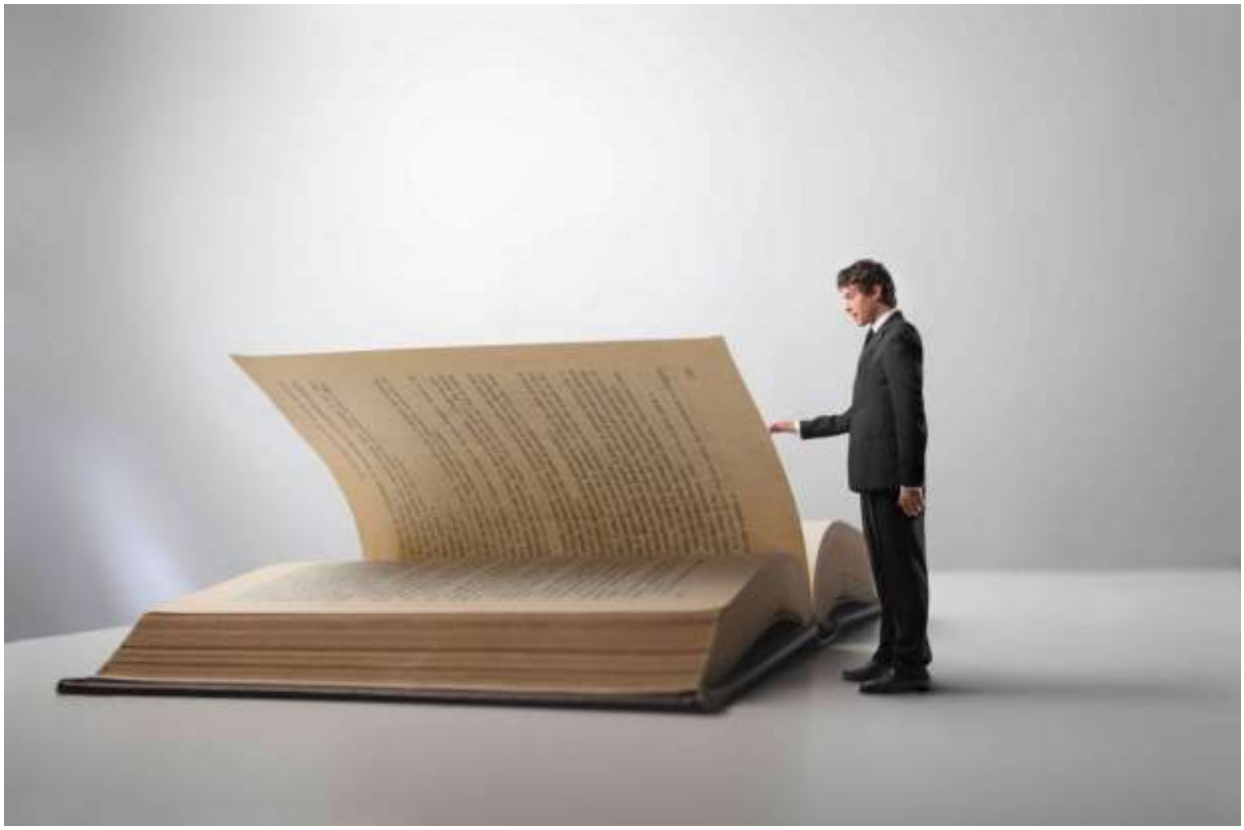
Аудит СКЗИ и криптоключей

С точки зрения информационной безопасности криптографические ключи являются критически важными данными. Если раньше, чтобы обокрасть компанию, злоумышленникам приходилось проникать на ее территорию, вскрывать помещения и сейфы, то теперь достаточно похитить токен с криптографическим ключом и сделать перевод через систему Интернет Клиент-Банк. Фундаментом обеспечения безопасности с помощью систем криптографической защиты информации (СКЗИ) является поддержание конфиденциальности криптографических ключей.

