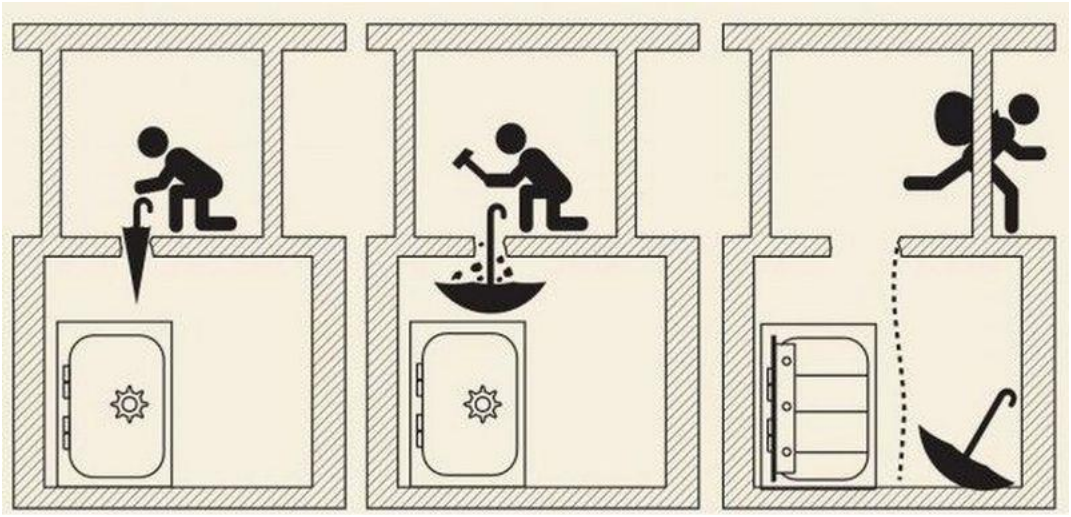
Информационная безопасность банковских безналичных платежей. Части 7 и 8 — Базовая и типовые модели угроз



АНОТАЦИЯ

В данной статье будет рассмотрена модель угроз информационной безопасности банковских безналичных платежей.

Модель угроз разделена на два слоя:

1. **Базовая модель угроз** формализует связь бизнес-требований с угрозами ИБ.
2. Набор **типовых моделей угроз,** описывающих низкоуровневые угрозы ИБ, на которые ссылается базовая модель.

Угрозы, представленные здесь, справедливы практически для любого банка в Российской Федерации, а также для любых других организаций, использующих для осуществления расчетов толстые клиенты с криптографическим подтверждением платежей.

Настоящая модель угроз предназначена для обеспечения практической безопасности и формирования внутренней документации банков в соответствии с требованиями Положений Банка России № 552-П от 24 августа 2016 г. и № 382-П от 9 июня 2012 г.

ОГЛАВЛЕНИЕ

АНОТАЦИЯ 1
МЕТОДИКА МОДЕЛИРОВАНИЯ 3
Структура модели угроз 3
Методика формирования модели угроз 4
Порядок применения данной модели угроз к реальным объектам 5
Особенности оформления модели угроз 5
БАЗОВАЯ МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКИХ БЕЗНАЛИЧНЫХ ПЛАТЕЖЕЙ 6
Объект защиты, для которого применяется модель угроз (scope) 6
Архитектура 6
Ограничения модели 6
Угрозы безопасности верхнего уровня 7
У1. Прекращение функционирования системы безналичных переводов 7
У2. Кража денежных средств в процессе функционирования системы безналичных переводов 9
ТИПОВАЯ МОДЕЛЬ УГРОЗ. СЕТЕВОЕ СОЕДИНЕНИЕ 15
Объект защиты, для которого применяется модель угроз (scope) 15
Архитектура 15
Угрозы безопасности верхнего уровня 16
У1. Несанкционированное ознакомление с передаваемыми данными 16
У2. Несанкционированная модификация передаваемых данных 16
У3. Нарушение авторства передаваемых данных 17
ТИПОВАЯ МОДЕЛЬ УГРОЗ. ИНФОРМАЦИОННАЯ СИСТЕМА, ПОСТРОЕННАЯ НА БАЗЕ АРХИТЕКТУРЫ КЛИЕНТ-СЕРВЕР 18
Объект защиты, для которого применяется модель угроз (scope) 18
Угрозы безопасности верхнего уровня 18
У1. Совершение злоумышленниками несанкционированных действий от имени легитимного пользователя 19
У2. Несанкционированная модификация защищаемой информации во время ее обработки серверной частью информационной системы 20
ТИПОВАЯ МОДЕЛЬ УГРОЗ. СИСТЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА 21
Объект защиты, для которого применяется модель угроз (scope) 21
Угрозы безопасности верхнего уровня 22
У1. Несанкционированное установление сеанса работы от имени легального пользователя 22

У2. Несанкционированное повышение привилегий пользователя в информационной системе 24
ТИПОВАЯ МОДЕЛЬ УГРОЗ. МОДУЛЬ ИНТЕГРАЦИИ 25
Объект защиты, для которого применяется модель угроз (scope) 25
Архитектура 25
Примеры модулей интеграции 26
Угрозы безопасности верхнего уровня 29
У1. Внедрение злоумышленниками подложной информации через модуль интеграции 29
ТИПОВАЯ МОДЕЛЬ УГРОЗ. СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ 29
Объект защиты, для которого применяется модель угроз (scope) 29
Архитектура 30
Особенности проверки корректности электронной подписи 32
Допущения, принятые при описании объекта защиты 33
Пример информационной системы, защищенной с помощью СКЗИ 34
Угрозы безопасности верхнего уровня 37
У1. Компрометация закрытых криптографических ключей 38
У2. Зашифрование подложных данных от имени легитимного отправителя 39
У3. Расшифрование зашифрованных данных лицами, не являющимися легитимными получателями данных (злоумышленниками) 39
У4. Создание электронной подписи легитимного подписанта под подложными данными 39
У5. Получение положительного результата проверки электронной подписи подложных данных 40
У6. Ошибочное принятие электронных документов к исполнению вследствие проблем в организации электронного документооборота. 41
У7. Несанкционированное ознакомление с защищаемыми данными во время их обработки СКЗИ 42
Примеры атак 42

МЕТОДИКА МОДЕЛИРОВАНИЯ

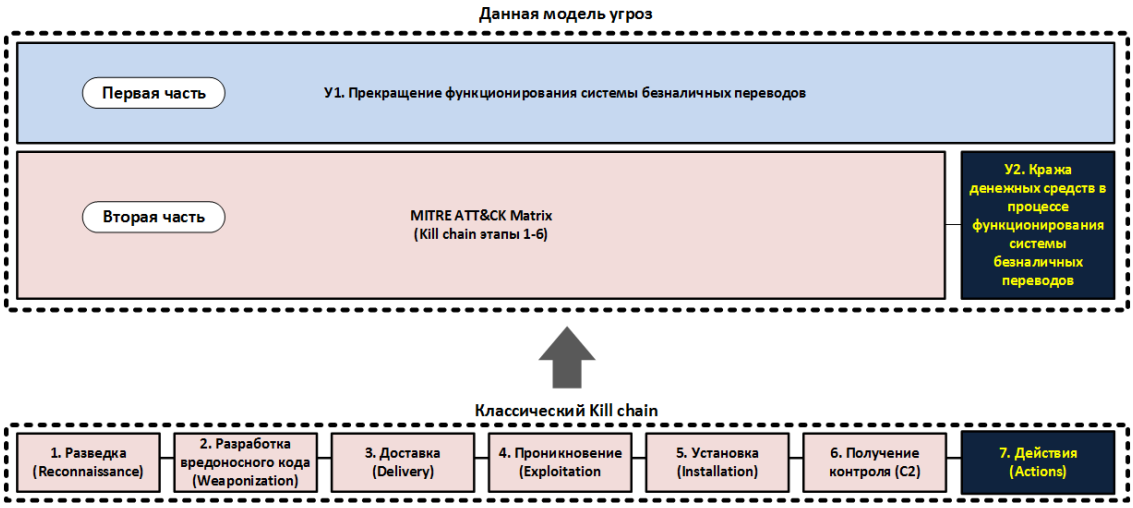
Структура модели угроз

Одним из наиболее удачных на сегодняшний день способов моделирования компьютерных атак является Kill chain. Данный способ представляет компьютерную атаку как последовательность этапов, выполняемую злоумышленниками для достижения поставленных ими целей.

Описание большинства этапов приведено в MITRE ATT&CK Matrix, но в ней нет расшифровки конечных действий — «Actions» (последнего этапа Kill chain), ради которых злоумышленники осуществляли атаку и которые, по сути, и являются кражей денег у банка. Другой проблемой применения классического Kill chain для моделирования угроз является отсутствие в нем описания угроз, связанных с доступностью.

Данная модель угроз призвана компенсировать эти недостатки. Для этого она формально будет состоять из двух частей:

- Первая будет описывать проблемы, связанные с доступностью.
- Вторая, представляющая собой классический Kill chain с расшифрованным последним этапом, будет описывать «компьютерную» кражу денег у банка.



Методика формирования модели угроз

Основными требованиями к создаваемой модели угроз были:

- сохранение компактности и минимизация дублирования,
- полнота идентификации угроз и простота уточнения модели,
- обеспечение возможности работы с моделью как бизнес-специалистам, так и техническим работникам.

Для реализации поставленных задач модель строилась на базе методики «дерево угроз», в которую были внесены небольшие улучшения:

1. Угрозы описывались, начиная с бизнес-уровня, и постепенно декомпозировались на технические составляющие.
2. Угрозы, свойственные типовым элементам информационной инфраструктуры (например, сетевым соединениям, системам криптографической защиты информации, ...) группировались в типовые модели угроз.
3. Далее при моделировании угроз, свойственных типовым элементам информационной инфраструктуры, вместо дублирования описания угроз давалась ссылка на соответствующую типовую модель.

Порядок применения данной модели угроз к реальным объектам

Применение данной модели угроз к реальным объектам следует начинать с уточнения описания информационной инфраструктуры, а затем, в случае необходимости, провести более детальную декомпозицию угроз.

Порядок актуализации угроз, описанных в модели, следует проводить в соответствии с внутренними документами организации. В случае отсутствия таких документов их можно разработать на базе методик, рассмотренных в предыдущей статье исследования.

Особенности оформления модели угроз

В данной модели угроз приняты следующие правила оформления:

1. Модель угроз представляет собой дерево угроз. Дерево угроз записывается в виде иерархического списка, где каждый элемент списка соответствует узлу дерева и соответственно определенной угрозе.
2. Наименование угрозы начинается с идентификатора угрозы, который имеет вид: **У<Код угрозы>**
   где «У» — сокращение от угроза, «Код угрозы» — номер угрозы в иерархическом списке (дереве угроз).
3. Описание угрозы может содержать в себе два блока:
   - **Пояснения** содержат разъяснения к описываемой угрозе. Здесь могут приводиться примеры реализации угрозы, объяснение решений, принятых во время декомпозиции, ограничения по моделированию и другая информация.
   - **Декомпозиция** содержит иерархический список дочерних угроз.
4. При декомпозиции угроз по умолчанию считается, что реализация хотя бы одной дочерней угрозы приводит к реализации родительской угрозы. Если реализация родительской угрозы зависит от реализации дочерних угроз другим образом, то при декомпозиции в конце строки, описывающей родительский элемент, обозначается тип зависимости:
   - (**И**) – реализация родительской угрозы происходит только при реализации всех дочерних угроз.
   - (**Сценарий**) – реализация родительской угрозы происходит при некотором определенном сценарии или алгоритме реализации дочерних угроз.
5. Ссылки на угрозы, описанные в этой же или других моделях угроз, оформляются по шаблону: **Ссылка: «<Наименование модели угроз>.<Наименование угрозы>**».
6. Если наименование дочерней угрозы начинается с <...>, то это означает, что при чтении вместо <...> необходимо полностью вставить наименование родительской угрозы.

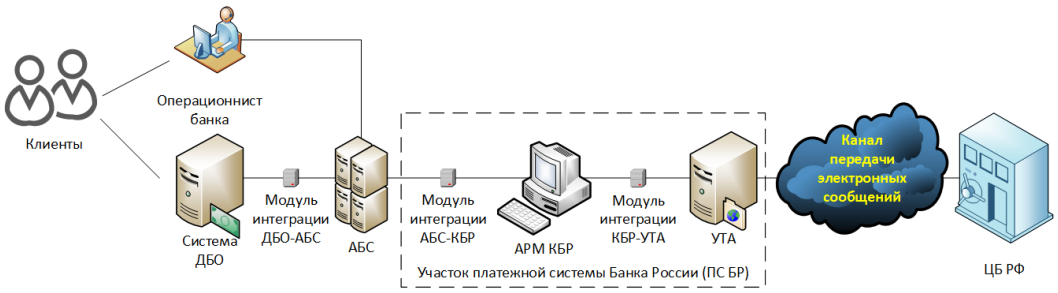
БАЗОВАЯ МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКИХ БЕЗНАЛИЧНЫХ ПЛАТЕЖЕЙ

Объект защиты, для которого применяется модель угроз (scope)

Область действия настоящей модели угроз распространяется на процесс безналичных переводов денежных средств через платежную систему Банка России.

