«Подводные камни» сертификации блокчейн-решений

Елистратов Андрей, Маршалко Григорий

- *«Фундаментальной проблемой некоторых блокчейн-решений является то, что за основу берется идея о том, что транзакции без доверия – это хорошо»*.

Джон Вундерлих, Совет по стандартам Канады

Доверие

- Необходимым условием безопасного и эффективного функционирования информационных систем является обеспечение доверия к ним.
- В соответствии с ГОСТ 54581-2011 «Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к ИТ» под доверием понимается выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности.

Сертификация СЗИ

Сертификация

- ФСТЭК России

В случаях отсутствия необходимости применения криптографических средств для защиты информации, подлежащей обязательной защите.

- ФСБ России

В случаях применения криптографических средств относящихся к сфере компетенции ФСБ России.

- Банк России

В случаях использования блокчейн-решений в финансовом секторе.

Сертификация криптографических средств (СКЗИ)

- ФСБ России

В случаях применения криптографических средств относящихся к сфере компетенции ФСБ России.

- Банк России

В случаях использования блокчейн-решений в финансовом секторе.

Сертификация Банком России

- Указание Банка России от 10 декабря 2015 г. № 3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».
- Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

В данных документах указывается, в каких случаях следует использовать средства криптографической защиты информации, прошедшие оценку соответствия требованиям по информационной безопасности ФСБ России.

Сертификация в ФСБ России обязательна (Положение ПКЗ-2005)

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в государственных органах Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в организациях, выполняющих государственные заказы;

Сертификация в ФСБ России обязательна (Положение ПКЗ-2005)

- если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации;
- при обрабатывании информации конфиденциального характера (криптографическим способом), обладателем которой являются государственные органы или организации, выполняющие государственные заказы;
- при обрабатывании информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации.

Сертификация в ФСБ России обязательна (Положение ПКЗ-2005)

В частности при применении СКЗИ для:

- Защиты информации в государственных информационных системах (ГИС).
- Защита персональных данных и другой информации подлежащей обязательной защите.
- Формирование/проверка квалифицированной ЭП.
- В случаях определенных Банком России

Приказ ФСБ РФ от 9.02.2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005)

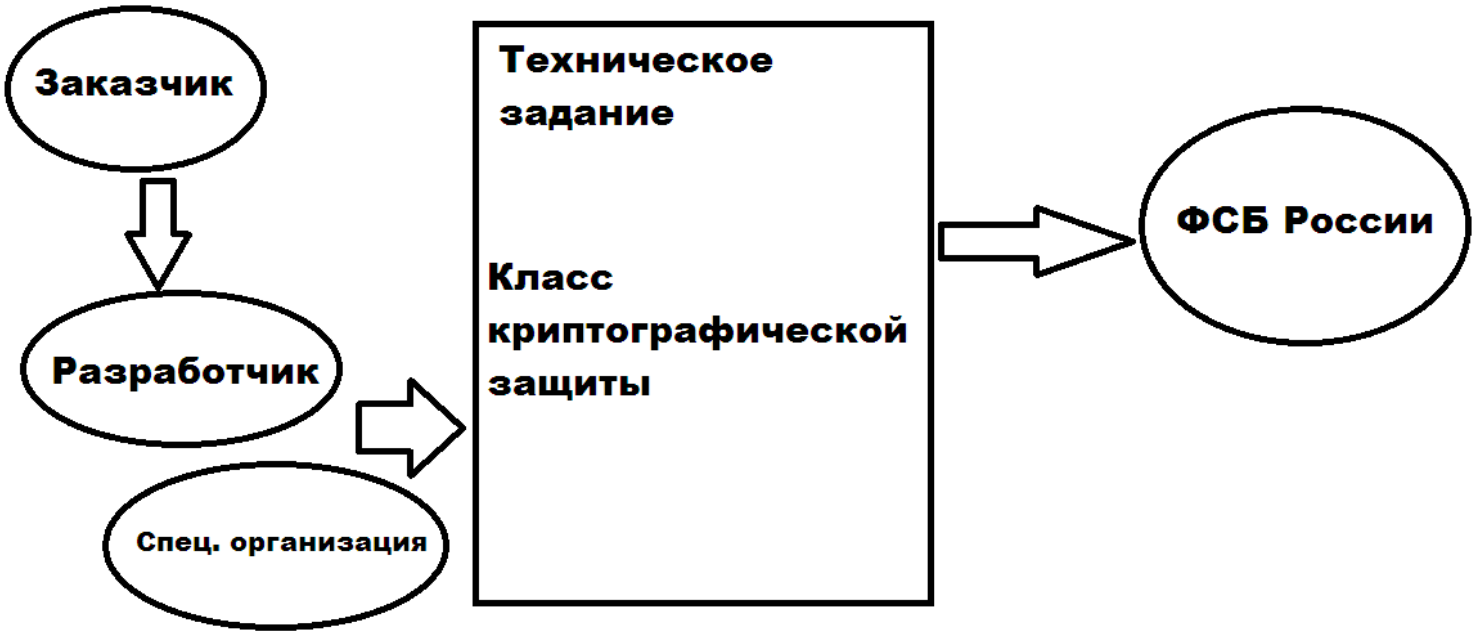
- Описан порядок действий при:

