Безопасность электронных архивов при доступе к ним организаций и граждан

Смирнов Николай Валерьевич, начальник Отдела научных исследований и развития продуктов компании ОАО «ИнфоТеКС»

В докладе рассматриваются риски использования популярной в настоящий момент парадигмы Cryptography free client при осуществлении удаленного доступа к архивам электронных документов, рисков доверенного обращения, посредством не доверенных каналов, к доверенной информации, размещенной на не доверенной площадке и затрагивается проблематика выполнения правил пользования СКЗИ.

Cryptography free client's

За последний год набирает популярность парадигма отказа от клиентской криптографии, при организации работ с удаленными ресурсами, документами, архивами документов.

Информационная безопасность в данной парадигме обеспечивается серверными механизмами авторизации и разграничения доступа к информации (файлам, директориям), встроенными в операционную систему. Преимущества внедрения подобной схемы очевидны:

- Нет необходимости проводить обучение персонала нюансам работы с СКЗИ и средствами ЭП
- Для доступа к ресурсам, включая удаленный доступ, могут быть использованы любые клиентские устройства, в том числе и популярные ныне планшеты
- Нет необходимости в строгой отчетности при использовании СКЗИ

Доверенный доступ к информации, в том числе, юридически значимой

Действительно безопасный доступ – это терминальный доступ к расположенному на доверенной площадке терминальному серверу через зашифрованный туннель. Этот способ доступа может гарантировать минимальные риски крупномасштабных утечек информации через пользовательские компьютеры (терминалы, рабочие станции, мобильные средства доступа), т.к. защищаемая информация не хранится и не обрабатывается (кроме отображения на экране терминала) на стороне пользователя.

К сожалению, абсолютные решения ИБ были, продолжают и будут оставаться недостижимыми в реальной жизни утопиями. Существующие средства ИБ, благодаря комплексному подходу обеспечения информационной безопасности, могут снижать вероятности нарушения доступности, конфиденциальности и целостности обрабатываемой (передаваемой) информации. Одной из важнейших, и одновременно наиболее часто нарушаемых компонент ИБ является выполнение регламентов правил пользования СКЗИ.

Справедливости ради, следует отметить, что встречаются СКЗИ, выполнения правил пользования которыми или невозможно в принципе, или нарушает бизнес сценарии или крайне ресурсоемко.

Вместе с тем, невыполнение правил пользования СКЗИ, так же как и отказ от использования СКЗИ, приводит к серьезным рискам, особенно опасным при работе с юридически значимой информацией.

Выводы

Современная распределенная информационная система обработки и хранения (включая архивное) информации немыслима без применения криптографических средств защиты информации, но их использование только тогда обеспечивает реальный уровень безопасности информации, когда соблюдаются организационные меры и правила использования СКЗИ.