениями;

лиц, допущенных к работе со СКЗИ;

лиц, ответственных за обеспечение функционирования и безопасности СКЗИ (ответственный пользователь СКЗИ);

лиц, обладающих правами по управлению криптографическими ключами, в том числе ответственных за формирование криптографических ключей и обеспечение безопасности криптографических ключей.

2. Клиентам рекомендуется обеспечивать хранение входящих и исходящих электронных сообщений, подписанных электронной подписью, не менее пяти лет.

3. При обмене электронными сообщениями между Клиентом и Банком России применяется электронная подпись, сертификат ключа проверки которой выдан Банком России.