А как обеспечить конфиденциальность того, о существования чего вы не догадываетесь? Чтобы убрать токен с ключом в сейф, надо знать о существовании токена и сейфа. Как это не парадоксально звучит, очень мало компаний обладают представлением о точном количестве ключевых документов, которыми они пользуются. Это может происходить по целому ряду причин, например, недооценка угроз информационной безопасности, отсутствие налаженных бизнес-процессов, недостаточная квалификация персонала в вопросах безопасности и т.д. Вспоминают про данную задачу обычно уже после инцидентов, таких как например этот.

В данной статье будет описан первый шаг на пути совершенствования защиты информации с помощью криптосредств, а если точнее, то рассмотрим один из подходов к проведению аудита СКЗИ и криптоключей. Повествование будет вестись от лица специалиста по информационной безопасности, при этом будем считать, что работы проводятся с нуля.

Термины и определения



В начале статьи, дабы не пугать неподготовленного читателя сложными определениями, мы широко использовали термины криптографический ключ или криптоключ, теперь настало время усовершенствовать наш понятийный аппарат и привести его в соответствие действующему законодательству. Это очень важный шаг, поскольку он позволит эффективно структурировать информацию, полученную по результатам аудита.

1. **Криптографический ключ (криптоключ)** — совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе (определение из «розовой инструкции – Приказа ФАПСИ № 152 от от 13 июня 2001 г., далее по тексту – ФАПСИ 152).
2. **Ключевая информация** — специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока [ФАПСИ 152]. Понять принципиальное отличие между криптоключем и ключевой информации можно на следующем примере. При организации HTTPS, генерируются ключевая пара открытый и закрытый ключ, а из открытого ключа и дополнительной информации получается сертификат. Так вот, в данной схеме совокупность сертификата и закрытого ключа образуют ключевую информацию, а каждый из них по отдельности является криптоключом. Тут можно руководствоваться следующим простым правилом – конечные пользователи при работе с СКЗИ используют ключевую информацию, а криптоключи обычно используют СКЗИ внутри себя. В тоже время важно понимать, что ключевая информация может состоять из одного криптоключа.

3. **Ключевые документы** — электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах. (определение из Постановления Правительства № 313 от от 16 апреля 2012 г., далее по тексту – ПП-313)
   Простым языком, ключевой документ — это ключевая информация, записанная на носителе. При анализе ключевой информации и ключевых документов следует выделить, что эксплуатируется (то есть используется для криптографических преобразований – шифрование, электронная подпись и т.д.) ключевая информация, а передаются работникам ключевые документы ее содержащие.
4. **Средства криптографической защиты информации (СКЗИ)** – средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов, ключевые документы, аппаратные шифровальные (криптографические) средства, программно-аппаратные шифровальные (криптографические) средства. [ПП-313]
   При анализе данного определения можно обнаружить в нем наличие термина ключевые документы. Термин дан в Постановлении Правительства и менять его мы не имеем права. В тоже время дальнейшее описание будет вестись из расчета что к СКЗИ будут относится только средства осуществления криптографических преобразований). Данный подход позволит упростить проведение аудита, но в тоже время не будет сказываться на его качестве, поскольку ключевые документы мы все равно все учтем, но в своем разделе и своими методами.

Методика аудита и ожидаемые результаты

Основными особенностями предлагаемой в данной статье методике аудита являются постулаты о том, что:

- ни один работник компании не может точно ответить на вопросы, задаваемые в ходе аудита;
- существующие источники данных (перечни, реестры и др.) не точны или слабо структурированы.

Поэтому предлагаемая в статье методика, это своеобразный data minning, в ходе которого будут один и те же данные извлекаться из разных источников, а затем сравниваться, структурироваться и уточняться.

