Ответы на вопросы по итогам вебинара КриптоПРО

1. Есть некий защищённый контур, к которому разные организации будут иметь доступ через ГОСТ-VPN. 3 вопроса по организации: 1. Пользователь СКЗИ (не являются сотрудниками Владельца контура и Продавца, сторонняя организация). Покупает у Продавца СКЗИ (полный комплект). Пользуется СКЗИ для доступа в закрытый контур Владельца. 2. Продавец СКЗИ. Продаёт Пользователю полный комплект СКЗИ. В него входит лицензия, диск, сертификат VPN. 3. Владелец контура. Передаёт Пользователю через Продавца сертификат VPN и предоставляет доступ к закрытому контуру. По какой форме журнала кто должен вести учёт (для Органа криптографической защиты/для Обладателей конфиденциальной информации)? Как осуществлять расписку в журналах, если пользователи СКЗИ - сторонняя организация, в т.ч. в другом городе?

   Что касается передачи самого СКЗИ пользователю, который будет подключаться к ГОСТ-VPN: организация, которая передаёт доступ, должна быть лицензиатом ФСБ и учитывать, как для органа криптографической защиты. Возможно два факта передачи ключевых документов: пользователь сам у себя сформирует ключ для пользования, а сертификат будет для него выпущен владельцем контура, или владелец контура сразу для него выпустит и ключ шифрования, и сертификат. В первом случае владелец контура ничего не будет учитывать, а во втором - владелец контура должен в журнал учёта передачи ключевых документов занести сведения о факте генерации этого ключа и передачи его пользователю. Пользователь ничего учитывать не должен, если он не является обладателем конфиденциальной информации, а пользуется только для доступа в контур.

2. Может ли организация беспрепятственно передавать СКЗИ своим подведомственным организациям? или для этого требуется лицензия? какие документы необходимы для передачи?

   Для компаний действует закон о лицензировании отдельных видов деятельности и Постановление правительства №313, которое направлено на регулирование 28-ми видов работ, связанных с шифровальным, криптографическими средствам. Ни в законе, ни в постановлении нет никаких оговорок, касающихся типов организации, которым будет передано СКЗИ. Если юридическое лицо передаёт лицензии, либо аппаратные СКЗИ другому предприятию, то у него должна быть соответствующая лицензия ФСБ.

3. Где написано, что можно использовать один дистрибутив СКЗИ и несколько лицензий ПО?

   Чётких регламентов нигде нет. Следуя обычной логике - с одного диска дистрибутива возможно установить СКЗИ на большое количество рабочих мест. На практике обычно так и происходит.

4. Какая ответственность налагается за не выполнения требований 152 инструкцией и формуляров к СКЗИ?

   Проверять требования Инструкции ФАПСИ №152 инструкции уполномочена Федеральная служба безопасности, в регионах этим может заниматься специальный отдел лицензирования. Он приходит в организацию, которая обеспечивает защиту конфиденциальной информации с помощью СКЗИ, и смотрит соответствие закону. Если проверяющий выявляет противоречие, то оформляется предписание на устранение замечаний. В случае неисполнения предписания, фискальный орган через суд накладывает административное наказание. Зачастую распространяется на руководителя организации, и предусматривает штраф или иную меру, установленную в соответствии с административным кодексом правонарушении.

5. В каких случаях при эксплуатации СКЗИ требования Инструкции №152 выполнять не обязательно?

   Пункт 1.1. инструкции гласит: “Настоящая Инструкция определяет единый на территории Российской Федерации порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных ФАПСИ средств криптографической защиты (шифровальных средств) подлежащей в соответствии с законодательством Российской Федерации обязательной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну*(1).” В остальных случаях инструкция носит рекомендательный порядок.

6. Вопрос по облачным провайдерам: каким образом вести учёт?

   Применительно к КриптоПРО Cloud CSP, который структурно входит в КриптоПро CSP 5.0 и является частью этого СКЗИ. Поэтому его можно учитывать, как обычный СКЗИ.

7. Можно самостоятельно ставить в своей организации КриптоПро CSP?