Архитектура

В зону действия модели входит следующая информационная инфраструктура:



Здесь:
«Участок платежной системы Банка России (ПС БР)» — участок информационной инфраструктуры, подпадающий под действие требований Положения Банка России от 24 августа 2016 г. № 552-П. Критерий отнесения информационной инфраструктуры к участку ПС БР — обработка на объектах информационной инфраструктуры электронных сообщений в формате УФЭБС.

«Канал передачи электронных сообщений» включает в себя канал связи банка с ЦБ РФ, построенный через специализированного оператора связи или модемное соединение, а так же механизм обмена электронными сообщениями, функционирующий с помощью курьера и отчуждаемых машинных носителей информации (ОМНИ).

Перечень помещений, входящих в зону действия модели угроз, определяется по критерию наличия в них объектов информационной инфраструктуры, участвующих в осуществлении переводов денежных средств.

Ограничения модели

Настоящая модель угроз распространяется только на вариант организации платежной инфраструктуры с АРМ КБР, совмещающим в себе функции шифрования и электронной подписи, и не рассматривает случая использования АРМ КБР-Н, где электронная подпись осуществляется «на стороне АБС».

Угрозы безопасности верхнего уровня

Декомпозиция

У1. Прекращение функционирования системы безналичных переводов.

У2. Кража денежных средств в процессе функционирования системы безналичных переводов.

У1. Прекращение функционирования системы безналичных переводов

Пояснения

Потенциальный ущерб от реализации данной угрозы можно оценить на основании следующих предпосылок:

- В договорах обслуживания банковского счета, заключенных между клиентами и банком, как правило, присутствует отметка о том, в течение какого времени банк обязан исполнить платеж. Нарушение указанных в договоре сроков влечет ответственность банка перед клиентом.
- Если банк неожиданно прекратит исполнять платежи, то это вызовет вопросы о его финансовой стабильности, и, как следствие, может спровоцировать массовый отток депозитов.
- Непрерывность осуществления платежей является одним из условий сохранения лицензии на банковскую деятельность. Систематические отказы и сбои могут породить серьезные вопросы к банку со стороны ЦБ РФ и привести к отзыву лицензии.

В общем случае максимально допустимой задержкой исполнения платежа можно считать один рейс в течение операционного дня. Дальнейшее увеличение задержки будет приводить ко все большему ущербу для банка.

При декомпозиции данной угрозы учитывались следующие документы:

- Каталог угроз BSI Threat catalogue.
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009. Обеспечение информационной безопасности организаций банковской системы Российской Федерации.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Декомпозиция

У1.1. Проблемы с оборудованием или носителями информации, используемыми в осуществлении переводов:

У1.1.1. Отказы и сбои.

У1.1.2. Кража.

У1.1.3. Утрата.

У1.2. Уничтожение программ или данных, необходимых для осуществления переводов.

У1.3. Совершение злоумышленниками атак, направленных на отказ в обслуживании (DoS, DDoS) технических средств и каналов связи, используемых для осуществления переводов.

У1.4. Невозможность обмена электронными сообщениями с платежной системой ЦБ РФ (**И**):
У1.4.1. <...>, осуществляемого через сетевые соединения:
У1.4.1.1. Неработоспособность каналов связи с ЦБ РФ (**И**):
У1.4.1.1.1. <...>, предоставляемых специализированным оператором связи.
У1.4.1.1.2. <...>, организованных как модемное соединение.
У1.4.1.2. Прекращение действия информации, используемой для аутентификации сетевого соединения с ЦБ РФ.

У1.4.2. <...>, осуществляемого с помощью курьера на отчуждаемых машинных носителях информации (ОМНИ):
У1.4.2.1. Отсутствие должным образом оформленных документов:
У1.4.2.1.1 <...>, подтверждающих полномочия курьера.
У1.4.2.1.2 <...>, сопровождающих платежи на ОМНИ.

У1.5. Прекращения действия криптографических ключей, используемых для защиты электронных сообщений:
У1.5.1. Окончание сроков действия криптографических ключей.
У1.5.2. Компрометация криптографических ключей.
У1.5.3. Провокация злоумышленниками удостоверяющего центра ЦБ РФ на блокирование действия криптографических ключей банка.

У1.6. Отсутствие на рабочем месте лиц, участвующих в осуществлении безналичных платежей.

У1.7. Использование устаревших версий программного обеспечения, применяемого для осуществления безналичных переводов.

У1.8. Возникновение в помещениях условий, при которых невозможно нормальное функционирование технических средств, каналов связи и персонала, участвующих в переводах:
У1.8.1. Отсутствие электропитания.
У1.8.2. Существенные нарушения температурного режима (перегрев, переохлаждение).
У1.8.3. Пожар.
У1.8.4. Затопление помещения.
У1.8.5. Обрушение или угроза обрушения помещений.
У1.8.6. Вооруженное нападение.
У1.8.7. Радиоактивное или химическое заражение.
У1.8.8. Сильные электромагнитные помехи.
У1.8.9. Эпидемии.

У1.9. Административное прекращение доступа в здания или помещения, в которых расположена информационная инфраструктура, используемая для осуществления платежей:
У1.9.1. Блокирование доступа со стороны органов власти:
У1.9.1.1. Проведение обысков или других оперативно-следственных мероприятий.
У1.9.1.2. Проведение культурно-массовых мероприятий, религиозных праздников и т.д.
У1.9.2. Блокирование доступа со стороны собственника:
У1.9.2.1. Конфликт хозяйствующих субъектов.

У1.10. Действие обстоятельств непреодолимой силы (стихийные бедствия, катастрофы, массовые беспорядки, теракты, военные действия, зомбиапокалипсис, ...).

У2. Кража денежных средств в процессе функционирования системы безналичных переводов

Пояснения

Кража денежных средств в процессе функционирования системы безналичных переводов представляет собой кражу безналичных денежных средств с их последующим или одновременным выводом из банка-жертвы.

Кража безналичных денежных средств представляет собой несанкционированное изменение остатка на счете клиента или банка. Данные изменения могут произойти в результате:

- нештатного изменения остатка на счете;
- несанкционированного внутрибанковского или межбанковского перевода денежных средств.

Нештатным изменением остатка на счете будем назвать не регламентированные внутренней документацией банка действия, в результате которых произошло несанкционированное уменьшение или увеличение остатка на банковском счете. Примерами подобных действий могу быть: проведение фиктивной банковской проводки, непосредственное изменение остатка в месте хранения (например, в базе данных) и другие действия.

Нештатное изменение остатка на счете, как правило, сопровождается штатными операциями по расходованию украденных денежных средств. К подобным операциям можно отнести:

- обналичивание денег в банкоматах банка-жертвы,
- осуществления переводов денежных средств на счета, открытые в других банках,
- совершения онлайн-покупок,
- и т.д.

Несанкционированный перевод денежных средств — это перевод, осуществленный без согласия лиц, правомочно распоряжающихся денежными средствами и, как правило, совершенный путем исполнения банком поддельного распоряжения о переводе денежных средств.

Формирование поддельных распоряжений о переводе денежных средств может производиться как по вине клиентов, так и по вине банка. В настоящей модели угроз будут рассмотрены только угрозы, находящиеся в зоне ответственности банка. В качестве распоряжений о переводах денежных средств в данной модели будут рассматриваться только платежные поручения.

В общем случае можно считать, что обработка банком внутрибанковских переводов является частным случаем обработки межбанковских переводов, поэтому для сохранения компактности модели далее будут рассматривать только межбанковские переводы.

Кража безналичных денежных средств может производиться как при исполнении исходящих платежных поручений, так и при исполнении входящих платежных поручений. При этом

исходящим платежным поручением будем называть платежное поручение, направляемое банком в платежную систему Банка России, а входящим будем называть платежное поручение, поступающие в банк из платежной системы Банка России.

Декомпозиция

У2.1. Исполнение банком поддельных исходящих платежных поручений.

У2.2. Исполнение банком поддельных входящий платежных поручений.

У2.3. Нештатное изменение остатков на счете.

У2.1. Исполнение банком поддельных исходящих платежных поручений

Пояснения

Основной причиной, из-за которой банк может исполнить поддельное платежное поручение является его внедрение злоумышленниками в бизнес-процесс обработки платежей.

Декомпозиция

У2.1.1. Внедрение злоумышленниками поддельного исходящего платежного поручения в бизнес-процесс обработки платежей.

У2.1.1. Внедрение злоумышленниками поддельного исходящего платежного поручения в бизнес-процесс обработки платежей

Пояснения

Декомпозиция данной угрозы будет производиться по элементам информационной инфраструктуры, в которых может произойти внедрение поддельного платежного поручения.

Элементы	Декомпозиция угрозы «У2.1.1. Внедрение злоумышленниками поддельного исходящего платежного поручения в бизнес-процесс обработки платежей»
Операционист банка	У2.1.1.1.
Сервер ДБО	У2.1.1.2.
Модуль интеграции ДБО-АБС	У2.1.1.3.
АБС	У2.1.1.4.
Модуль интеграции АБС-КБР	У2.1.1.5.
АРМ КБР	У2.1.1.6.
Модуль интеграции КБР-УТА	У2.1.1.7.
УТА	У2.1.1.8.
Канал передачи электронных сообщений	У2.1.1.9.

Декомпозиция

У2.1.1.1. <...> в элементе «Операционист банка».

У2.1.1.2. <...> в элементе «Сервер ДБО».

У2.1.1.3. <...> в элементе «Модуль интеграции ДБО-АБС».

У2.1.1.4. <...> в элементе «АБС».

У2.1.1.5. <...> в элементе «Модуль интеграции АБС-КБР».

У2.1.1.6 .<...> в элементе «АРМ КБР».

У2.1.1.7 .<...> в элементе «Модуль интеграции КБР-УТА».

У2.1.1.8. <...> в элементе «УТА».

У2.1.1.9. <...> в элементе «Канал передачи электронных сообщений».

У2.1.1.1. <...> в элементе «Операционист банка»

Пояснения
Операционист при приеме бумажного платежного поручения от клиента заносит на его основании электронный документ в АБС. Подавляющее большинство современных АБС основано на архитектуре клиент-сервер, что позволяет произвести анализ данной угрозы на базе типовой модели угроз клиент-серверных информационных систем.

Декомпозиция
У2.1.1.1.1. Операционист банка принял от злоумышленника, представившегося клиентом банка, поддельное платежное поручение на бумажном носителе.
У2.1.1.1.2. От имени операциониста банка в АБС внесено поддельное электронное платежное поручение.
У2.1.1.1.2.1. Операционист действовал по злому умыслу или совершил непреднамеренную ошибку.
У2.1.1.1.2.2. От имени операциониста действовали злоумышленники:
У2.1.1.1.2.2.1. Ссылка: «Типовая модель угроз. Информационная система, построенная на базе архитектуры клиент-сервер. У1. Совершение злоумышленниками несанкционированных действий от имени легитимного пользователя».

У2.1.1.2. <...> в элементе «Сервер ДБО»

Декомпозиция
У2.1.1.2.1. Сервер ДБО принял от имени клиента должным образом заверенное платежное поручение, но составленное злоумышленниками без согласия клиента:
У2.1.1.2.1.1. Ссылка: «Типовая модель угроз. Информационная система, построенная на базе архитектуры клиент-сервер. У1. Совершение злоумышленниками несанкционированных действий от имени легитимного пользователя».
У2.1.1.2.2. Злоумышленники внедрили в сервер ДБО поддельное платежное поручение:
У2.1.1.2.2.1. Ссылка: «Типовая модель угроз. Информационная система, построенная на базе архитектуры клиент-сервер. У2. Несанкционированная модификация защищаемой информации во время ее обработки серверной частью информационной системы».

У2.1.1.3. <...> в элементе «Модуль интеграции ДБО-АБС»

Декомпозиция
У2.1.1.3.1. Ссылка: «Типовая модель угроз. Модуль интеграции. У1. Внедрение злоумышленниками подложной информации через модуль интеграции».

У2.1.1.4. <...> в элементе «АБС»

Декомпозиция
У2.1.1.4.1. Ссылка: «Типовая модель угроз. Информационная система, построенная на базе архитектуры клиент-сервер. У2. Несанкционированная модификация защищаемой информации во время ее обработки серверной частью информационной системы».

У2.1.1.5. <...> в элементе «Модуль интеграции АБС-КБР»

Декомпозиция
У2.1.1.5.1. Ссылка: «Типовая модель угроз. Модуль интеграции. У1. Внедрение злоумышленниками подложной информации через модуль интеграции».

У2.1.1.6. <...> в элементе «АРМ КБР»

Пояснения
Основной функцией АРМ КБР с точки зрения информационной безопасности является криптографическая защита электронных сообщений, которыми банк обменивается с платежной системой Банка России. Все исходящие платежные документы шифруются на открытых ключах Банка России и закрытых ключах электронной подписи банка.

Декомпозиция (И):

У2.1.1.6.1. Шифрование поддельного платежного поручения на открытых ключах Банка России:
У2.1.1.6.1.1. Ссылка: «Типовая модель угроз. Система криптографической защиты информации. У2. Зашифрование подложных данных от имени легитимного отправителя».
У2.1.1.6.2. Электронная подпись поддельного платежного поручения на закрытых ключах банка:
У2.1.1.6.2.1. Ссылка: «Типовая модель угроз. Система криптографической защиты информации. У4. Создание электронной подписи легитимного подписанта под подложными данными».

