конференция
РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто’2024»

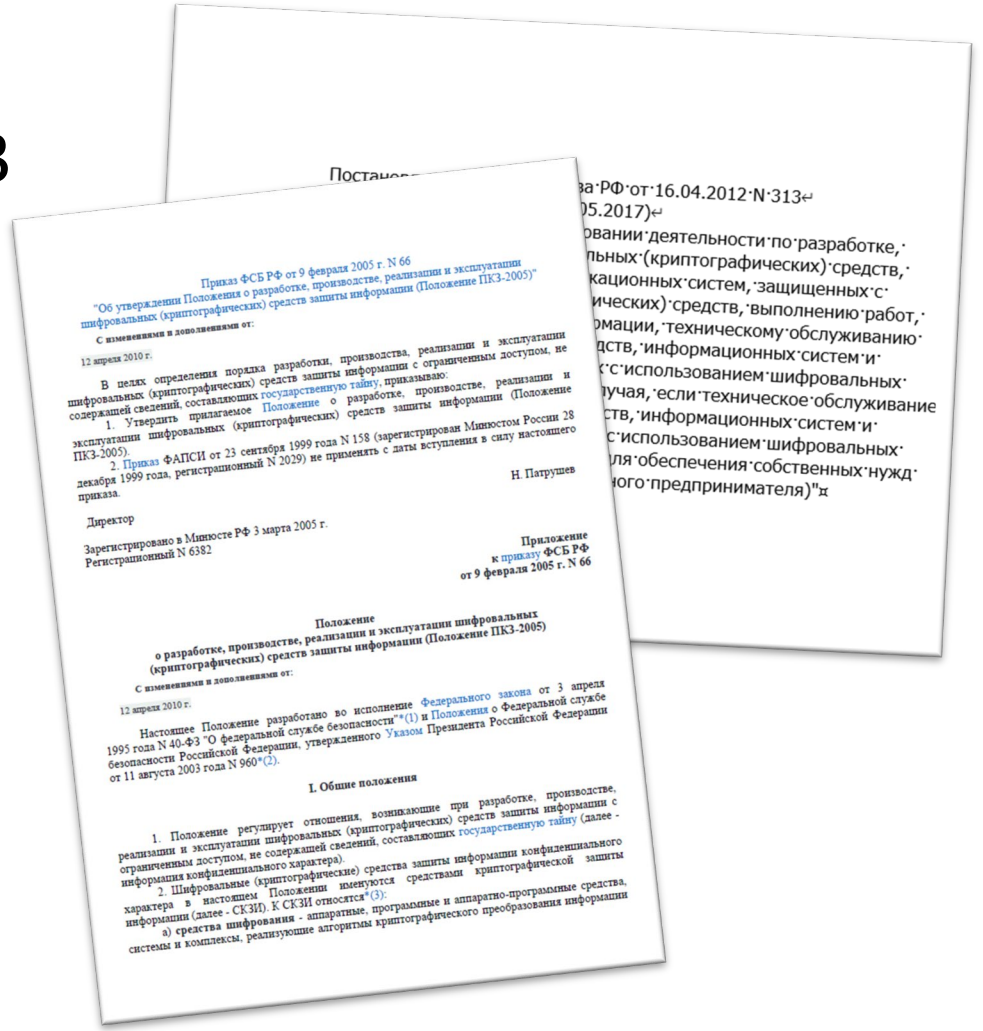
Сценарии, в которых (не) требуются дополнительные исследования при встраивании СКЗИ

Багин Д.В., КриптоПро

Хачатуров А.И., АНСЕР ПРО

Ситуация глазами разработчика

- Постановление правительства №313
  - Получение лицензии
- Положение ПКЗ-2005
  - Исследования кода решения
  - Фиксация кода решения



Приказ ФСБ РФ от 9 февраля 2005 г. N 66
"Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)"

С изменениями и дополнениями от:

12 апреля 2010 г.

В целях определения порядка разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, приказываю:

1. Утвердить прилагаемое Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

2. Приказ ФАПСИ от 23 сентября 1999 года N 158 (зарегистрирован Минюстом России 28 декабря 1999 года, регистрационный N 2029) не применять с даты вступления в силу настоящего приказа.