   Можно.

8. Как корректно передать не экспортируемый ключ ЭП ГД (полученный в ФНС) в стороннюю организацию, ведущую бух учёт, взаимодействие с ПФР и т.п.?

   Вопрос целесообразно передать в ФНС и уточнить, что делать в данном случае. Мы можем предложить два выхода:
   - Организация, которая осуществляет сдачу отчётности должна иметь доверенность на представителя, на которого будет оформлен сертификат.
   - Передачу возможно осуществить по акту приёма-передачи с указанием, что принимающая сторона гарантирует применение ключа подписи только для сдачи, обязуется обеспечить его защиту от несанкционированного доступа, и стороны не считают передачу данных от этой стороны другой компрометацией этих данных.

9. Могу ли я у себя в организации самостоятельно ставить СКЗИ (КриптоПро, например)? Есть мнение, что если дословно читать ПП №313, то самому себе можно делать только тех. обслуживание, а ставить только с лицензией на крипту.

   Исходя из общего Федерального закона о лицензировании отдельных видов деятельности, на основе которого появилось Постановление правительства №313, если сотрудники организации устанавливают у себя на рабочем месте шифровальные криптографические средства, это не вид деятельности вовсе и лицензировать не нужно. Однако тот, кто будет устанавливать СКЗИ должен внимательно изучить техническую документацию, обеспечить корректную установку и настройку СКЗИ.

10. Где написано, что лицевой счёт должен быть на бумаге? Что нарушает порядок, когда лицевой счёт ведётся в файле, при необходимости распечатывается на бумаге и подписывается?

    Такого предписания нет. Лицевой счёт можно вести в файле и распечатывать документ при прохождении проверки.

11. Каким образом можно законно передать СКЗИ другому сотруднику или, например, подпись директора передать сисадмину для установки на сервер для организации ЭДО, например, в 1С?

    Есть два вида сертификатов - обезличенный и не обезличенный. Владельцем второго считается юридическое лицо или генеральный директор, т.е. лицо осуществляющее деятельность без доверенности. В этом случае передать СКЗИ можно через распоряжение или приказ генерального директора, где он поручит ответственному лицу поручит использовать ключ подписи на технических средствах, обеспечить его хранение и защиту от несанкционированного доступа и потенциальной компрометации данных.
    В обезличенном сертификате нет сведений о компании и для него может быть назначено ответственное лицо, в обязанности которого будет входить хранение и использование ключа подписи.

12. Коллеги, есть информация по реформированию этого документа (прим. – речь о Приказе ФАПСИ №152)?

    Такой информации нет.

13. Если СКЗИ выдаётся в головной организации для своих подчинённых организаций, то головная организация является ОКЗ?

    При создании ОКЗ в организации должен быть разработан локальный нормативный акт, определяющий какие функции будут возложены на подразделение в соответствии с ПКЗ №2005 и Инструкцией ФАПСИ №152. Если орган криптографической защиты создан

в том числе и для подведомственных организаций, подчинённых дочерних компаний, то это будет прописано в документе.

14. Расскажите подробнее про лицевые счета?

В соответствии с требованием ФАПСИ 152 пункт 27 на каждого пользователя СКЗИ необходимо вести лицевой счёт. Пункт звучит следующим образом:
«Все полученные обладателем конфиденциальной информации экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учёта пользователям СКЗИ, несущим персональную ответственность за их сохранность.»
Органы криптографической защиты заводят и ведут на каждого пользователя СКЗИ лицевой счёт, в котором регистрируют числящиеся за ним СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы

15. Можете рассказать о заполнении формуляров?

Формуляр поставляется вместе с диском дистрибутива, в него требуется вносить изменения, когда меняется СКЗИ. Заполнять необходимо разделы, связанные с проведением установки шифровального средств на рабочем месте.

16. Допустима ли передача СКЗИ по бухгалтерским документам, а именно по факту оформления универсального передаточного документа (не журнал, не акт передачи)?

