Импортозамещение в криптографической защите массового сегмента пользователей

Криптографическая защита конфиденциальной информации у многомиллионного контингента пользователей востребована как государственными организациями так и частными лицами по всем трем направлениям обеспечения информационной безопасности(ИБ): конфиденциальность, целостность, доступность

Конфиденциальность – остается первой по объему нагрузки и целью применения криптографии среди массы пользователей

- Домашние устройства связи с роутером для подключения к Интернет.
- Криптография в сотовой связи на всем тракте

  ТЛФ - вышка - IP канал до коммутатора – вышка – ТЛФ
- Аналогично и для обмена данными, включая использование облачных технологий.
- Ключевая технология защиты тракта «ТЛФ-вышка» - иностранной разработки. Иностранные криптосхемы опубликованы, но:
  - Насколько верифицирована их реализация на ТЛФ?
  - Каковы возможности импортозамещения?
  - Только ли переход на IP- телефонию с последующим абонентским шифрованием?
- Чем закрывается IP-канал связи «вышка-вышка» у провайдеров телефонии?
- Принципиальная возможность импортозамещения на базе использования отечественных средств шифрования конфиденциальной информации имеется как по скорости, так и по сервису.

Импортозамещение VPN у массового пользователя (МП) персонального компьютера

- У МП применяется VPN от Microsoft, который устроен удобно для пользователя, встроен в операционную систему Windows и не требует от пользователя никаких специальных действий, кроме нажатия на иконку.
- SSL от Microsoft принимается Госуслугами, если он адресуется из России. Из заграницы его не принимают. А какой отечественный SSL принимают в Госуслугах?
- Работа с тремя отечественными VPN показала сложность их применения массовым, не групповым пользователем, без квалифицированной поддержки.
- Нет встроенных по умолчанию средств шифрования , предназначенных для защиты конфиденциальной информации, в отечественные ОС широкого применения (Астра, Альт), включая специальные.
- Разработчикам криптосредств следовало бы плотно поработать с держателями отечественных ОС.

Иностранный VPN - засада неизвестности

- Многократное перешифрование с помощью различных сервисов не дает никаких гарантий сохранения конфиденциальности. Например: Ключ в личном мобильном, даже кнопочном телефоне мы не меняем никогда.
- Шифрование в канале данных сотовой связи широко применяется мессенджерами с рекламой применения SSL и абонентского принципа использования ключевой пары. Однако при образовании общего ключа присутствует сервер для идентификации пользователя.
- С момента открытия принципа «открытого ключа» была известна проблема наличия атаки «человек посередине». Именно по этому существует удостоверяющий центр для SSL у провайдера услуги
- Отсутствие возможности реализации атаки «человек посередине» дает только государственная аттестация и контроль за соблюдением провайдером условий эксплуатации системы, что для иностранных мессенджеров неприемлемо.
- Давно обещан в России государственный VPN от Ростелекома с необходимыми сертификатами для защиты персональных данных- ждем с нетерпением.

Целостность сообщения - неотъемлемое свойство информационной безопасности

- Нарушение требований обеспечения квалифицированности электронной подписи (ЭП) для уровней КС2-КС3 у массового пользователя – обычная норма, поскольку ограничивает спектр применяемых технологий.
- Квалифицированной массовой ЭП не существует. Это иллюзия даже с применением специального токена. Это относится так же и к иностранной ЭП.
- Дистанционная выдача квалифицированной ЭП без личной явки при отсутствии у заявителя действующей ЭП, даже при использовании биометрии, противоречит смыслу ЭП , которая фактически является заменителем личности. Подобная практика может применятся только в мало бюджетных сделках или в непринципиальных документах.
- В каждой системе, применяющей ЭП, должен быть свой уровень декларированной защиты, одинаковый для всех пользователей системы.

ЭП и понимание надежности компьютерной технологии у массового пользователя

- Следует различать условия применения ЭП. Это надежный инструмент только при соблюдении ВСЕХ условий, сформулированных в отечественном сертификате на различные уровни способностей нападающей стороны.
- Юридическая и финансовая значимость ЭП фактически одинакова для всех уровней формирования по КС1-КА.
- Классификация КС1-КА понятна только специалистам. Нужен переводчик на понятный массовому пользователю язык. Например:
  - КС1 это защита с помощью ЭП от изменения собственной информации как при хранении, так и при пересылке, модификация которой нанесет ущерб в тысячу рублей;
  - КС2 – ущерб 100 тысяч рублей; КС3 – ущерб 1 млн. рублей и т. д.
- В Требованиях от ФСБ России так вряд ли можно сформулировать, но в методических материалах от соответствующего подразделения, наверное, можно.
- Какие уровни защиты обеспечивает и декларирует иностранная ЭП?

Массовые, аттестованные по требованиям ИБ с применением криптографии услуги: мессенджеры и электронная почта

- Аттестация зарубежных пользовательских систем невозможна.
- Существует государственная почтовая связь. Можно ли создать массовую отечественную электронную почту с аттестованным шифрованием и ЭП? Например, на базе Яндекса. Осуществим таким образом реальное импортозамещение зарубежных почтовых систем.
- Аналогично и отечественные мессенджеры, например, «Вконтакте».
- Уровень криптозащиты будет небольшой (КС1), но это существенно скажется на общем уровне ИБ компьютерных технологий в стране.
- А может быть, ввести специальный, дополнительный уровень защиты массовых систем: КМ –криптография массовая?

Роботы и доступность систем

- Дроны прочно вошли в нашу жизнь. Их число измеряется в стране миллионами и соответственно число связей с ними такое же. От игрушек до боевых систем. Какие отечественные криптографические технологии в них применяются?
- Защита канала от злоумышленника может быть на уровне «сотовый тлф – вышка», в соответствующем протоколе с шифратором на борту.
- Можно представить ситуации, когда будет востребована ЭП для подтверждения команды, например на химобработку поля или лесного участка.
- Доступность дрона или любого управляемого робота может быть повышена применением криптографии. Современный, домашний автономный пылесос управляется из Интернета, как холодильник и как газовый котел, что куда как опаснее.

Целостность обеспечивает доступность

- Хранение личной информации в компьютере полагается на штатную ОС. Криптозащиту применяют в основном в корпоративных системах. Установленных по умолчанию отечественных систем шифрования для защиты хранящейся информации нет, а объемы (например, уже терабайты фотографий) и важность растут быстро.
- Наличествующее в персональном компьютере программное обеспечение проверяется на целостность, как правило, по контрольным суммам, которые защищают от случайных изменений, но не от преднамеренных, специальных.
- От специальных изменений защищает только ЭП. В отечественных, импортозамещающих ОС должен быть предустановлен соответствующий криптографический механизм.
- Обеспечение импортозамещения иностранных криптографических систем в массовых отечественных, компьютерных технологиях должно быть поставлено как важнейшая государственная задача с соответствующим финансированием и контролем.