У2.1.1.7. <...> в элементе «Модуль интеграции КБР-УТА»

Пояснения

В соответствии с технологическим процессом обработки платежей электронные сообщения на участке АРМ КБР — ЦБ РФ подписаны электронной подписью и зашифрованы. Соответственно внедрение поддельного платежного поручения на данном этапе возможно только в том случае, если злоумышленникам удалось в обход стандартной процедуры криптографической защиты зашифровать и подписать поддельное платежное поручение.

Декомпозиция (И):
У2.1.1.7.1. Ссылка: «Текущая модель угроз. У2.1.1.6. <...> в элементе «АРМ КБР».
У2.1.1.7.2. Ссылка: «Типовая модель угроз. Модуль интеграции. У1. Внедрение злоумышленниками подложной информации через модуль интеграции».

У2.1.1.8. <...> в элементе «УТА»

Пояснения
УТА — это, по сути, информационный робот, осуществляющий обмен криптографически защищенными электронными сообщениями с ЦБ РФ. Угрозы информационной безопасности данного элемента соответствуют с угрозами модулей интеграции.

Декомпозиция (И):
У2.1.1.8.1. Ссылка: «Текущая модель угроз. У2.1.1.6. <...> в элементе «АРМ КБР».
У2.1.1.8.2. Ссылка: «Типовая модель угроз. Модуль интеграции. У1. Внедрение злоумышленниками подложной информации через модуль интеграции».

У2.1.1.9. <...> в элементе «Канал передачи электронных сообщений»

Декомпозиция (И):

У2.1.1.9.1. Ссылка: «Текущая модель угроз. У2.1.1.6. <...> в элементе «АРМ КБР».
У2.1.1.9.2. Передача злоумышленниками поддельного платежного поручения в Банк России:
У2.1.1.9.2.1. <...> во время сеанса связи с Банком России, установленного от имени банка.
У2.1.1.9.2.2. <...> с помощью курьера на ОМНИ.

У2.2. Исполнение банком поддельного входящего платежного поручения

Декомпозиция
У2.2.1. Внедрение злоумышленниками поддельного входящего платежного поручения в бизнес-процесс обработки платежей.

У2.2.1. Внедрение злоумышленниками поддельного входящего платежного поручения в бизнес-процесс обработки платежей

Пояснения

На участке АРМ КБР — платежная система Банка России платежные поручения зашифрованы и подписаны электронной подписью. На участке АРМ КБР — АБС платежные поручения в общем случае криптографически не защищены.

Поступающие в банк платежные поручения зашифрованы на открытых ключах банка и подписаны закрытыми ключами Банка России. Ключевая система криптографической защиты базируется на частной инфраструктуре открытых ключей (private PKI), реализованной на базе СКЗИ СКАД Сигнатура и включающей в себя: удостоверяющий центр Банка России и пользователей — кредитные организации. Все участники инфраструктуры открытых ключей доверяют сертификатам, выпущенным удостоверяющим центром ЦБ РФ.

Таким образом, чтобы внедрить поддельное входящее платежное поручение злоумышленникам необходимо скомпрометировать открытые ключи шифрования банка-получателя и ключи электронной подписи, сертификатам которых доверяет банк-получатель.

Декомпозиция данной угрозы будет производиться на основании элементов инфраструктуры, в которых может произойти внедрение поддельных входящих платежных поручений

Элементы	Декомпозиция угрозы «У2.2.1. Внедрение злоумышленниками поддельного входящего платежного поручения в бизнес-процесс обработки платежей»
АБС	У2.2.1.1.
Модуль интеграции АБС-КБР	У2.2.1.2.
АРМ КБР	У2.2.1.3.
Модуль интеграции КБР-УТА	У2.2.1.4.
УТА	У2.2.1.5.
Канал передачи электронных сообщений	У2.2.1.6.

Декомпозиция

У2.2.1.1. <...> в элементе «АБС».
У2.2.1.2. <...> в элементе «Модуль интеграции АБС-КБР».
У2.2.1.3 .<...> в элементе «АРМ КБР».
У2.2.1.4 .<...> в элементе «Модуль интеграции КБР-УТА».
У2.2.1.5. <...> в элементе «УТА».
У2.2.1.6. <...> в элементе «Канал передачи электронных сообщений».

У2.2.1.1. <...> в элементе «АБС»

Декомпозиция

У2.2.1.1.1. Ссылка: «Типовая модель угроз. Информационная система, построенная на базе архитектуры клиент-сервер. У2. Несанкционированная модификация защищаемой информации во время ее обработки серверной частью информационной системы».

У2.2.1.2. <...> в элементе «Модуль интеграции АБС-КБР»

Декомпозиция

У2.2.1.2.1. Ссылка: «Типовая модель угроз. Модуль интеграции. У1. Внедрение злоумышленниками подложной информации через модуль интеграции».

У2.2.1.3. <...> в элементе «АРМ КБР»

Пояснения

При обработке входящих платежных документов АРМ КБР является последним рубежом обороны, задача которого расшифровать и проверить целостность входящих криптографически защищенных электронных сообщений. Защита данного этапа будет нейтрализована, если АРМ КБР, получив на вход поддельное платежное поручение, сообщит, что электронная подпись под ним верна.

Декомпозиция

У2.2.1.3.1. Успешная проверка электронной подписи поддельного входящего платежного поручения:
У2.2.1.3.1.1. Ссылка: «Типовая модель угроз. Система криптографической защиты информации. У5. Получение положительного результата проверки электронной подписи подложных данных».

У2.2.1.4. <...> в элементе «Модуль интеграции КБР-УТА»

Пояснения

Начиная с данного элемента и далее, до платежной системы Банка России, злоумышленники теряют возможность несанкционированного воздействия на систему криптографической защиты информации (СКЗИ), поэтому все данные, попадающие из Модуля интеграции в АРМ КБР, должны быть корректно зашифрованы и подписаны. Для зашифрования злоумышленники должны использовать открытые ключи банка, а для электронной подписи закрытые ключи, сертификатам которых доверяет банк.

Декомпозиция (И):

У2.2.1.4.1. Нейтрализация криптографической защиты входящих электронных сообщений (И):
У2.2.1.4.1.1. Шифрование поддельного платежного поручения на открытых ключах банка:
У2.2.1.4.1.1.1. Ссылка: «Типовая модель угроз. Система криптографической защиты информации. У2. Зашифрование подложных данных от имени легитимного отправителя».

У2.2.1.4.1.2. Электронная подпись поддельного платежного поручения на закрытых ключах, сертификатам которых доверяет банк:
У2.2.1.4.1.2.1. Ссылка: «Типовая модель угроз. Система криптографической защиты информации. У4. Создание электронной подписи легитимного подписанта под подложными данными».
У2.2.1.4.2. Ссылка: «Типовая модель угроз. Модуль интеграции. У1. Внедрение злоумышленниками подложной информации через модуль интеграции».

У2.2.1.5. <...> в элементе «УТА»

Декомпозиция

У2.2.1.5.1. Ссылка: «Текущая модель угроз. У2.2.1.4. <...> в элементе «Модуль интеграции КБР-УТА».

У2.2.1.6. <...> в элементе «Канал передачи электронных сообщений»

Декомпозиция (И):

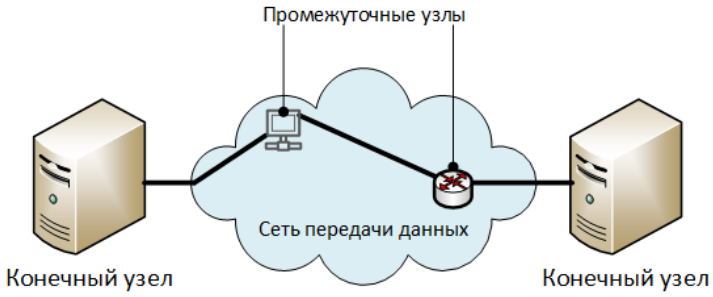
У2.2.1.6.1. Ссылка: «Текущая модель угроз.У2.2.1.4.1. Нейтрализация криптографической защиты входящих электронных сообщений».
У2.2.1.6.2. Получение поддельного платежного поручения из ЦБ РФ:
У2.2.1.6.2.1. <...> во время сеанса связи с Банком России, установленного от имени банка.
У2.2.1.6.2.2. <...> с помощью курьера на ОМНИ.

ТИПОВАЯ МОДЕЛЬ УГРОЗ. СЕТЕВОЕ СОЕДИНЕНИЕ

Объект защиты, для которого применяется модель угроз (scope)

Объектом защиты являются данные, передаваемые через сетевое соединение, функционирующее в сетях передачи данных, построенных на базе стека TCP/IP.

Архитектура



Описание элементов архитектуры:

- *«Конечные узлы»* — узлы, обменивающиеся защищаемой информацией.
- *«Промежуточные узлы»* — элементы сети передачи данных: маршрутизаторы, коммутаторы, сервера доступа, proxy-сервера и другое оборудование, — через которые передается трафик сетевого соединения. В общем случае сетевое

соединение может функционировать без промежуточных узлов (напрямую между конечными узлами).

Угрозы безопасности верхнего уровня

Декомпозиция

У1. Несанкционированное ознакомление с передаваемыми данными.
У2. Несанкционированная модификация передаваемых данных.
У3. Нарушение авторства передаваемых данных.

У1. Несанкционированное ознакомление с передаваемыми данными

Декомпозиция

У1.1. <...>, осуществляемое на конечных или промежуточных узлах:
У1.1.1. <...> путем считывания данных во время их нахождения в запоминающих устройствах узла:
У1.1.1.1. <...> в оперативной памяти.
Пояснения к У1.1.1.1.
Например, во время обработки данных сетевым стеком узла.

У1.1.1.2. <...> в энергонезависимой памяти.
Пояснения к У1.1.1.2.
Например, при хранении передаваемых данных в кэше, временных файлах или файлах подкачки.

У1.2. <...>, осуществляемое на сторонних узлах сети передачи данных:
У1.2.1. <...> методом захвата всех пакетов, попадающих на сетевой интерфейс узла:
Пояснения к У1.2.1.
Захват всех пакетов осуществляется путем перевода сетевой карты в неразборчивый режим (promiscuous режим для проводных адаптеров или в режим монитора для wi-fi адаптеров).

У1.2.2. <...> путем осуществления атак типа «человек посередине (MiTM)», но без модификации передаваемых данных (не считая служебных данных сетевых протоколов).
У1.2.2.1. Ссылка: «Типовая модель угроз. Сетевое соединение. У2. Несанкционированная модификация передаваемых данных».

У1.3. <...>, осуществляемое за счет утечки информации по техническим каналам (ТКУИ) с физических узлов или линий связи.

У1.4. <...>, осуществляемое за установки на конечные или промежуточные узлы специальных технических средств (СТС), предназначенных для негласного съема информации.

У2. Несанкционированная модификация передаваемых данных

Декомпозиция

У2.1. <...>, осуществляемая на конечных или промежуточных узлах:
У2.1.1. <...> путем считывания и внесения изменения в данные во время их нахождения в

запоминающих устройствах узлов:
У2.1.1.1. <...> в оперативной памяти:
У2.1.1.2. <...> в энергонезависимой памяти:

У2.2. <...>, осуществляемая на сторонних узлах сети передачи данных:
У2.2.1. <...> путем осуществлении атак типа «человек посередине (MiTM)» и перенаправления трафика на узел злоумышленников:
У2.2.1.1. Физическое подключение оборудования злоумышленников в разрыв сетевого соединения.
У2.2.1.2. Осуществление атак на сетевые протоколы:
У2.2.1.2.1. <...> управления виртуальными локальными сетями (VLAN):
У2.2.1.2.1.1. VLAN hopping.
У2.2.1.2.1.2. Несанкционированная модификация настроек VLAN на коммутаторах или маршрутизаторах.
У2.2.1.2.2. <...> маршрутизации трафика:
У2.2.1.2.2.1. Несанкционированная модификация таблиц статической маршрутизации роутеров.
У2.2.1.2.2.2. Анонсирование злоумышленниками подложных маршрутов через протоколы динамической маршрутизации.
У2.2.1.2.3. <...> автоматического конфигурирования:
У2.2.1.2.3.1. Rogue DHCP.
У2.2.1.2.3.2. Rogue WPAD.
У2.2.1.2.4. <...> адресации и разрешения имен:
У2.2.1.2.4.1. ARP spoofing.
У2.2.1.2.4.2. DNS spoofing.
У2.2.1.2.4.3. Внесение несанкционированных изменений в локальные файлы имен узлов (hosts, lmhosts и др.)

У3. Нарушение авторства передаваемых данных

Декомпозиция
У3.1. Нейтрализации механизмов определения авторства информации путем указания подложных сведений об авторе или источнике данных:
У3.1.1. Изменение сведений об авторе, содержащихся в передаваемой информации.
У3.1.1.1. Нейтрализация криптографической защиты целостности и авторства передаваемых данных:
У3.1.1.1.1. Ссылка: «Типовая модель угроз. Система криптографической защиты информации. У4. Создание электронной подписи легитимного подписанта под подложными данными».
У3.1.1.2. Нейтрализация защиты авторства передаваемых данных, реализованной с помощью одноразовых кодов подтверждений:
У3.1.1.2.1. SIM swap.