Если аппаратные СКЗИ или лицензии продаются от одной организации в другую, то они передаются по бухгалтерским документам. Передача прав на использование осуществляется по акту приёма-передачи прав, независимо от ПО. Однако, применительно к шифровальным средствам, необходимо руководствоваться предписаниями Инструкции №152, если она обязательна к исполнению.

17. Лицевые счета, ЖПУ, аппаратные журналы подписываются УКЭП?

X-Control позволяет применять усиленную квалифицированную электронную подпись, поэтому если в организации принято решение использовать УКЭП для ведения журналов и лицевых счетов, то подписывать можно.

18. Где написано, что допуск должен осуществляться комиссией? Чему противоречит, если допуск осуществляет работник ОКЗ?

Это указано в пункте 21 Инструкции ФАПСИ №152.

19. Коллеги, такой кейс, организация лицензиат участвует в аукционе на поставку средств СКЗИ, выигрывает его, покупает у вендора СКЗИ и передаёт заказчику, должна ли организация лицензиат (поставщик) вести учёт этих СКЗИ в своих журналах учёта?

Осуществлять поставку может только организация-лицензиат ФСБ, которая должна вести учёт шифровальных средств, чтобы позже отчитаться кому, когда и в каком объёме были переданы эти средства. Поэтому учитывать нужно согласно Инструкции ФАПСИ №152.

20. Какая курьерская служба может доставлять СКЗИ в коммерческой компании (любая/спецсвязь/иное)? И почему? "32. СКЗИ и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или ..."

    На практике курьерская служба используется для передачи дистрибутивов СКЗИ, для передачи ключевых документов необходимо выбрать другой способ.

21. Какой временной период хранения Журналов учёта СКЗИ? И какой временной период хранения информации будет в X-Control? Как, и на каких носителях хранить информацию, которая отражается в X-Control, чтобы это удовлетворило требованиям контролирующего и проверяющего органам?

    Регулятор не выдвигал требований о необходимости защиты данных, обрабатываемых в системе. Данные X-Control хранятся в базе данных Postgres при этом возможно использование версии, сертифицированной ФСТЭК РФ. В ТЗ на внедрение заказчик может предъявить дополнительные требования к защите данных, которые могут быть перекрыты с помощью СЗИ от НСД, либо заказчик может самостоятельно обеспечить установку и настройку любых средств защиты.

22. Есть ли в системе где-то статус обучен/не обучен ли пользователь? Очень мало информации по АРМу, не увидел где заполняется версия ОС, наличие и версии антивирусных средств и средств защиты от НСД. Как обстоят дела с ведением схемы криптографической защиты конфиденциальной информации, которая также предусмотрена 152 инструкцией?

    Порядок обучения в X-Control указывается следующим образом: сначала пользователю назначают обучение в системе, а после прохождения выдают допуск о возможности самостоятельной работы с СКЗИ. В системе есть возможность указать номер аппаратного средства, при желании можно указать туда данные об ОС. Схема ОКЗ есть в отдельном разделе.

23. Есть интеграция в X-Control с 1С?

    Пока нет.

24. Каким SSL-сертификатом защищается веб-интерфейс x-Control? Можно ли на веб-сервер системы "повесить" ГОСТ сертификат?

    Сертификат выбирает заказчик.

25. Чем гарантирована целостность журналов, актов?

Целостность журналов обеспечивается применением электронной подписи, которая сопровождает в системе все ключевые действия.

26. В системе учёта можно ставить подписи пользователей СКЗИ?

    Да, можно.

27. X-Control это решение совместное с infosec? А существуют кейсы, когда за неисполнение 152 ФАПСИ наказывают? Я имею в виду конечных собственников СКЗИ.

    Нет, X-Control - это решение компании Spacebit.
    На нашей практике не было случаев привлечение к ответственности конечных собственников СКЗИ, т.е. пользователей.

28. Нам надо заключить соглашение с пользователями, что используем ПЭП?

    Да, обязательно должен быть определён порядок использования простой электронной подписи в компании.

29. X-Control - это web версия? Где хранятся данные? Если нет, то как защищаются данные при передаче и хранении?

    Да, это веб версия. Все данные хранятся на сервере, развёрнутом на мощностях заказчика.