Приведем основные зависимости, которые нам в этом помогут:

1. Если есть СКЗИ, то есть и ключевая информация.
2. Если есть электронный документооборот (в том числе с контрагентами и регуляторами), то скорее всего в нем применяется электронная подпись и как следствие СКЗИ и ключевая информация.
3. Электронный документооборот в данном контексте следует понимать широко, то есть к нему будут относится, как непосредственный обмен юридически значимыми электронными документами, так и сдача отчетности, и работа в платежных или торговых системах и так далее. Перечень и формы электронного документооборота определяются бизнес-процессами компании, а также действующим законодательством.
4. Если работник задействован в электронном документообороте, то скорее всего у него есть ключевые документы.
5. При организации электронного документооборота с контрагентами обычно выпускаются организационно-распорядительные документы (приказы) о назначении ответственных лиц.
6. Если информация передается через сеть Интернет (или другие общественные сети), то скорее всего она шифруется. В первую очередь это касается VPN и различных систем удаленного доступа.
7. Если в сетевом трафике обнаружены протоколы, передающие трафик в зашифрованном виде, то применяются СКЗИ и ключевая информация.
8. Если производились расчеты с контрагентами, занимающимися: поставками средств защиты информации, телекоммуникационных устройств, оказанием услуг по передаче отёчности, услуг удостоверяющих центров, то при данном взаимодействии могли приобретаться СКЗИ или ключевые документы.
9. Ключевые документы могут быть как на отчуждаемых носителях (дискетах, флешках, токенах, …), так и записаны внутрь компьютеров и аппаратных СКЗИ.
10. При использовании средств виртуализации, ключевые документы могут храниться как внутри виртуальных машин, так и монтироваться к виртуальным машинам с помощью гипервизора.
11. Аппаратные СКЗИ могут устанавливаться в серверных и быть недоступны для анализа по сети.
12. Некоторые системы электронного документооборота могут находится в неактивном или малоактивном виде, но в тоже время содержать активную ключевую информацию и СКЗИ.
13. Внутренняя нормативная и организационно-распорядительная документация может содержать сведения о системах электронного документооборота, СКЗИ и ключевых документов.

Для добычи первичной информации будем:

- опрашивать работников;
- проводить анализ документации компании, включая внутренние нормативные и распорядительные документы, а также исходящие платежные поручения;
- проводить визуальный анализ серверных комнат и коммуникационных шкафов;
- проводить технических анализ содержимого автоматизированных рабочих мест (АРМ), серверов и средств виртуализации.

Конкретные мероприятия сформулируем позже, а пока рассмотрим конечные данные, которые мы должны получить по итогам аудита:

Перечень СКЗИ:
По каждому элементу перечня фиксируем следующие данные:

1. Модель СКЗИ. Например, СКЗИ Крипто CSP 3.9, или OpenSSL 1.0.1
2. Идентификатор экземпляра СКЗИ. Например, серийный, лицензионный (или регистрационный по ПКЗ-2005) номер СКЗИ
3. Сведения о сертификате ФСБ России на СКЗИ, включая номер и даты начала и окончания сроков действия.
4. Сведения о месте эксплуатации СКЗИ. Например, имя компьютера на которое установлено программное СКЗИ, или наименование технических средств или помещения где установлены аппаратные СКЗИ.

Данная информация позволит:

1. Управлять уязвимостями в СКЗИ, то есть быстро их обнаруживать и исправлять.
2. Отслеживать сроки действия сертификатов на СКЗИ, а также проверять используется ли сертифицированное СКЗИ в соответствии с правилами, установленными документацией или нет.
3. Планировать затраты на СКЗИ, зная сколько уже находится в эксплуатации и сколько еще есть сводных средств.

4. Формировать регламентную отчетность.