разработке СКЗИ,

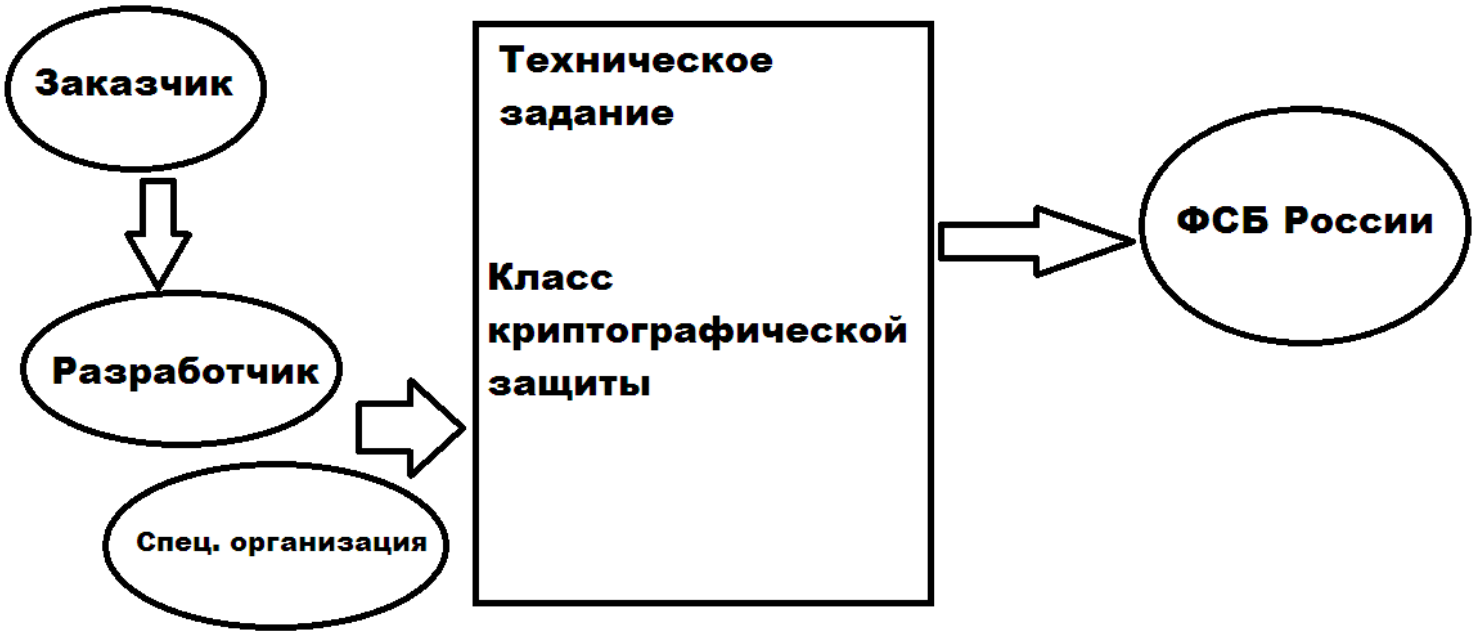
производстве СКЗИ,

эксплуатации СКЗИ.