У3.1.2. Изменение сведений об источнике передаваемой информации:
У3.1.2.1. IP spoofing.
У3.1.2.2. MAC spoofing.

ТИПОВАЯ МОДЕЛЬ УГРОЗ. ИНФОРМАЦИОННАЯ СИСТЕМА, ПОСТРОЕННАЯ НА БАЗЕ АРХИТЕКТУРЫ КЛИЕНТ-СЕРВЕР

Объект защиты, для которого применяется модель угроз (scope)

Объектом защиты является информационная система, построенная на базе архитектуры клиент-сервер.

Архитектура

Описание элементов архитектуры:

- *«Клиент»* – устройство, на котором функционирует клиентская часть информационной системы.
- *«Сервер»* – устройство, на котором функционирует серверная часть информационной системы.
- *«Хранилище данных»* — часть серверной инфраструктуры информационной системы, предназначенная для хранения данных, обрабатываемых информационной системой.
- *«Сетевое соединение»* — канал обмена информацией между Клиентом и Сервером, проходящий через сеть передачи данных. Более подробное описание модели элемента приведено в «Типовой модели угроз. Сетевое соединение».

Ограничения

При моделировании объекта установлены следующие ограничения:

1. Пользователь взаимодействует с информационной системой в рамках конечных промежутков времени, называемых сеансами работы.
2. В начале каждого сеанса работы происходит идентификация, аутентификация и авторизация пользователя.
3. Вся защищаемая информация хранится на серверной части информационной системы.

Угрозы безопасности верхнего уровня

Декомпозиция

У1. Совершение злоумышленниками несанкционированных действий от имени легитимного пользователя.

У2. Несанкционированная модификация защищаемой информации во время ее обработки серверной частью информационной системы.

У1. Совершение злоумышленниками несанкционированных действий от имени легитимного пользователя

Пояснения

Обычно в информационных системах соотнесение действий с выполнившим их пользователем производится с помощью:

- журналов работы системы (logs).
- специальных атрибутов объектов данных, содержащих сведения об создавшем или изменившем их пользователе.

По отношению к сеансу работы данная угроза может декомпозироваться на:

1. <...> выполненные в рамках сеанса работы пользователя.
2. <...> выполненные вне сеанса работы пользователя.

Сеанс работы пользователя может быть инициирован:

1. Самим пользователем.
2. Злоумышленниками.

На данном этапе промежуточная декомпозиция данной угрозы будет выглядеть следующим образом:

У1.1. Несанкционированные действия выполнены в рамках сеанса работы пользователя:

У1.1.1. <...>, установленного атакованным пользователем.

У1.1.2. <...>, установленного злоумышленниками.

У1.2. Несанкционированные действия выполнены вне сеанса работы пользователя.

С точки зрения объектов информационной инфраструктуры, на которые могут воздействовать злоумышленники, декомпозиция промежуточных угроз будет выглядеть следующим образом:

Элементы	**Декомпозиция угроз**		
	У1.1.1.	**У1.1.2.**	**У1.2.**
Клиент	У1.1.1.1.	У1.1.2.1.	
Сетевое соединение	У1.1.1.2.		
Сервер			У1.2.1.

Декомпозиция

У1.1. Несанкционированные действия выполнены в рамках сеанса работы пользователя:

У1.1.1. <...>, установленного атакованным пользователем:

У1.1.1.1. Злоумышленники самостоятельно действовали с Клиента:

У1.1.1.1.1 Злоумышленники использовали штатные средства доступа информационной системы:

У1.1.1.1.1.1. Злоумышленники использовали физические средства ввода-вывода Клиента (клавиатура, мышь, монитор или сенсорный экран мобильного устройства):

У1.1.1.1.1.1.1. Злоумышленники действовали в периоды времени, когда сеанс активен, средства ввода-вывода доступны, а пользователя нет на месте.

У1.1.1.1.1.2. Злоумышленники использовали средства удаленного администрирования

(штатные или предоставленные вредоносным кодом) для управления Клиентом:
У1.1.1.1.1.2.1. Злоумышленники действовали в периоды времени, когда сеанс активен, средства ввода-вывода доступны, а пользователя нет на месте.
У1.1.1.1.1.2.2. Злоумышленники использовали средства удаленного администрирования, работа которых незаметна атакованному пользователю.
У1.1.1.2. Злоумышленники подменяли данные в сетевом соединении между Клиентом и Сервером, модифицируя их таким образом, чтобы они воспринимались как действия легитимного пользователя:
У1.1.1.2.1. Ссылка: «Типовая модель угроз. Сетевое соединение. У2. Несанкционированная модификация передаваемых данных».
У1.1.1.3. Злоумышленники принудили пользователя к выполнению указанных ими действий, используя методы социальной инженерии.

У1.1.2 <...> установленного злоумышленниками:
У1.1.2.1. Злоумышленники действовали с Клиента (**И**):
У1.1.2.1.1. Злоумышленники нейтрализовали систему разграничения доступа информационной системы:
У1.1.2.1.1.1. Ссылка: «Типовая модель угроз. Система разграничения доступа. У1. Несанкционированное установление сеанса работы от имени легального пользователя».
У1.1.2.1.2. Злоумышленники использовали штатные средства доступа информационной системы
У1.1.2.2. Злоумышленники действовали с других узлов сети передачи данных, с которых можно установить сетевое соединение с Сервером (**И**):
У1.1.2.2.1. Злоумышленники нейтрализовали систему разграничения доступа информационной системы:
У1.1.2.2.1.1. Ссылка: «Типовая модель угроз. Система разграничения доступа. У1. Несанкционированное установление сеанса работы от имени легального пользователя».
У1.1.2.2.2. Злоумышленники использовали нештатные средства доступа информационной системы.
Пояснения У1.1.2.2.2.
Злоумышленники могли установить штатный клиент информационной системы на сторонний узел или могли использовать нештатное ПО, реализующее штатные протоколы обмена между Клиентом и Сервером.

У1.2 Несанкционированные действия выполнены вне сеанса работы пользователя.
У1.2.1 Злоумышленники выполнили несанкционированные действия, а затем внесли несанкционированные изменения в журналы работы информационной системы или специальные атрибуты объектов данных, указав, что совершенные ими действия выполнены легитимным пользователем.

У2. Несанкционированная модификация защищаемой информации во время ее обработки серверной частью информационной системы

Декомпозиция
У2.1. Злоумышленники модифицируют защищаемую информацию с помощью штатных средств информационной системы и проводят это от имени легитимного пользователя.
У2.1.1. Ссылка: «Типовая модель угроз. Информационная система, построенная на базе

архитектуры клиент-сервер. У1. Совершение злоумышленниками несанкционированных действий от имени легитимного пользователя».

У2.2. Злоумышленники модифицируют защищаемую информацию путем использования не предусмотренных штатным режимом функционирования информационной системы механизмов доступа к данным.
У2.2.1. Злоумышленники модифицируют файлы, содержащие защищаемую информацию:
У2.2.1.1. <...>, используя механизмы работы с файлами, предоставляемые операционной системой.
У2.2.1.2. <...> путем провокации восстановления файлов из несанкционированно модифицированной резервной копии.

У2.2.2. Злоумышленники модифицируют защищаемую информацию, хранящуюся в базе данных (**И**):
У2.2.2.1. Злоумышленники нейтрализовывают систему разграничения доступа СУБД:
У2.2.2.1.1. Ссылка: «Типовая модель угроз. Система разграничения доступа. У1. Несанкционированное установление сеанса работы от имени легального пользователя».
У2.2.2.2. Злоумышленники модифицируют информацию, используя штатные интерфейсы СУБД для доступа к данным.

У2.3. Злоумышленники модифицируют защищаемую информацию путем несанкционированной модификации алгоритмов работы обрабатывающего ее ПО.
У2.3.1. Модификации подвергается исходный код ПО.
У2.3.1. Модификации подвергается машинный код ПО.

У2.4. Злоумышленники модифицируют защищаемую информацию путем использования уязвимостей в программном обеспечении информационной системы.

У2.5. Злоумышленники модифицируют защищаемую информацию при ее передаче между компонентами серверной части информационной системы (например, сервером баз данных и сервером приложений):
У2.5.1. Ссылка: «Типовая модель угроз. Сетевое соединение. У2. Несанкционированная модификация передаваемых данных».

ТИПОВАЯ МОДЕЛЬ УГРОЗ. СИСТЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА

Объект защиты, для которого применяется модель угроз (scope)

Объект защиты, для которого применяется данная модель угроз, соответствует объекту защиты модели угроз: «Типовая модель угроз. Информационная система, построенная на базе архитектуры клиент-сервер».

Под системой разграничения доступа пользователей в данной модели угроз подразумевается компонент информационной системы, реализующий функции:

1. Идентификации пользователей.
2. Аутентификации пользователей.
3. Авторизации пользователей.
4. Протоколирования действий пользователей.

Угрозы безопасности верхнего уровня

Декомпозиция

У1. Несанкционированное установление сеанса работы от имени легального пользователя.

У2. Несанкционированное повышение привилегий пользователя в информационной системе.

У1. Несанкционированное установление сеанса работы от имени легального пользователя

Пояснения

Декомпозиция данной угрозы в общем случае будет зависеть от применяемого типа систем идентификации и аутентификации пользователей.

В данной модели будет рассмотрена только система идентификации и аутентификации пользователей, использующая текстовые логин и пароль. При этом будем считать, что логин пользователя — общедоступная информация, известная злоумышленникам.

Декомпозиция

У1.1. <...> за счет компрометации учетных данных:

У1.1.1. Злоумышленники скомпрометировали учетные данные пользователя в процессе их хранения.

Пояснения У1.1.1.

Например, учетные данные могли быть написаны на стикере, приклеенном к монитору.

У1.1.2. Пользователь случайно или по злому умыслу передал реквизиты доступа злоумышленникам.

У1.1.2.1. Пользователь проговаривал учетные данные вслух при вводе.

У1.1.2.2. Пользователь умышлено передал свои учетные данные:

У1.1.2.2.1. <...> коллегам по работе.

Пояснения У1.1.2.2.1.

Например, для того, чтобы они могли его заменить на период болезни.

У1.1.2.2.2. <...> контрагентам работодателя, выполняющим работы над объектами информационной инфраструктуры.

У1.1.2.2.3. <...> третьим лицам.

Пояснения У1.1.2.2.3.

Одним, но не единственными вариантом реализации данной угрозы является использование злоумышленниками методов социальной инженерии.

У1.1.3. Злоумышленники подобрали учетные данные методом перебора:

У1.1.3.1. <...> с использованием штатных механизмов доступа.

У1.1.3.2. <...> по ранее перехваченным кодам (например, хэшам паролей) хранения учетных

данных.

У1.1.4. Злоумышленники использовали вредоносный код для перехвата учетных данных пользователя.

У1.1.5. Злоумышленники извлекли учетные данные из сетевого соединения между Клиентом и Сервером:
У1.1.5.1. Ссылка: «Типовая модель угроз. Сетевое соединение. У1. Несанкционированное ознакомление с передаваемыми данными».

У1.1.6. Злоумышленники извлекли учетные данные с записей систем мониторинга работы:
У1.1.6.1. <...> систем видеонаблюдения (в случае, если во время работы фиксировались нажатия клавиш на клавиатуре).
У1.1.6.2. <...> систем контроля действий сотрудников за компьютером
Пояснения У1.1.6.2.
Пример подобной системы — StuffCop.

У1.1.7. Злоумышленники скомпрометировали учетные данные пользователя из-за недостатков процесса их передачи.
Пояснения У1.1.7.
Например, передача паролей в открытом виде по электронной почте.

У1.1.8. Злоумышленники узнали учетные данные путем наблюдения за сеансом работы пользователя с помощью систем удаленного администрирования.

У1.1.9. Злоумышленники извлекли учетные данные в результате их утечки по техническим каналам (ТКУИ):
У1.1.9.1. Злоумышленники подглядели, как пользователь вводит учетные данные с клавиатуры:
У1.1.9.1.1 Злоумышленники располагались в непосредственной близости к пользователю и видели ввод учетных данных своими глазами.
Пояснения У1.1.9.1.1
К подобным случаям можно отнести действия коллег по работе или случай, когда клавиатуру пользователя видно посетителям организации.

У1.1.9.1.2 Злоумышленники использовали дополнительные технические средства, такие как бинокль или беспилотный летательный аппарат, и увидели ввод учетных данных через окно.
У1.1.9.2. Злоумышленники извлекли учетные данные из записей радиообмена между клавиатурой и системным блоком компьютера в случае подключения их по радиоинтерфейсу (например, Bluetooth).
У1.1.9.3. Злоумышленники осуществили перехват учетных данных за счет их утечки по каналу побочных электромагнитных излучений и наводок (ПЭМИН).
Пояснения У1.1.9.3.
Примеры атаки тут и тут.

У1.1.9.4. Злоумышленник осуществил перехват ввода учетных данных с клавиатуры за счет

использования специальных технических средств (СТС), предназначенных для негласного съема информации.
Пояснения У1.1.9.4.
Примеры устройств.