Перечень ключевой информации:
По каждому элементу перечня фиксируем следующие данные:

1. Наименование или идентификатор ключевой информации. Например, «Ключ квалифицированной ЭП. Серийный номер сертификата 31:2D:AF», при этом идентификатор следует подбирать таким образом, чтобы по нему можно было найти ключ. Например, удостоверяющие центры, когда посылают уведомления обычно идентифицируют ключи по номерам сертификатов.
2. Центр управления ключевой системой (ЦУКС), выпустивший данную ключевую информацию. Это может быть организация выпустившая ключ, например, удостоверяющий центр.
3. Физическое лицо, на имя которого выпущена ключевая информация. Эту информацию можно извлечь из полей CN сертификатов X.509
4. Формат ключевой информации. Например, СКЗИ КриптоПРО, СКЗИ Верба-OW, X.509 и т.д (или другими словами для использования с какими СКЗИ предназначена данная ключевая информация).
5. Назначение ключевой информации. Например, «Участие в торгах на площадке Сбербанк АСТ», «Квалифицированная электронная подпись для сдачи отчетности» и т.д. С точки зрения техники, в данном поле можно фиксировать органичения зафиксированные полях extended key usage и др сертификатов X.509.
6. Начало и окончание сроков действия ключевой информации.
7. Порядок перевыпуска ключевой информации. То есть знания о том, что нужно делать и как, при перевыпуске ключевой информации. По крайней мере желательно фиксировать контакты должностных лиц ЦУКС, выпустившего ключевую информацию.
8. Перечень информационных систем, сервисов или бизнес-процессов в рамках которых используется ключевая информация. Например, «Система дистанционного банковского обслуживания Интернет Клиент-Банк».

Данная информация позволит:

1. Отслеживать сроки действия ключевой информации.
2. В случае необходимости быстро перевыпускать ключевую информацию. Это может понадобится как при плановом, так при внеплановом перевыпуске.
3. Блокировать использование ключевой информации, при увольнении работника на которого она выпущена.
4. Расследовать инциденты информационной безопасности, отвечая на вопросы: «У кого были ключи для совершения платежей?» и др.

Перечень ключевых документов:
По каждому элементу перечня фиксируем следующие данные:

1. Ключевая информация, содержащаяся в ключевом документе.
2. Носитель ключевой информации, на который записана ключевая информация.
3. Лицо, ответственное за сохранность ключевого документа и конфиденциальность содержащейся в нем ключевой информации.

Данная информация позволит:

1. Перевыпускать ключевую информацию в случаях: увольнения работников, обладающих ключевыми документами, а также при компрометации носителей.
2. Обеспечивать конфиденциальность ключевой информации, путем инвентаризации носителей ее содержащих.

План аудита

Настало время рассмотреть практически особенности проведения аудита. Сделаем это на примере кредитно-финансовой организации или другими словами на примере банка. Данный пример выбран не случайно. Банки используют довольно большое число разношерстных систем криптографической защиты, которые задействованы в гигантском количестве бизнес-процессов, да и к тому же практически все банки являются Лицензиатами ФСБ России по криптографии. Далее в статье будет представлен план аудита СКЗИ и криптоключей, применительно к Банку. В тоже время, данный план может быть взят за основу при проведении аудита практически любой компании. Для удобства восприятия план разбит на этапы, которые в свою очередь свернуты в сполйеры.

Этап 1. Сбор данных с инфраструктурных подразделений компании

№	Действие	Ожидаемый результат и его использование
Источник – все работники компании.		
1	Делаем рассылку по корпоративной почте всем работниками компании с просьбой сообщить в службу информационной	Получаем электронные письма, на базе которых формируем **перечень ключевой информации** и **перечень ключевых документов**