Н. Патрушев

Директор

Зарегистрировано в Минюсте РФ 3 марта 2005 г.
Регистрационный N 6382

Приложение
к приказу ФСБ РФ
от 9 февраля 2005 г. N 66

Положение
о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)

С изменениями и дополнениями от:

12 апреля 2010 г.

Настоящее Положение разработано во исполнение Федерального закона от 3 апреля 1995 года N 40-ФЗ "О федеральной службе безопасности"*(1) и Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 года N 960*(2).

I. Общие положения

1. Положение регулирует отношения, возникающие при разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее - информация конфиденциального характера).

2. Шифровальные (криптографические) средства защиты информации конфиденциального характера в настоящем Положении именуются средствами криптографической защиты информации (далее - СКЗИ). К СКЗИ относятся*(3):

а) средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации

Какие варианты?

- Возможные сценарии без исследований

  Защита канала (ГОСТ-TLS)

- Возможные сценарии с меньшим контуром объекта исследований

  Создание/проверка ЭП

Сценарии без исследований
Защита канала (ГОСТ-TLS) на стороне клиента

- Яндекс.Браузер
  (Windows|Linux|Mac OS)
- Chromium ГОСТ
  (Windows|Linux|Mac OS|Android)
- Internet Explorer/Microsoft Edge
- Stunnel

Сценарии без исследований
Защита канала (ГОСТ-TLS) на стороне сервера

- Microsoft IIS
- nginx
  (в т.ч. в ОС Astra Linux SE)
- Apache,
  (в т.ч. в ОС Astra Linux SE)
- Apache Tomcat
- Bellsoft Libercat

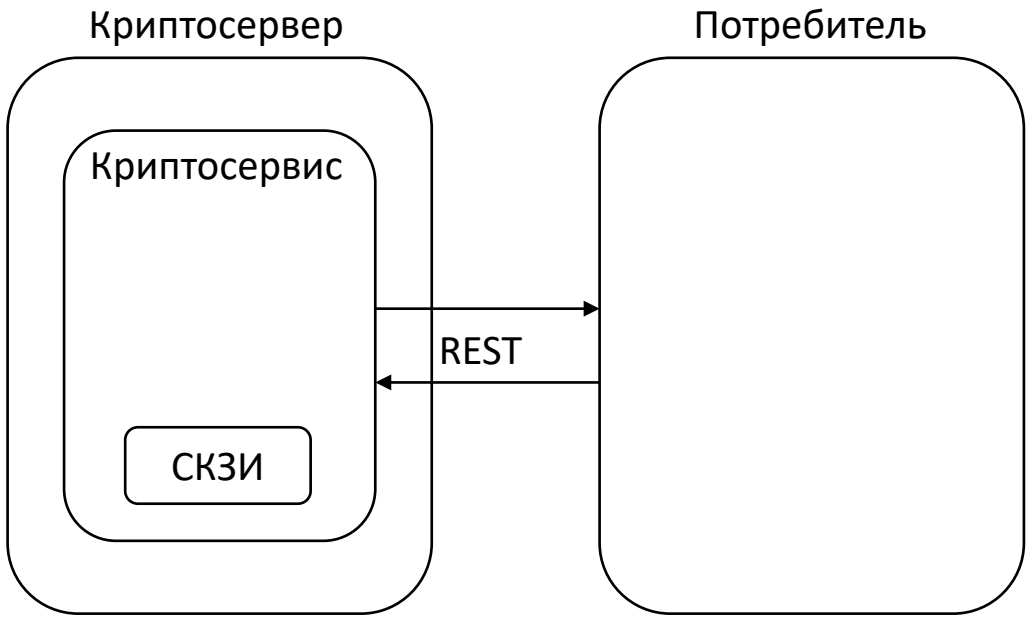
Нюансы:

- использовать можно только версии, прошедшие исследования
- доработки версий возможны, но с учетом существующего цикла сертификации СКЗИ

Подходы, позволяющие упростить выполнение требований к оценке влияния.

Оценка влияния охватывает в прикладной системе потоки данных, защищаемых с использованием криптографических методов.