У1.1.9.5. Злоумышленники осуществили перехват ввода учетных данных с клавиатуры за счет анализа Wi-Fi сигнала, модулированного процессом нажатия клавиш пользователем.
Пояснения У1.1.9.5.
Пример атаки.

У1.1.9.6. Злоумышленники осуществили перехват ввода учетных данных с клавиатуры за счет анализа звуков нажатия на клавиши.
Пояснения У1.1.9.6.
Пример атаки.

У1.1.9.7. Злоумышленники осуществили перехват ввода учетных данных с клавиатуры мобильного устройства за счет анализа показаний акселерометра.
Пояснения У1.1.9.7.
Пример атаки.

У1.1.10. <...>, предварительно сохраненных на Клиенте.
Пояснения У1.1.10.
Например, пользователь мог сохранить в браузере логин и пароль для доступа к определенному сайту.

У1.1.11. Злоумышленники скомпрометировали учетные данные из-за недостатков процесса отзыва доступов пользователей.
Пояснения У1.1.11.
Например, после увольнения пользователя его учетные записи остались не заблокированными.

У1.2. <...> за счет использования уязвимостей в системе разграничения доступа.

У2. Несанкционированное повышение привилегий пользователя в информационной системе

Декомпозиция
У2.1 <...> путем внесения несанкционированных изменений в данные, содержащие сведения о привилегиях пользователя.

У2.2 <...> за счет использования уязвимостей в системе разграничения доступа.

У2.3. <...> из-за недостатков процесса управления доступом пользоватлей.
Пояснения У2.3.
Пример 1. Пользователю для работы был предоставлен доступ больший, нежели ему требовался по служебной необходимости.

Пример 2. После перевода пользователя на другую должность ранее предоставленные права доступа не были отозваны.

ТИПОВАЯ МОДЕЛЬ УГРОЗ. МОДУЛЬ ИНТЕГРАЦИИ

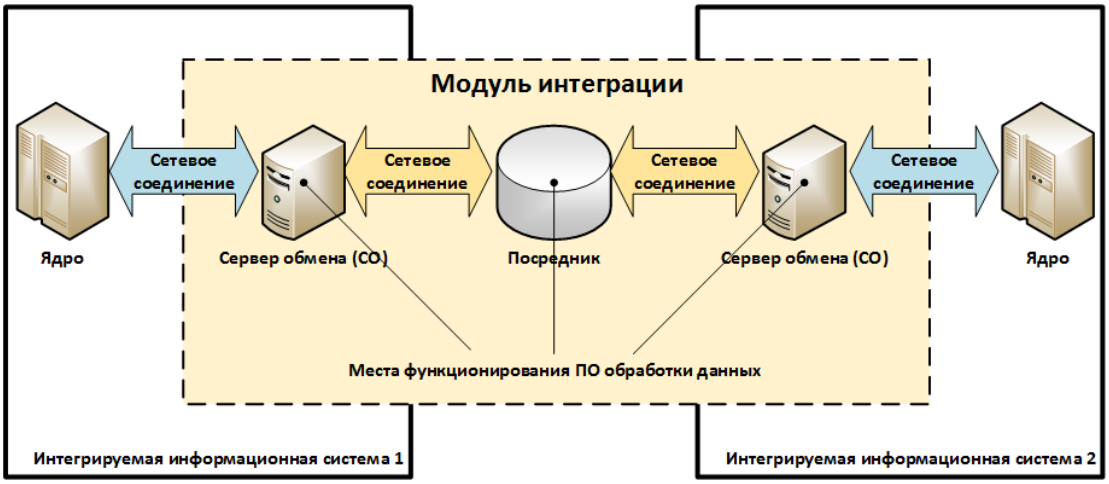
Объект защиты, для которого применяется модель угроз (scope)

Модуль интеграции – набор объектов информационной инфраструктуры, предназначенный для организации обмена информацией между информационными системами.

Учитывая тот факт, что в корпоративных сетях не всегда возможно однозначно отделить одну информационную систему от другой, модуль интеграции можно рассматривать и как связующее звено между компонентами внутри одной информационной системы.

Архитектура

Обобщенная схема модуля интеграции выглядит следующим образом:



Описание элементов архитектуры:

- *«Сервер обмена (СО)»* – узел / сервис / компонент информационной системы, выполняющий функцию обмена данными с другой информационной системой.
- *«Посредник»* – узел / сервис, предназначенный для организации взаимодействия между информационными системами, но не входящий в их состав. Примерами *«Посредников»* могут быть сервисы электронной почты, сервисные шины предприятия (enterprise service bus / SoA-архитектура), сторонние файловые сервера и т.д. В общем случае модуль интеграции может и не содержать «Посредников».
- *«ПО обработки данных»* – совокупность программ, реализующая протоколы обмена данными и преобразование форматов. Например, преобразование данных из формата УФЭБС в формат АБС, изменение статусов сообщений в процессе передачи и т.д.

- *«Сетевое соединение»* соответствует объекту, описанному в типовой модели угроз «Сетевое соединение». Некоторых сетевых соединений из тех, что представлены на схеме выше, может и не быть.

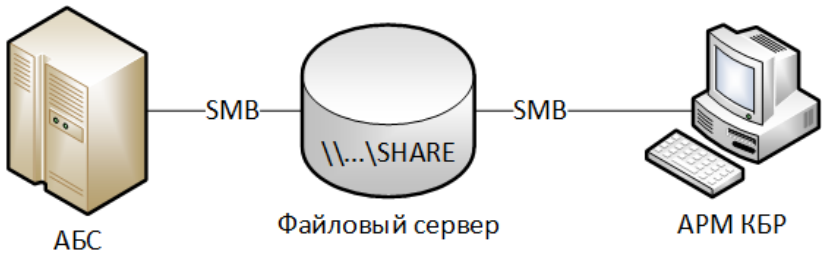
Примеры модулей интеграции

Схема 1. Интеграция АБС и АРМ КБР через сторонний файловый сервер

Для исполнения платежей уполномоченный работник банка выгружает из АБС электронные платежные документы и сохраняет их в файл (собственного формата, например SQL-дамп) на сетевой папке (\\...\SHARE\) файлового сервера. Затем этот файл с помощью скрипта-конвертера преобразуется в набор файлов формата УФЭБС, которые затем считывает АРМ КБР.
После этого уполномоченный работник — пользователь АРМ КБР — шифрует и подписывает полученные файл и отправляет их в платежную систему Банка России.

При поступлении платежей из Банка России АРМ КБР проводит их расшифровку и проверку электронной подписи, после чего записывает в виде набора файлов формата УФЭБС на файловый сервер. Перед импортом платежных документов в АБС они преобразуются с помощью скрипта-конвертера из формата УФЭБС в формат АБС.

Будем считать, что в данной схеме АБС функционирует на одном физическом сервере, АРМ КБР функционирует на выделенном компьютере, а скрипт-конвертер работает на файловом сервере.

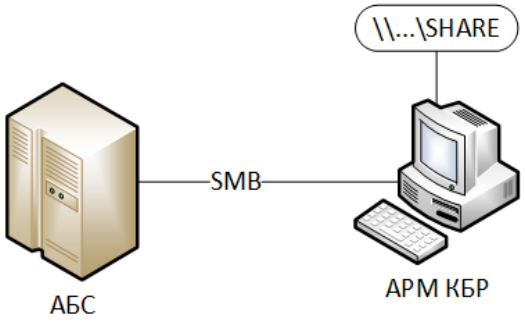


Соответствие объектов рассмотренной схемы элементам модели модуля интеграции:

«Сервера обмена со стороны АБС» – сервер АБС.
«Сервера обмена со стороны АРМ КБР» – компьютер АРМ КБР.
«Посредник» – сторонний файловый сервер.
«ПО обработки данных» – скрипт-конвертер.

Схема 2. Интеграция АБС и АРМ КБР при размещении общей сетевой папки с платежами на АРМ КБР

Все аналогично Схеме 1, но отдельный файловый сервер не используется, вместо этого сетевая папка (\\...\SHARE\) с электронными платежными документами размещается на компьютере с АРМ КБР. Скрипт-конвертер также работает на АРМ КБР.



Соответствие объектов рассмотренной схемы элементам модели модуля интеграции:

Аналогично Схеме 1, но *«Посредник»* не используется.

Схема 3. Интеграция АБС и АРМ КБР-Н через IBM WebSphera MQ и осуществление подписи электронных документов «на стороне АБС»

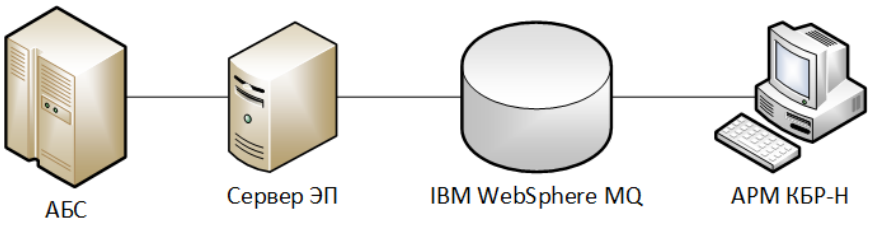
АБС работает на платформе, не поддерживаемой СКЗИ СКАД Сигнатура. Подпись исходящих электронных документов проводится на специальном сервере электронной подписи (Сервер ЭП). Этот же сервер проверяет электронную подпись под входящими из Банка России документами.

АБС выгружает на Сервер ЭП файл с платежными документами в собственном формате. Сервер ЭП с помощью скрипта-конвертера преобразует файл в электронные сообщения формата УФЭБС, после этого электронные сообщения подписываются и передаются на IBM WebSphere MQ.

АРМ КБР-Н обращается к IBM WebSphere MQ и получает оттуда подписанные платежные сообщения, после чего уполномоченный работник — пользователь АРМ КБР — их шифрует и отправляет в платежную систему Банка России.

При поступлении платежей из Банка России АРМ КБР-Н расшифровывает их и проверяет электронную подпись. Успешно обработанные платежи в виде расшифрованных и подписанных электронных сообщений формата УФЭБС передаются в IBM WebSphere MQ, откуда их получает Сервер ЭП.

Сервер ЭП проверяет электронную подпись поступивших платежей и сохраняет их в файл формата АБС. После этого уполномоченный работник — пользователь АБС — загружает получившийся файл в АБС в установленном порядке.



Соответствие объектов рассмотренной схемы элементам модели модуля интеграции:

«Сервер обмена со стороны АБС» – сервер АБС.
«Сервер обмена со стороны АРМ КБР» — компьютер АРМ КБР.
«Посредник» – Сервер ЭП и IBM WebSphere MQ.
«ПО обработки данных» – скрипт-конвертер, СКЗИ СКАД Сигнатура на Сервере ЭП.

Схема 4. Интеграция Сервера ДБО и АБС через API, предоставляемый выделенным сервером обмена

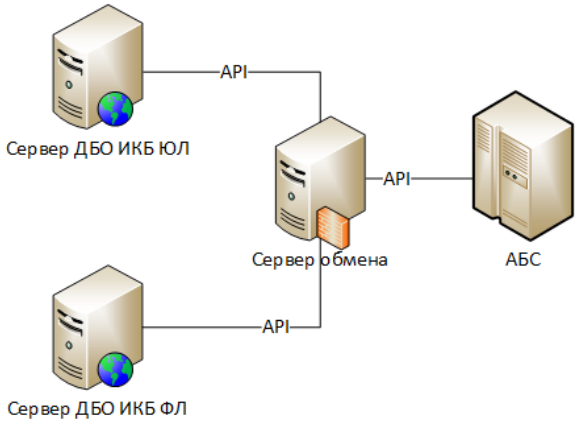
Будем считать, что в банке используется несколько систем дистанционного банковского обслуживания (ДБО):

- «Интернет Клиент-Банк» для физических лиц (ИКБ ФЛ);
- «Интернет Клиент-Банк» для юридических лиц (ИКБ ЮЛ).

В целях обеспечения информационной безопасности все взаимодействие АБС с системами ДБО осуществляется через выделенный сервер обмена, работающий в рамках информационной системы «АБС».

Далее рассмотрим процесс взаимодействия системы ДБО ИКБ ЮЛ с АБС. Сервер ДБО, получив от клиента должным образом заверенное платежное поручение, должен на его основе создать соответствующий документ в АБС. Для этого он с помощью API передает информацию в сервер обмена, а тот, в свою очередь, вносит данные в АБС.

При изменении остатков на счете клиента АБС формирует электронные уведомления, которые с помощью сервера обмена передаются на сервер ДБО.



Соответствие объектов рассмотренной схемы элементам модели модуля интеграции:

«Сервер обмена со стороны ДБО» – сервер ДБО ИКБ ЮЛ.
«Сервер обмена со стороны АБС» – сервер обмена.
«Посредник» – отсутствует.
«ПО обработки данных» – компоненты Сервера ДБО, ответственные за использование API сервера обмена, компоненты сервера обмена, ответственные за использование API АБС.

Угрозы безопасности верхнего уровня

Декомпозиция

У1. Внедрение злоумышленниками подложной информации через модуль интеграции.

У1. Внедрение злоумышленниками подложной информации через модуль интеграции

Декомпозиция

У1.1. Несанкционированная модификация легитимных данных при их передаче через сетевые соединения:

У1.1.1 Ссылка: «Типовая модель угроз. Сетевое соединение. У2. Несанкционированная модификация передаваемых данных».