№	Действие	Ожидаемый результат и его использование
	безопасности обо всех используемых ими криптографических ключах	
Источник – Руководитель Службы информационных технологий.		
1	Запрашиваем перечень ключевой информации и ключевых документов	С некоторой вероятностью Служба ИТ ведет подобные документы, будем использовать их для формирования и уточнения **перечней ключевой информации, ключевых документов и СКЗИ**
2	Запрашиваем перечень СКЗИ	
3	Запрашиваем реестр ПО, установленного на серверах и рабочих станциях	В данном реестре ищем программные СКЗИ и их компоненты. Например, КриптоПРО CSP, Верба-OW, Signal-COM CSP, Сигнатура, PGP, ruToken, eToken, КритоАРМ и др. На базе этих данных формируем **перечень СКЗИ.**
4	Запрашиваем перечень работников (вероятно техническая поддержка), помогающих пользователям по использованию СКЗИ и перевыпуску ключевой информации.	Запрашиваем у данных лиц аналогичную информацию, что и у системных администраторов
Источник – системные администраторы Службы информационных технологий.		
1	Запрашиваем перечень отечественных криптошлюзов (VIPNET, Континент, S-terra и др.)	В случаях, когда в компании не реализованы регулярные бизнес процессы управления ИТ и ИБ, подобные вопросы могут помочь вспомнить системным администраторам о существовании того или иного устройства или ПО. Используем данную информацию для получения **перечня СКЗИ**.
2	Запрашиваем перечень отечественных программных СКЗИ (VIPNET CSP, СКЗИ МагПро КриптоПакет, Crypton Disk, Secret Disk, …)	
3	Запрашиваем перечень маршрутизаторов, реализующих VPN для: а) связи офисов компании; б) взаимодействия с контрагентами и партнерами.	
4	Запрашиваем перечень информационных сервисов, опубликованных в Интернет (доступных из Интернет). Они могу включать: а) корпоративную электронную почту; б) системы обмена мгновенными сообщениями; в) корпоративные web-сайты; г) сервисы для обмена информации с партнерами и контрагентами (экстранет); д) системы дистанционного банковского обслуживания (если компания – Банк); е) системы удаленного доступа в сеть компании. Для проверки полноты предоставленных сведений сверяем их с перечнем правил Port forwarding пограничных межсетевых экранов.	Анализируя полученную информацию с высокой вероятностью можно встретить использование СКЗИ и криптоключей. Используем полученные данные для формирования **перечня СКЗИ и ключевой информации**.

№	Действие	Ожидаемый результат и его использование
5	Запрашиваем перечень информационных систем, используемых для сдачи отчетности (Такском, Контур и т. д.)	В данных системах используются ключи квалифицированной электронной подписи и СКЗИ. Через данный перечень формируем **перечень СКЗИ**, **перечень ключевой информации**, а также узнаем работников, пользующихся этими системами для формирования **перечня ключевых документов**.
6	Запрашиваем перечень систем внутреннего электронного документооборота (Lotus, DIRECTUM, 1С:Документооборот и др.), а также перечень их пользователей.	В рамках внутренних систем электронного документооборота могут встретиться ключи электронной подписи. На основании полученной информации формируем **перечень ключевой информации** и **перечень ключевых документов**.
7	Запрашиваем перечень внутренних удостоверяющих центров.	Средства, используемые для организации удостоверяющих центров, фиксируем в **перечне СКЗИ**. В дальнейшем будем анализировать содержимое баз данных удостоверяющих центров для выявления ключевой информации.
8	Запрашиваем информацию об использовании технологий: IEEE 802.1x, WiFi WPA2 Enterprise и систем IP-видеонаблюдения	В случае использования данных технологий мы можем обнаружить в задействованных устройствах ключевые документы.
Источник – Руководитель кадровой службы		
1	Просим описать процесс приема и увольнение работников. Фокусируемся на вопросе о том, кто забирает у увольняющихся работников ключевые документы	Анализируем документы (обходные листы) на предмет наличия в них информационных систем в которых могут использоваться СКЗИ.