Ограничиться проведением оценки влияния только для криптобиблиотеки / криптосервиса, являющимися «оберткой» для интерфейса СКЗИ, в общем случае невозможно.



Создание ЭП пользователя

Для компонента, выполняющего создание ЭП пользователя возможно создать интерфейс, не требующий дальнейшей оценки влияния при встраивании данного компонента.

Компоненты, предназначенные для установки на АРМ пользователей, обеспечивающих создание ЭП пользователем, и предусматривающие интеграцию с пользовательским ПО (плагины для браузеров, программные библиотеки, самостоятельные приложения), которые:

- имеют только функцию создания ЭП, но не имеют функции проверки ЭП;
- предназначены для создания ЭП данных в определенны форматах;
- сами имеют (обычно, графический) интерфейс взаимодействия с пользователем, в котором реализованы требования по визуализации процесса создания ЭП (Приказ ФСБ 796, п.8 требований к средствам ЭП): визуализация подписываемых данных, подтверждение пользователем создания ЭП.

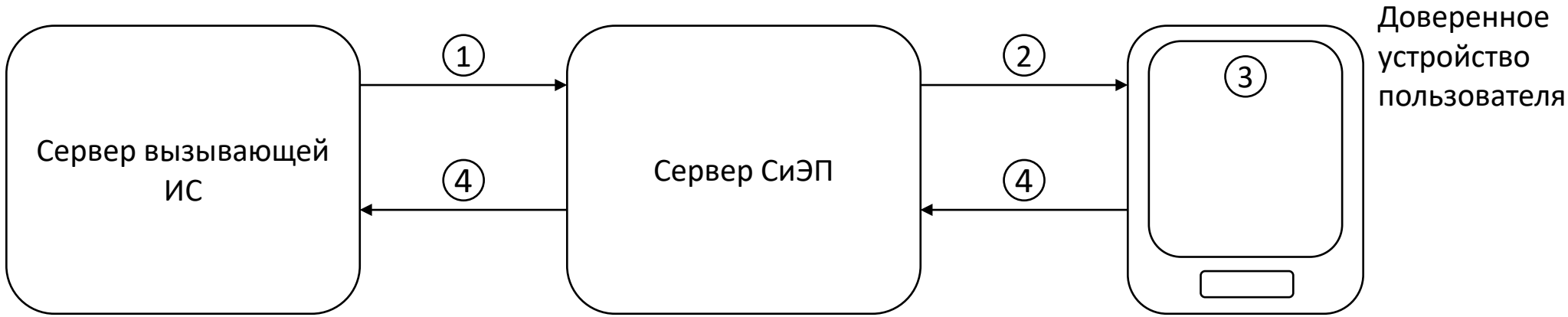
Такая реализация позволяет снять требования по оценке влияния для вызывающего ПО (по крайней мере, для классов КС1, КС2, а в отдельных случаях и для более высокого класса).

Создание ЭП пользователя

Дальнейшее развитие данного подхода при решении той же задачи (создание ЭП пользователем) – системы электронной подписи (СиЭП), интегрируемые с ИС, в которой требуется создавать ЭП пользователя для документов.

1. Вызывающая ИС передает серверу СиЭП документ и идентификатор пользователя, который должен подписать документ.
2. Сервер СиЭП сам связывается обеспечивает передачу документа на устройство пользователя.
3. Пользователь выполняет подписание документа на доверенном устройстве (подписание реализуется с соблюдением всех требований).
4. Подписанный документ / ЭП передается на сервер СиЭП, и далее в вызывающую ИС.

Такая схема также позволяет избежать проведения оценки влияния для ПО вызывающей ИС, а также в вызывающей ИС не требуется заниматься выдачей пользователям ключей/сертификатов.