У1.2. Передача по каналам связи подложных данных от имени легитимного участника обмена:

У1.1.2 Ссылка: «Типовая модель угроз. Сетевое соединение. У3. Нарушение авторства передаваемых данных».

У1.3. Несанкционированная модификация легитимных данных при их обработке на Серверах обмена или Посреднике:

У1.3.1. Ссылка: «Типовая модель угроз. Информационная система, построенная на базе архитектуры клиент-сервер. У2. Несанкционированная модификация защищаемой информации во время ее обработки серверной частью информационной системы»..

У1.4. Создание на Серверах обмена или Посреднике подложных данных от имени легитимного участника обмена:

У1.4.1. Ссылка: «Типовая модель угроз. Информационная система, построенная на базе архитектуры клиент-сервер. У1. Совершение злоумышленниками несанкционированных действий от имени легитимного пользователя».

У1.5. Несанкционированная модификация данных при их обработке с помощью ПО обработки данных:

У1.5.1. <...> за счет внесения злоумышленниками несанкционированных изменений в настройки (конфигурацию) ПО обработки данных.

У1.5.2. <...> за счет внесения злоумышленниками несанкционированных изменений в исполняемые файлы ПО обработки данных.

У1.5.3. <...> за счет интерактивного управления злоумышленниками работой ПО обработки данных.

ТИПОВАЯ МОДЕЛЬ УГРОЗ. СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Объект защиты, для которого применяется модель угроз (scope)

Объектом защиты является система криптографической защиты информации, используемая для обеспечения безопасности информационной системы.

Архитектура

Основой любой информационной системы является прикладное программное обеспечение (ПО), реализующее ее целевой функционал.

Криптографическая защита при этом обычно реализуется путем вызова из бизнес-логики прикладного ПО криптографических примитивов, которые размещаются в специализированных библиотеках – криптоядрах.

К криптографическим примитивам относятся низкоуровневые криптографические функции, такие как:

- зашифровать / расшифровать блок данных;
- создать / проверить электронную подпись блока данных;
- вычислить хэш-функцию блока данных;
- сформировать / загрузить / выгрузить ключевую информацию;
- и т.д.

Бизнес-логика прикладного ПО с помощью криптографических примитивов реализует более высокоуровневый функционал:

- зашифровать файл на ключах выбранных получателей;
- установить защищенное сетевое соединение;
- информировать о результатах проверки электронной подписи;
- и т. п.

Взаимодействие бизнес-логики и криптоядра может производиться:

- напрямую, путем вызова бизнес-логикой криптографических примитивов из динамических библиотек криптоядра (.DLL – для Windows, .SO – для Linux);
- опосредственно, через криптографические интерфейсы – обертки (wrappers), например, MS Crypto API, Java Cryptography Architecture, PKCS#11 и др. В данном случае бизнес-логика обращается к криптоинтерфейсу, а тот транслирует вызов к соответствующему криптоядру, которое в подобном случае называется криптопровайдером. Использование криптографических интерфейсов позволяет прикладному ПО абстрагироваться от конкретных криптографических алгоритмов и быть более гибким.

Можно выделить две типовые схемы организации криптоядра:

Схема 1 – Монолитное криптоядро

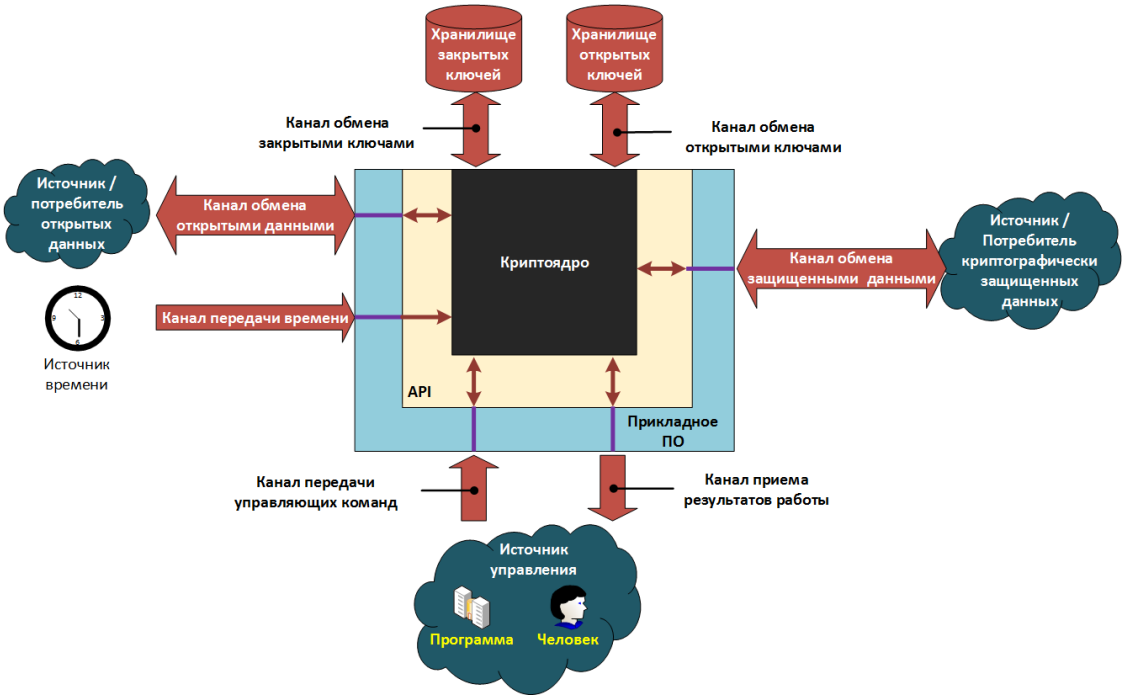
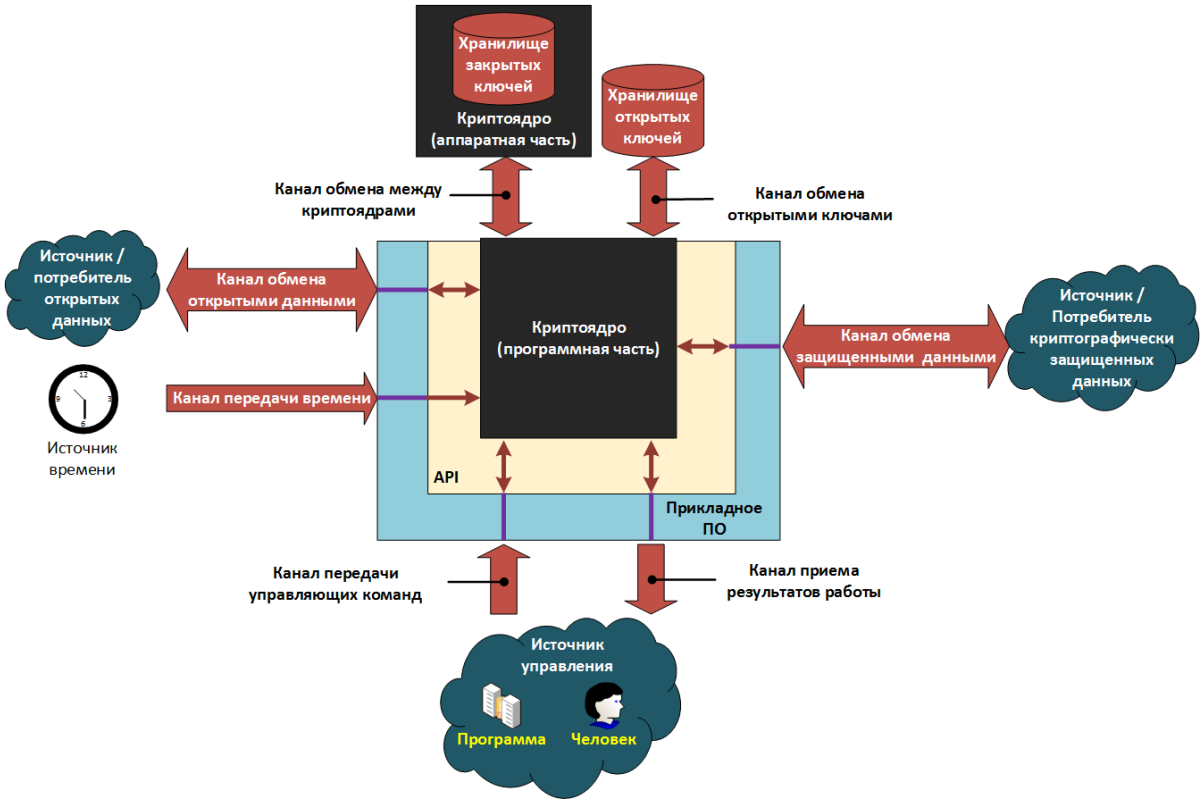


Схема 2 – Разделенное криптоядро



Элементы на приведенных схемах могут быть как отдельными модулями ПО, работающими на одном компьютере, так и сетевыми сервисами, взаимодействующими в рамках вычислительной сети.

При использовании систем, построенных по схеме 1, прикладное ПО и криптоядро работают в рамках единой среды функционирования криптосредства (СФК), например, на одном и том же компьютере, под управлением одной и той же операционной системы. Пользователь системы, как правило, может запускать в рамках этой же среды функционирования и другие программы, в том числе содержащие вредоносный код. В подобных условиях существует серьезный риск утечки закрытых криптографических ключей.

Для минимизации риска применяют схему 2, при которой криптоядро разделяется на две части:

1. Первая часть вместе с прикладным ПО работает в недоверенной среде, где существует риск заражения вредоносным кодом. Будем называть эту часть – «программной частью».
2. Вторая часть работает в доверенной среде на выделенном устройстве, которое содержит в своем составе хранилище закрытых ключей. Далее будем называть эту часть – «аппаратной частью».

Разделение криптоядра на программную и аппаратную части весьма условно. На рынке есть системы, построенные по схеме с разделенным криптоядром, но «аппаратная» часть которых представлена в виде образа виртуальной машины — virtual HSM (пример).

Взаимодействие обеих частей криптоядра происходит таким образом, что закрытые криптографические ключи никогда не передаются в программную часть и, соответственно, не могут быть похищены с помощью вредоносного кода.

Интерфейс взаимодействия (API) и набор криптографических примитивов, предоставляемых прикладному ПО криптоядром, в обоих случаях одинаковый. Различие кроется в способе их реализации.

Так, при использовании схемы с разделенным криптоядром, взаимодействие программной и аппаратной части выполняется по следующему принципу:

1. Криптографические примитивы, не требующие использования закрытого ключа (например, расчет хэш-функции, проверка электронной подписи и др.), выполняются программной частью.
2. Криптографические примитивы, использующие закрытый ключ (создание электронной подписи, расшифровка данных и др.), выполняются аппаратной частью.

Проиллюстрируем работу разделенного криптоядра на примере создания электронной подписи:

1. Программная часть рассчитывает хэш-функцию подписываемых данных и по каналу обмена между криптоядрами передает это значение в аппаратную часть.
2. Аппаратная часть, используя закрытый ключ и хэш, формирует значение электронной подписи и по каналу обмена передает его в программную часть.
3. Программная часть возвращает полученное значение в прикладное ПО.

Особенности проверки корректности электронной подписи

Когда принимающая сторона получает данные, подписанные электронной подписью, она должна провести несколько этапов проверки. Положительный результат проверки электронной подписи достигается только при успешном прохождении всех этапов проверки.

Этап 1. Контроль целостности данных и авторства данных.

Содержание этапа. Проводится проверка электронной подписи данных по соответствующему криптографическому алгоритму. Успешное прохождение данного этапа говорит о том, что данные не модифицировались с момента их подписания, а также то, что подпись была произведена закрытым ключом, соответствующим открытому ключу проверки электронной подписи.
Место выполнения этапа: криптоядро.

Этап 2. Контроль доверия к открытому ключу подписанта и контроль срока действия закрытого ключа электронной подписи.

Содержание этапа. Этап состоит из двух промежуточных подэтапов. На первом устанавливается, являлся ли открытый ключ проверки электронной подписи доверенным на момент подписания данных. На втором устанавливается, действовал ли на момент подписания данных закрытый ключ электронной подписи. В общем случае сроки действия этих ключей могут не совпадать (например, для квалифицированных сертификатов ключей проверки электронной подписи). Способы установления доверия к открытому ключу подписанта определяются правилами электронного документооборота, принятыми взаимодействующими сторонами.

Место выполнения этапа: прикладное ПО / криптоядро.

Этап 3. Контроль полномочий подписанта.

Содержание этапа. В соответствии с установленными правилами электронного документооборота проверяется, имел ли подписант право заверять защищаемые данные. Для примера приведем ситуацию нарушения полномочий. Предположим, есть организация, где все работники имеют электронную подпись. Во внутреннюю систему электронного документооборота поступает приказ руководителя, но подписанный электронной подписью заведующего складом. Соответственно, подобный документ не может считаться легитимным.

Место выполнения этапа: прикладное ПО.