Этап 2. Сбор данных с бизнес-подразделений компании (на примере Банка)

№	Действие	Ожидаемый результат и его использование
Источник – Руководитель служба расчетов (корреспондентских отношений)		
1	Просим предоставить схему организации взаимодействия с платежной системой Банка России. В частности, это будет актуально для Банков, имеющих развитую филиальную сеть, при которой филиалы могут подключать в платежную систему ЦБ напрямую	На базе полученных данных определяем местоположение платежных шлюзов (АРМ КБР, УТА) и перечень задействованных пользователей. Полученную информацию используем для формирования **перечня СКЗИ, ключевой информации и ключевых документов**.
2	Запрашиваем перечень Банков, с которыми установлены прямые корреспондентские отношения, а также просим рассказать кто занимается осуществлением переводов и какие технические средства используются.	Аналогично, как для платежной системы Банка России
3	Запрашиваем перечень платежных систем, в которых участвует Банк (SWIFT, VISA,	Аналогично, как для платежной системы Банка России

№	Действие	Ожидаемый результат и его использование
	MasterCard, НСПК, и т.д), а также месторасположение терминалов для связи	
Источник – Руководитель подразделения, отвечающего за предоставление дистанционных банковских услуг		
1	Запрашиваем перечень систем дистанционного банковского обслуживания.	В указанных системах анализируем использование СКЗИ и ключевой информации. На основании полученных данных формируем **перечень СКЗИ и ключевой информации и ключевых документов**.
Источник – Руководитель подразделения, отвечающего за функционирование процессинга платежных карт		
1	Запрашиваем реестр HSM	На базе полученной информации формируем **перечень СКЗИ, ключевой информации и ключевых документов**.
2	Запрашиваем реестр офицеров безопасности	
4	Запрашиваем информацию о компонентах LMK HSM	
5	Запрашиваем информацию об организации систем типа 3D-Secure и организации персонализации платежных карт	
Источник – Руководители подразделений, выполняющих функции казначейства и депозитария		
1	Перечень банков, с которыми установлены корреспондентские отношения и которые участвую в межбанковском кредитовании.	Используем полученную информацию для уточнения ранее полученных данных от службы расчетов, а также фиксируем информацию о взаимодействии с биржами и депозитариями. На базе полученной информации формируем **перечень СКЗИ и ключевой информации.**
2	Перечень бирж и специализированных депозитариев с которыми работает Банк	
Источник – Руководители служб финансового мониторинга и подразделений ответственных за сдачу отчетности в Банк России		
1	Запрашиваем информацию о том, как они отправляют сведения и получают сведения из ЦБ. Перечень задействованных лиц и технических средств.	Информационное взаимодействие с Банком России жестко регламентировано соответствующими документами, например, 2332-У, 321-И и многими другими, проверяем соответствие этим документам и формируем **перечни СКЗИ, ключевой информации и ключевых документов**.
Источник – Главный бухгалтер и работники бухгалтерии, занимающиеся оплатой счетов по внутрибанковским нуждам		
1	Запрашиваем информацию, о том, как происходит подготовка и сдача отчетности в налоговые инспекции и Банк России	Уточняем ранее полученные сведения
2	Запрашиваем реестр платежных документов, для оплаты внутрибанковских нужд	В данном реестре будем искать документы где: 1) в качестве адресатов платежей указаны удостоверяющие центры, специализированные операторы связи, производители СКЗИ, поставщики телекоммуникационного оборудования.