Проверка ЭП

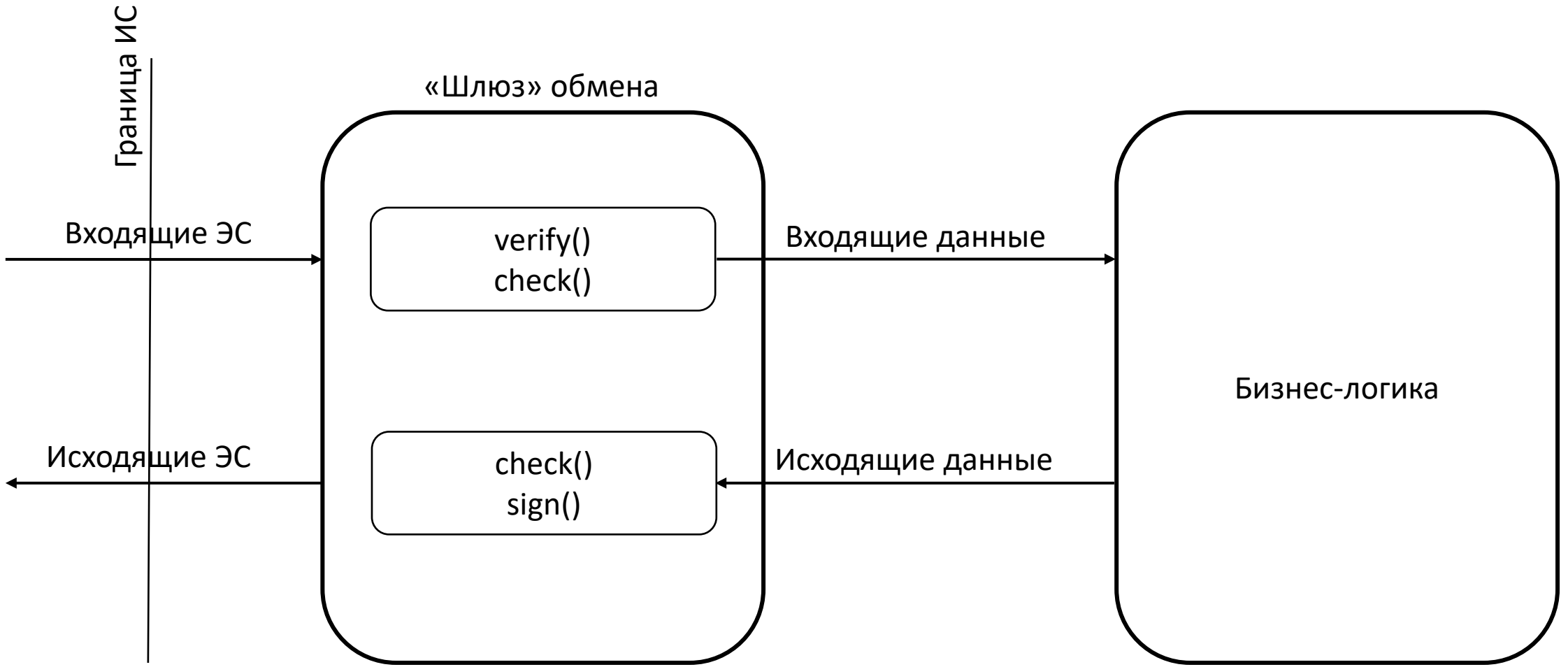
Задача усложняется, т. к. требуется, чтобы при оценке влияния оценивались все точки в прикладном ПО, где принимаются решения в зависимости от корректности и некорректности ЭП.

Создание и проверка ЭП

Если идет обмен криптографически защищенным сообщениями с «внешним миром», можно выделить шлюз обмена, который стоит в разрыве между компонентами, реализующими прикладной бизнес-функционал и внешними сервисами. Шлюз должен:

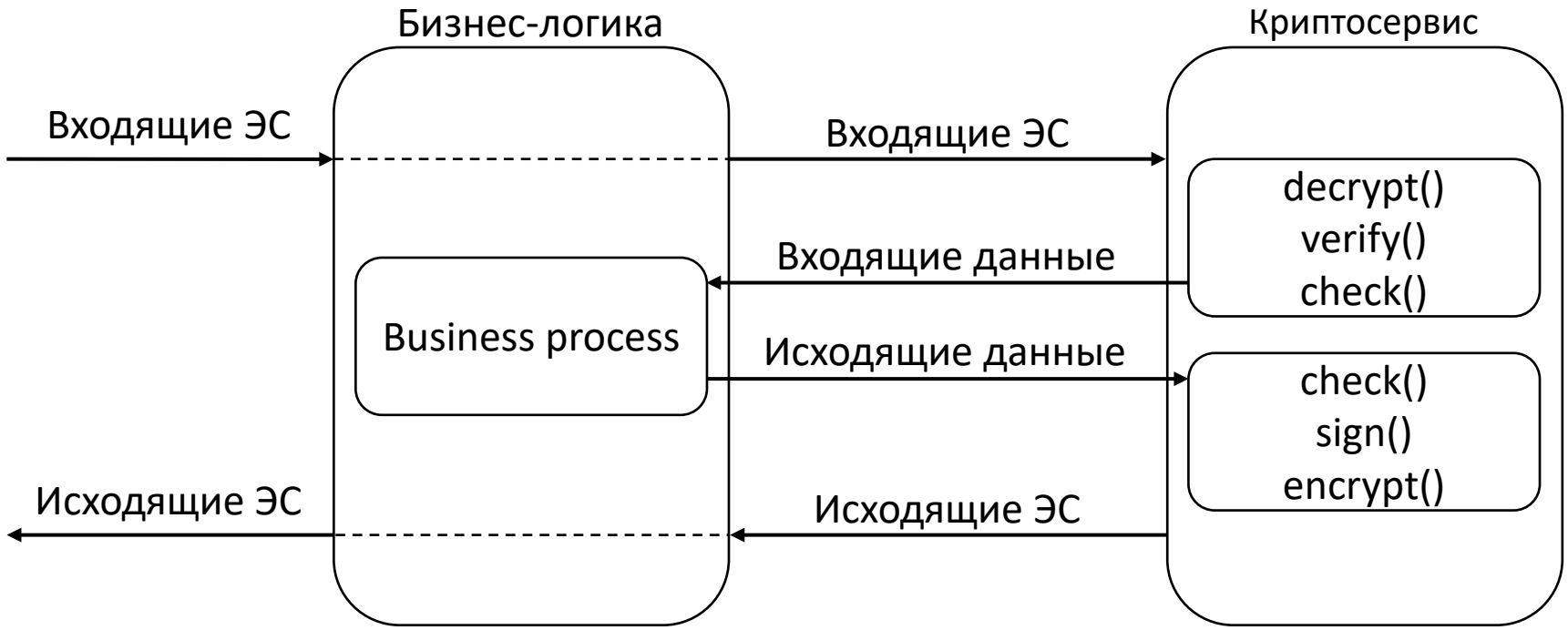
- самостоятельно вести сетевой обмен;
- защищать (выполнять форматно-логический контроль и подписывать) исходящие сообщения;
- валидировать (выполнять проверку ЭП, форматно-логический контроль) входящие сообщения;

Компоненты, реализующие прикладной бизнес-функционал вообще не должны получать сообщения, не прошедшие проверку. Такая архитектура позволяет проводить оценку влияния только для ПО шлюза обмена и дает возможность не фиксировать компоненты, реализующие прикладной бизнес-функционал.


Граница ИС
«Шлюз» обмена
Входящие ЭС
verify()
check()
Входящие данные
Бизнес-логика
Исходящие ЭС
check()
sign()
Исходящие данные

Создание и проверка ЭП с шифрованием

Альтернативой шлюзу, стоящему "в разрыве" является применение протокола, в котором передаваемые сообщения не только защищены ЭП, но и зашифрованы. В этом случае у используемого условного криптосервиса должна быть только общая функция валидации, которая предусматривает сразу и расшифрование, и проверку ЭП, и форматно-логический контроль сообщения. Если в процессе возникают любые ошибки, то в прикладное ПО данные не возвращаются.



Уточнение требований регуляторами

Регуляторы в различных сферах работают совместно с ФСБ России чтобы для отдельных классов продуктов разработать индивидуальные подходы к сертификации / оценке влияния.

Стандартизация

Ведущие компании в области криптографии (в том числе компания «КРИПТО-ПРО») много уже сделали и продолжают делать для стандартизации протоколов и схем применения российских криптографических алгоритмов, что позволяет уже в настоящее время совместно использовать решения разных вендоров и создает возможности для массового применения криптографии.

Вопросы

???