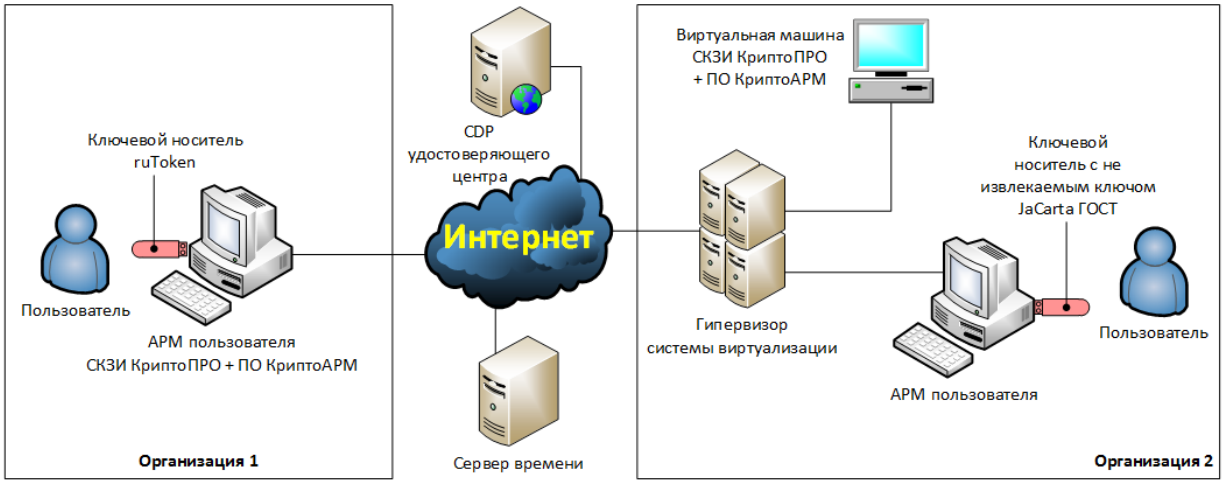
Допущения, принятые при описании объекта защиты

1. Каналы передачи информации, за исключением каналов обмена ключами, в том числе проходят через прикладное ПО, API и криптоядро.
2. Сведения о доверии к открытым ключам и (или) сертификатам, а также информация о полномочиях владельцев открытых ключей, размещается в хранилище открытых ключей.
3. Прикладное ПО работает с хранилищем открытых ключей через криптоядро.

Пример информационной системы, защищенной с помощью СКЗИ

Для иллюстрации ранее представленных схем рассмотрим гипотетическую информационную систему и выделим на ней все структурные элементы.

Описание информационной системы



Две организации решили внедрить между собой юридически значимый электронный документооборот (ЭДО). Для этого они заключили соглашение, в котором прописали, что документы будут передаваться по электронной почте, и при этом они должны быть зашифрованы и подписаны квалифицированной электронной подписью. В качестве средств создания и обработки документов должны использоваться офисные программы из пакета Microsoft Office 2016, а в качестве средств криптографической защиты — СКЗИ КриптоПРО и ПО шифрования КриптоАРМ.

Описание инфраструктуры организации 1

Организация 1 решила, что установит СКЗИ КриптоПРО и ПО КриптоАРМ на АРМ пользователя — физический компьютер. Ключи шифрования и электронной подписи будут храниться на ключевом носителе ruToken, работающем в режиме извлекаемого ключа. Пользователь будет подготавливать электронные документы локально на своем компьютере, после чего их шифровать, подписывать и отправлять с помощью локально установленного почтового клиента.

Описание инфраструктуры организации 2

Организация 2 решила вынести функции шифрования и электронной подписи на выделенную виртуальную машину. При этом все криптографические операции будут производиться в автоматическом режиме.

Для этого на выделенной виртуальной машине организовано две сетевых папки: "\\...\In\", "\\...\Out\". В сетевую папку "\\...\In\" будут автоматически помещаться полученные от

контрагента файлы в открытом виде. Эти файлы будут расшифрованы, и на них будет проверена электронная подпись.

В папку "\\...\Out\" пользователь будет помещать файлы, которые необходимо зашифровать, подписать и отправить контрагенту. Сами файлы пользователь будет готовить на своем АРМе. Для выполнения функций шифрования и электронной подписи на виртуальную машину установлены СКЗИ КриптоПРО, ПО КриптоАРМ и почтовый клиент. Автоматическое управление всеми элементами виртуальной машины будет осуществляться с помощью скриптов, разработанных системными администраторами. Работа скриптов протоколируется в файлы журналов (logs).

Криптографические ключи электронной подписи будут размещаться на токене с неизвлекаемым ключом JaCarta ГОСТ, который пользователь будет подключать к своему локальному компьютеру.

Токен будет пробрасываться на виртуальную машину с помощью специализированных программных средств USB-over-IP, установленных на АРМе пользователя и на виртуальной машине.

Системные часы на АРМе пользователя в организации 1 будут корректироваться в ручном режиме. Системные часы специализированной виртуальной машины в организации 2 будут синхронизироваться с системными часами гипервизора, а те, в свою очередь, будут синхронизироваться через Интернет с публичными серверами времени.

Выделение структурных элементов СКЗИ

На основании вышеприведенного описания IT-инфраструктуры выделим структурные элементы СКЗИ и запишем их в таблицу.

Наименование элемента	Организация 1	Организация 2
Прикладное ПО	ПО КриптоАРМ	ПО КриптоАРМ
Программная часть криптоядра	СКЗИ КриптоПРО CSP	СКЗИ КриптоПРО CSP
Аппаратная часть криптоядра	отсутствует	JaCarta ГОСТ
API	MS CryptoAPI	MS CryptoAPI
Хранилище открытых ключей	АРМ пользователя: — жесткий диск; — стандартное хранилище сертификатов Windows.	Гипервизор: — жесткий диск. Виртуальная машина: — жесткий диск; — стандартное хранилище сертификатов Windows.
Хранилище закрытых ключей	Ключевой носитель ruToken, работающий в режиме извлекаемого ключа	Ключевой носитель JaCarta ГОСТ, работающий в режиме неизвлекаемого ключа
Канал обмена открытыми ключами	АРМ пользователя: — оперативная память.	Гипервизор: — оперативная память. Виртуальная машина: — оперативная память.

Наименование элемента	Организация 1	Организация 2
Канал обмена закрытыми ключами	АРМ пользователя: — USB шина; — оперативная память.	отсутствует
Канал обмена между криптоядрами	отсутствует (нет аппаратной части криптоядра)	АРМ пользователя: — USB шина; — оперативная память; — программный модуль USB-over-IP; — сетевой интерфейс. Корпоративная сеть организации 2. Гипервизор: — оперативная память; — сетевой интерфейс. Виртуальная машина: — сетевой интерфейс; — оперативная память; — программный модуль USB-over-IP.
Канал обмена открытыми данными	АРМ пользователя: — средства ввода-вывода; — оперативная память; — жесткий диск.	АРМ пользователя: — средства ввода-вывода; — оперативная память; — жесткий диск; — сетевой интерфейс. Корпоративная сеть организации 2. Гипервизор: — сетевой интерфейс; — оперативная память; — жесткий диск. Виртуальная машина: — сетевой интерфейс; — оперативная память; — жесткий диск.
Канал обмена защищенными данными	Интернет. Корпоративная сеть организации 1. АРМ пользователя: — жесткий диск; — оперативная память; — сетевой интерфейс.	Интернет. Корпоративная сеть организации 2. Гипервизор: — сетевой интерфейс; — оперативная память; — жесткий диск. Виртуальная машина:

Наименование элемента	Организация 1	Организация 2
		— сетевой интерфейс; — оперативная память; — жесткий диск.
Канал передачи времени	АРМ пользователя: — средства ввода-вывода; — оперативная память; — системный таймер.	Интернет. Корпоративная сеть организации 2, Гипервизор: — сетевой интерфейс; — оперативная память; — системный таймер. Виртуальная машина: — оперативная память; — системный таймер.
Канал передачи управляющих команд	АРМ пользователя: — средства ввода-вывода; — оперативная память. (Графический пользовательский интерфейс ПО КриптоАРМ)	Виртуальная машина: — оперативная память; — жесткий диск. (Скрипты автоматизации)
Канал приема результатов работы	АРМ пользователя: — средства ввода-вывода; — оперативная память. (Графический пользовательский интерфейс ПО КриптоАРМ)	Виртуальная машина: — оперативная память; — жесткий диск. (Файлы журналов работы скриптов автоматизации)

Угрозы безопасности верхнего уровня

Пояснения

Допущения, принятые при декомпозиции угроз:

1. Используются стойкие криптографические алгоритмы.
2. Криптографические алгоритмы используются безопасным образом в правильных режимах функционирования (например, ECB не применяется для шифрования больших объемов данных, учитывается допустимая нагрузка на ключ и т.д.).
3. Злоумышленникам известны все применяемые алгоритмы, протоколы и открытые ключи.
4. Злоумышленникам доступны для чтения все зашифрованные данные.
5. Злоумышленники в состоянии воспроизвести любые программные элементы в системе.

Декомпозиция

У1. Компрометация закрытых криптографических ключей.

У2. Зашифрование подложных данных от имени легитимного отправителя.

У3. Расшифрование зашифрованных данных лицами, не являющимися легитимными получателями данных (злоумышленниками).

У4. Создание электронной подписи легитимного подписанта под подложными данными.

У5. Получение положительного результата проверки электронной подписи подложных данных.
У6. Ошибочное принятие электронных документов к исполнению вследствие проблем в организации электронного документооборота.
У7. Несанкционированное ознакомление с защищаемыми данными во время их обработки СКЗИ.

У1. Компрометация закрытых криптографических ключей

Декомпозиция
У1.1. Получение закрытого ключа из хранилища закрытых ключей.

У1.2. Получение закрытого ключа из объектов среды функционирования криптосредства, в которых он может временно находиться.
Пояснения У1.2.
К объектам, в которых может временно храниться закрытый ключ, будут относиться:

1. оперативная память,
2. временные файлы,
3. файлы подкачки,
4. файлы гибернации,
5. файлы снапшотов «горячего» состояния виртуальных машин, включая файлы содержимого оперативной памяти виртуальных машин, поставленных на паузу.

У1.2.1. Извлечение закрытых ключей из работающей оперативной памяти за счет заморозки модулей ОЗУ, их извлечения и последующее считывание данных (freeze attack).
Пояснения У1.2.1.
Пример атаки.

У1.3. Получение закрытого ключа из канала обмена закрытыми ключами.
Пояснения У1.3.
Пример реализации данной угрозы будет приведен ниже.

У1.4. Несанкционированная модификация криптоядра, в результате которой закрытые ключи становятся известны злоумышленникам.

У1.5. Компрометация закрытого ключа в результате использования технических каналов утечки информации (ТКУИ).
Пояснения У1.5.
Пример атаки.

У1.6. Компрометация закрытого ключа в результате использования специальных технических средств (СТС), предназначенных для негласного съема информации («жучков»).

У1.7. Компрометация закрытых ключей в процессе их хранения вне СКЗИ.
Пояснения У1.7.

Например, пользователь хранит свои ключевые носители в ящике рабочего стола, из которого те легко могут быть извлечены злоумышленникам.

У2. Зашифрование подложных данных от имени легитимного отправителя

Пояснения

Данная угроза рассматривается только для схем шифрования данных с аутентификацией отправителя. Примеры подобных схем указаны в рекомендациях по стандартизации Р 1323565.1.004-2017 «Информационная технология. Криптографическая защита информации. Схемы выработки общего ключа с аутентификацией на основе открытого ключа». Для остальных криптографических схем данной угрозы не существует, поскольку шифрование производится на открытых ключах получателя, а они в общем случае известны злоумышленникам.

Декомпозиция

У2.1. Компрометация закрытого ключа отправителя:
У2.1.1. Ссылка: «Типовая модель угроз. Система криптографической защиты информации. У1. Компрометация закрытых криптографических ключей».

У2.2. Подмена входных данных в канале обмена открытыми данными.
Примечания У2.2.
Примеры реализации данной угрозы приведены ниже тут и тут.

У3. Расшифрование зашифрованных данных лицами, не являющимися легитимными получателями данных (злоумышленниками)

Декомпозиция

У3.1. Компрометация закрытых ключей получателя зашифрованных данных.
У3.1.1 Ссылка: «Типовая модель угроз. Система криптографической защиты информации. У1. Компрометация закрытых криптографических ключей».

У3.2. Подмена зашифрованных данных в канале обмена защищенными данными.

У4. Создание электронной подписи легитимного подписанта под подложными данными

Декомпозиция

У4.1. Компрометация закрытых ключей электронной подписи легитимного подписанта.
У4.1.1 Ссылка: «Типовая модель угроз. Система криптографической защиты информации. У1. Компрометация закрытых криптографических ключей».

У4.2. Подмена подписываемых данных в канале обмена открытыми данными.
Примечание У4.2.
Примеры реализации данной угрозы приведены ниже тут и тут.

У5. Получение положительного результата проверки электронной подписи подложных данных

Декомпозиция

У5.1. Злоумышленники перехватывают в канале передачи результатов работы сообщение об отрицательном результате проверки электронной подписи и подменяют его на сообщение с положительным результатом.

У5.2. Злоумышленники осуществляют атаку на доверие к сертификатам подписи (**СЦЕНАРИЙ — все элементы обязательны**):

У5.2.1. Злоумышленники генерируют открытый и закрытый ключ электронной подписи. Если в системе применяются сертификаты ключей электронной подписи, то они генерируют сертификат электронной подписи максимально похожий на сертификат предполагаемого отправителя данных, чье сообщение они хотят подделать.