№	Действие	Ожидаемый результат и его использование
		Наименования данных компаний можно получить из Реестра сертифицированных СКЗИ ФСБ России, перечня аккредитованных удостоверяющих центров Минкомсвязи и других источников. 2) в качестве расшифровки платежа присутствуют слова: «СКЗИ», «подпись», «токен», «ключевой», «БКИ» и т. д.
Источник – Руководители служб по работе с просроченной задолженностью и управления рисков		
1	Запрашиваем перечень бюро кредитных историй и коллекторских агентств, с которыми работает Банк.	Совместно со службой ИТ анализируем полученные данные с целью выяснения организации электронного документооборота, на базе чего уточняем **перечни СКЗИ, ключевой информации и ключевых документов**.
Источник – Руководители служб документооборота, внутреннего контроля и внутреннего аудита		
1	Запрашиваем реестр внутренних организационно распорядительных документов (приказов).	В данных документах ищем документы, относящиеся к СКЗИ. Для этого анализируем наличие ключевых слов «безопасность», «ответственное лицо», «администратор», «электронная подпись», «ЭП», «ЭЦП», «ЭДО», «АСП», «СКЗИ» и их производных. После чего выявляем перечень работников Банка зафиксированных в этих документах. Проводим с работниками интервью на тему использования ими криптосредств. Полученную информацию отражаем в **перечнях СКЗИ, ключевой информации и ключевых документов.**
2	Запрашиваем перечни договоров с контрагентами	Стараемся выявить договора об электронном документообороте, а также договора с компаниями, занимающимися поставной средств защиты информации или оказывающими услуги в этой области, а также компаниями, предоставляющими услуги удостоверяющих центров и услуги сдачи отчетности через Интернет.
3	Анализируем технологию хранения документов дня в электронном виде	При реализации хранения документов дня в электронном виде обязательно применяются СКЗИ

Этап 3. Технический аудит

№	Действие	Ожидаемый результат и его использование
1	Проводим техническую инвентаризацию ПО установленного на компьютерах. Для этого используем: • аналитические возможности корпоративных систем антивирусной защиты (например, Антивирус Касперского умеет строить подобный реестр). • скрипты WMI для опроса компьютеров под управлением ОС Windows; • возможности пакетных менеджеров для опроса *nix систем; • специализированное ПО для инвентаризации.	Среди установленного ПО ищем программные СКЗИ, драйвера для аппаратных СКЗИ и ключевых носителей. На базе полученной информации обновляем **перечень СКЗИ**.
2	Осуществляем поиск ключевых документов на серверах и рабочих станциях. Для этого • Logon-скриптами опрашиваем АРМ в домене на предмет наличия сертификатов с закрытыми ключами в профилях пользователей и профилях компьютера. • На всех компьютерах, файловых серверах, гипервизорах ищем файлы с расширениями: crt, cer, key, pfx, p12, pem, pse, jks и др. • На гипервизорах систем виртуализации ищем примонтированные дисководы и образы дискет.	Очень часто ключевые документы представлены в виде файловых ключевых контейнеров, а также контейнерами, хранящимися в реестрах компьютеров, работающих под управлением ОС Windows. Найденные ключевые документы фиксируем в **перечне ключевых документов**, а содержащеюся в них ключевую информацию в **перечне ключевой информации.**
3	Анализируем содержание баз данных удостоверяющих центров	Базы данных удостоверяющих центров обычно содержат в себе данные о выпущенных этим центрами сертификатов. Полученную информацию заносим в **перечень ключевой информации** и **перечень ключевых документов**.
4	Проводим визуальный осмотр серверных комнат и коммутационных шкафов, ищем СКЗИ и аппаратные ключевые носители (токены, дисководы)	В некоторых случаях, невозможно провести инвентаризацию СКЗИ и ключевых документов по сети. Системы могут находится в изолированных сетевых сегментах, либо вообще не иметь сетевых подключений. Для этого проводим визуальный осмотр, в результатах которого должно быть установлены названия и назначение всего оборудования, представленного в серверных. Полученную информацию заносим в **перечень СКЗИ и ключевых документов**.

№	Действие	Ожидаемый результат и его использование
5	Проводим анализ сетевого трафика, с целью выявления информационных потоков, использующих шифрованный обмен	Шифрованные протоколы – HTTPS, SSH и др. позволят нам идентифицировать сетевые узлы на которых выполняются криптографические преобразования, и как следствие содержащие СКЗИ и ключевые документы.

Заключение

В данной статье мы рассмотрели теорию и практику проведения аудита СКЗИ и криптоключей. Как вы убедились, процедура эта довольно сложная и трудоемкая, но если к ней грамотно подходить вполне осуществимая. Будем надеется данная статья вам поможет в реальной жизни.

Спасибо за внимание.