Перед разработкой СКЗИ обязательно согласование технического задания на разработку с ФСБ России



Для определения в ТЗ класса криптографической защиты надо выбрать адекватную разрабатываемому решению модель угроз и нарушителя.



Модель угроз и нарушителя.

- Приказ ФСБ России от 27 декабря 2011 года № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».
- Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных …»
- Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации»

Модель угроз и нарушителя.

В частности рекомендации Р 1323565.1.012-2017 приведен детальный перечень угроз для каждого из пяти классов криптографической информации:

КС1, КС2, КС3, КВ, КА.

Для определения требуемого класса криптографической необходимо провести анализ предполагаемых условий эксплуатации СКЗИ и оценить возможность появления тех или иных угроз безопасности – построить модель угроз, которая ляжет в основу технического задания.

Построение модели угроз и нарушителя для блокчейн-решения

При составлении модели угроз информацией о реализуемой бизнес-логике могут быть сведения о функциях, выполняемых субъектами системы, их права, которые, в свою очередь и определяют возможный спектр угроз:

- Может ли нарушитель являться администратором/привилегированным пользователем блокчейн-решения .
- Может ли нарушитель являться пользователем блокчейн-решения .
- Есть ли у нарушителя возможности (в том числе и потенциальные) влиять на работу (как удаленные так и локальные) модели блокчейн-решения в целом.

Построение модели угроз и нарушителя для блокчейн-решения

Также при построении модели угроз и нарушителя необходимо ответить на следующие вопросы:

- Является ли информация, обрабатываемая в блокчейн-решении , конфиденциальной.
- Нужна ли юридическая значимость совершенных в блокчейн-решении действий.
- Можно ли воспользоваться для обработки информации в блокчейн-решении уже готовым криптографическим модулем.

Почему блокчейн-решения в разрезе классификации ФСБ России относятся к СКЗИ

У любого сертифицированного СКЗИ в правилах пользования зафиксирован набор его целевых функций:

- функция шифрования (обеспечение конфиденциальности информации);
- функция формирования и/или проверки электронной подписи;
- функция имитозащиты (обеспечение контроля целостности информации и проверки авторства);
- функция аутентификации (локальная/удаленная, обеспечение авторизованного доступа к функциям СКЗИ или защищаемой информации персонифицированного (одного) пользователя или процесса).
- другие функции…

Почему блокчейн-решения в разрезе классификации ФСБ России относятся к СКЗИ

Блокчейн-решение формирует качественно новую сущность – достижение консенсуса при реализации *протокола взаимодействия* между участниками информационного обмена, доверие к которому формируется за счет использования *криптографических атомарных запросов*.

Алгоритм достижения консенсуса/смарт-контракт - криптографический протокол.

Новый криптографический протокол -

новое СКЗИ .

Объективная оценка времени сертификации

- Согласование ТЗ с ФСБ России (в случае отсутствия замечаний) – до 1 месяца.
- При проведении тематических исследований Вашего решения специализированной организацией часто требуется его доработка .
- Экспертиза отчетных материалов тематических исследований (после получения всех отчетных материалов) – до 2 месяцев.

Объективная оценка времени сертификации

- Проведение тематических исследований блокчейн-решения специализированной организацией не является типичным/типовым.
- Для упрощения анализа уже на этапе проектирования системы желательно заранее представить разрабатываемое ПО в виде функционально законченных модулей.

Понимание объекта сертификации

- Сертификация по требованием ФСБ России библиотеки, реализующей некоторый блокчейн-сервис, - невозможна.
- Смарт-контракты и интерпретаторы их языков программирования требуют особого внимания при проведении исследований.

«Подводные камни» сертификации блокчейн-решений

- Блокчейн-решение это СКЗИ.
- Если ГИС или обрабатываемые данные подлежат обязательной защите – ПКЗ-2005.
- Разработка СКЗИ – лицензируемый вид деятельности.
- Описание модели угроз и нарушителя позволяет смягчить или конкретизировать требования к используемым в блокчейн-решении СКЗИ, снизив расходы на создание/сертификацию решения.
- В ТЗ обязательно точно определить объект сертификации.
- Реалистично оценивать время.

Блокчейн-решение - это набор исходных текстов и скомпилированных модулей со всеми вытекающими проблемами в области информационной безопасности…

Спасибо за внимание!