У5.2.2. Злоумышленники вносят несанкционированные изменения в хранилище открытых ключей, наделяя сгенерированный ими открытый ключ необходимым уровнем доверия и полномочиями.

У5.2.3. Злоумышленники подписывают подложные данные ранее сформированным ключом электронной подписи и внедряют их в канал обмена защищенными данными.

У5.3. Злоумышленники осуществляют атаку с помощью просроченных ключей электронной подписи легального подписанта (**СЦЕНАРИЙ — все элементы обязательны**):

У5.3.1. Злоумышленники компрометируют истекшие (не действующие на данный момент) закрытые ключи электронной подписи легитимного отправителя.

У5.3.2. Злоумышленники подменяют время в канале передачи времени на время, при котором скомпрометированные ключи еще действовали.

У5.3.3. Злоумышленники подписывают подложные данные ранее скомпрометированным ключом электронной подписи и внедряют их в канал обмена защищенными данными.

У5.4. Злоумышленники осуществляют атаку с помощью скомпрометированных ключей электронной подписи легального подписанта (**СЦЕНАРИЙ — все элементы обязательны**):

У5.4.1. Злоумышленники делает копию хранилища открытых ключей.

У5.4.2. Злоумышленники компрометируют закрытые ключи одного из легальных отправителей. Тот замечает компрометацию, отзывает ключи, сведения об отзыве ключа помещаются в хранилище открытых ключей.

У5.4.3. Злоумышленники заменяют хранилище открытых ключей на ранее скопированное.

У5.4.4. Злоумышленники подписывают подложные данные ранее скомпрометированным ключом электронной подписи и внедряют их в канал обмена защищенными данными.

У5.5. <...> за счет наличия ошибок в реализации 2-го и 3-го этапа проверки электронной подписи:

Пояснения У5.5.

Пример реализации данной угрозы приведен ниже.

У5.5.1. Проверка доверия к сертификату ключа электронной подписи только по наличию доверия к сертификату, с помощью которого он подписан, без проверок CRL или OCSP.

Пояснения У5.5.1.

Пример реализации угрозы.

У5.5.2. При построении цепочки доверия к сертификату не анализируются полномочия выпускающих сертификатов
Пояснения У5.5.2.
Пример атаки в отношении SSL/TLS сертификатов.
Злоумышленники купили легитимный сертификат для своего e-mail. Затем они сделали мошеннический сертификат сайта и подписали его своим сертификатом. Если проверка полномочий проводиться не будет, то при проверке цепочки доверия она окажется корректной, и, соответственно, мошеннический сертификат тоже будет корректным.

У5.5.3. При построении цепочки доверия к сертификату не проверяются промежуточные сертификаты на отзыв.

У5.5.4. Обновление CRL происходит реже, чем их выпускает удостоверяющий центр.

У5.5.5. Решение о доверии к электронной подписи принимается раньше, чем получен OCSP-ответ о статусе сертификата, направленный по запросу, сделанному позже времени формирования подписи или раньше, чем получен следующий после формирования подписи CRL.
Пояснения У5.5.5.
В регламентах большинства УЦ временем отзыва сертификата считается время выпуска ближайшего CRL, содержащего информацию об отзыве сертификата.

У5.5.6. При получении подписанных данных не проверяется принадлежность сертификата отправителю.
Пояснения У5.5.6.
Пример атаки. Применительно к SSL-сертификатам: может не проверяться соответствие адреса вызываемого сервера значению поля CN в сертификате.
Пример атаки. Злоумышленники скомпрометировали ключи электронной подписи одного из участников платежной системы. После этого они взломали сеть другого участника и от его имени направили на расчетный сервер платежной системы платежные документы, подписанные скомпрометированными ключами. Если сервер анализирует только доверие и не проверяет соответствие, то мошеннические документы будут считаться легитимными.

У6. Ошибочное принятие электронных документов к исполнению вследствие проблем в организации электронного документооборота.

Декомпозиция
У6.1. Принимающая сторона не обнаруживает дублирование получаемых документов.
Пояснения У6.1.
Пример атаки. Злоумышленники могут перехватить передаваемый получателю документ, пусть даже криптографически защищенный, а затем многократно отправить его в канал передачи защищенных данных. Если получатель не выявляет дубли, то все получаемые документы будут восприниматься и отрабатываться как различные документы.

У7. Несанкционированное ознакомление с защищаемыми данными во время их обработки СКЗИ

Декомпозиция

У7.1. <...> вследствие утечки информации по сторонним каналам (side channel attack).

Пояснения У7.1.

Пример атаки.

У7.2. <...> вследствие нейтрализации защиты от несанкционированного доступа к информации, обрабатываемой на СКЗИ:

У7.2.1. Эксплуатация СКЗИ с нарушениями требований, описанных в документации на СКЗИ.

У7.2.2. <...>, осуществленной в за счет наличия уязвимостей в:

У7.2.2.1. <...> средствах защиты от несанкционированного доступа.

У7.2.2.2. <...> самой СКЗИ.

У7.2.2.3. <...> среде функционирования криптосредства.

Примеры атак

Рассмотренные ниже сценарии заведомо содержат ошибки организации информационной безопасности и служат только для иллюстрации возможных атак.

Сценарий 1. Пример реализации угроз У2.2 и У4.2.

Описание объекта

ПО АРМ КБР и СКЗИ СКАД Сигнатура установлены на физическом компьютере, не подключенном к вычислительной сети. В качестве ключевого носителя используется ФКН vdToken в режиме работы с неизвлекаемым ключом.

Регламент осуществления расчетов предполагает, что специалист по расчетам со своего рабочего компьютера скачивает электронные сообщения в открытом виде (схема старого АРМ КБР) со специального защищенного файлового сервера, затем записывает их на отчуждаемый носитель USB-флешку и переносит на АРМ КБР, где их шифрует и подписывает. После этого специалист переносит на отчуждаемый носитель защищенные электронные

сообщения, а потом через свой рабочий компьютер записывает их на файловый сервер, откуда они попадают на УТА и далее в платежную систему Банка России.

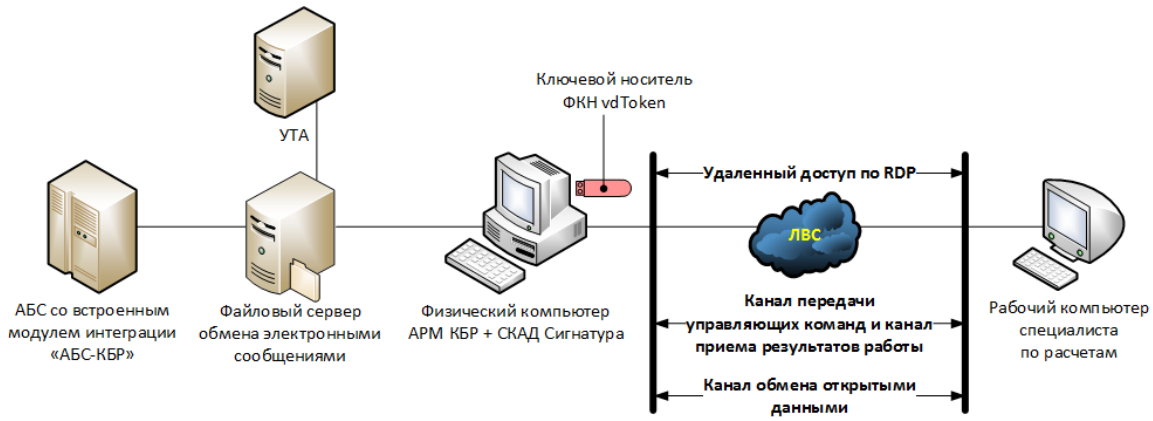
В данном случае каналы обмена открытыми и защищенными данными будут включать в себя: файловый сервер, рабочий компьютер специалиста и отчуждаемый носитель.

Атака

Злоумышленники несанкционированного устанавливают на рабочий компьютер специалиста систему удаленного управления и в момент записи на отчуждаемый носитель платежных поручений (электронных сообщений) в открытом виде подменяют содержимое одного из них. Специалист переносит платежные поручения на АРМ КБР, подписывает и шифрует их, не замечая подмены (например, из-за большого количества платежных поручений в рейсе, усталости и т.д.). После этого поддельное платежное поручение, пройдя через технологическую цепочку, попадает в платежную систему Банка России.

Сценарий 2. Пример реализации угроз У2.2 и У4.2.

Описание объекта



Компьютер с установленными АРМ КБР, СКАД Сигнатура и подключенным ключевым носителем ФКН vdToken функционирует в выделенном помещении без доступа со стороны персонала.

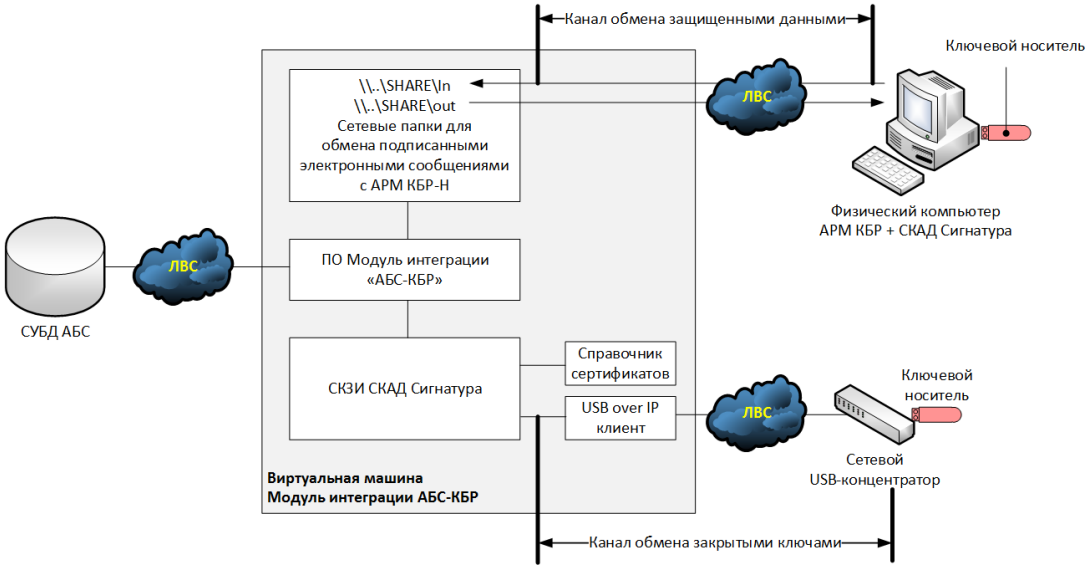
Специалист по расчетам подключается к АРМ КБР в режиме удаленного доступа по протоколу RDP.

Атака

Злоумышленники перехватывают реквизиты, используя которые специалист по расчетам осуществляет подключение и работу с АРМ КБР (например, за счет вредоносного кода на его компьютере). Затем проводят подключение от его имени и отправляют в платежную систему Банка России поддельное платежное поручение.

Сценарий 3. Пример реализация угрозы У1.3.

Описание объекта



Рассмотрим один из гипотетических вариантов реализации модулей интеграции «АБС-КБР» для новой схемы (АРМ КБР-Н), при которой электронная подпись исходящих документов происходит на стороне АБС. При этом будем считать, что АБС функционирует на базе операционной системы, не поддерживаемой СКЗИ СКАД Сигнатура, и, соответственно, криптографический функционал вынесен на отдельную виртуальную машину — модуль интеграции «АБС-КБР».

В качестве ключевого носителя используется обычный USB-токен, работающий в режиме извлекаемого ключа. При подключении ключевого носителя к гипервизору оказалось, что в системе нет свободных USB-портов, поэтому было решено подключить USB-токен через сетевой USB-концентратор, а на виртуальную машину установить клиент USB-over-IP, который будет осуществлять связь с концентратором.

Атака

Злоумышленники перехватили закрытый ключ электронной подписи из канала связи между USB-концентратором и гипервизором (данные передавались в открытом виде). Имея закрытый ключ, злоумышленники сформировали поддельное платежное поручение, подписали его электронной подписью и отправили в АРМ КБР-Н на исполнение.

Сценарий 4. Пример реализации угроз У5.5.

Описание объекта

Рассмотрим ту же схему, что и в предыдущем сценарии. Будем считать, что электронные сообщения, поступающие из АРМ КБР-Н, попадают в папку \\...\SHARE\In, а те, что отправляются в АРМ КБР-Н и дальше в платежную систему Банка России, — в \\...\SHARE\out. Также будем считать, что при реализации модуля интеграции списки отозванных сертификатов обновляются только при перевыпуске криптографических ключей, а также то, что электронные сообщения, поступившие в папку \\...\SHARE\In проверяются только на предмет контроля целостности и контроля доверия к открытому ключу электронной подписи.

Атака

Злоумышленники, воспользовавшись похищенными в предыдущем сценарии ключами,

подписали поддельное платежное поручение, содержащее сведения о поступлении денег на счет клиенту-мошеннику и внедрили его в канал обмена защищенными данными. Поскольку проверки того, что платежное поручение подписано именно Банком России не проводится, он принимается к исполнению.