30. Каким образом учитываются ключи ЭП в рамках плановой смены сертификатов, когда заявитель самостоятельно формирует запрос со своего рабочего места?

    Если заявитель самостоятельно формирует себе СКЗИ, к которым относятся ключ подписи, то у организации нет информации об этом ключе, значит учесть его нет возможности.
    В случае формирования ключей подписи через организацию, необходимо руководствоваться Инструкцией №152 по ведению журналов.

31. Каким образом реализована преемственность электронной системы после бумажной? т.е. у нас есть куча бумаги (акты, заключения, журналы и т.д.), есть ваша электронная система. Что сделать, чтобы отказаться от ведения, ранее учтённого СКЗИ на бумаге?

    Все сканы возможно перенести в систему.

32. При постановке СКЗИ на учёт нужно указать дату. Их несколько:1) Дата установки 2) Дата формирования лицензии собственно компанией КриптоПРО 3) Дата приобретения СКЗИ у поставщика (их товарная накладная) Все даты отличаются друг от друга. Так какую дату надо указывать в журнале учёта?

В журнале учёта необходимо указывать все даты.

33. Вы сказали, что регулятор не против применения квалифицированной электронной подписи для ведения электронных журналов, а как они относятся к применению не квалифицированной или простой ЭП?

Однозначная позиция регулятора нам неизвестна. Но мы можем предположить, что к ПЭП у регулятора может возникнуть вопрос, потому что она НЕ обеспечивает целостность электронных документов. Что касается КЭП и УКЭП, нам кажется, что регулятор возражать не должен.

34. X-Control есть интеграция с ДБО и УЦ?

Да, есть интеграция с УЦ КриптоПро и Юнисерт.

35. Подскажите, пожалуйста, существует ли нормативный документ, распространяющий действие положений Инструкции, утверждённой приказом ФАПСИ №152, на все СКЗИ, эксплуатируемые сегодня в России? На сегодняшний день: 1. ФАПСИ не является регулятором в области криптографии. 2. Криптосредства, сертифицированные ФАПСИ, о которых говорит пункт 1 этой инструкции уже не используются. 3. Сами положения инструкции, например, о решётках на окнах и поэкземплярном учёте криптосредств продублированы в гораздо более поздних документах ФСБ (пкз-2005, 378 приказ) 4. Эксплуатационная документация, например, на Vipnet, относит требования по помещениям к рекомендациям.

Правопреемником ФАПСИ в области шифровальных криптографических средств является ФСБ. Нормативно-правовой акт остался действующий, поэтому под “сертифицированными средствами ФАПСИ” понимаем “сертифицированные средства ФСБ”.
Касаемо несостыковок положений Инструкции и документации к СКЗИ, необходимо руководствоваться документами СКЗИ. Все документы, которые относятся СКЗИ, утверждены ФСБ и являются более “свежей” трактовкой.

36. Вопрос по продукту X-Control. Пользователь получает ключевые документы ЭЦП\СКЗИ первично, чем будет подписывать?

В данном случае можно использовать ПЭП соглашение или подписать документы собственноручно.

37. Как регуляторы относятся к ведению журналов в электронном виде с использованием стороннего ПО без учёта их через делопроизводство?

По нашему опыту, это не вызывает вопросов у регуляторов.

38. Какая ответственность налагается за не выполнения требований 152 инструкцией и формуляров к СКЗИ? КоАП РФ ст.13.12

Административная ответственность и срочное устранение всех недочётов.

39. X-Control есть в перечне Отечественного ПО?

    Да.

40. У X-Control есть только веб версия или также предусмотрено приложение?

    У продукта есть веб версия с серверной частью.

41. Откуда берётся эталонный экземпляр СКЗИ? Копируете с диска? Как доказываете, что это именно с диска (контрольная сумма)?

    Да, в следующем релизе будет проверка из системы контрольных сумм.

42. Нужно ли вести журнал лицензий СКЗИ?

    По 152 Инструкции ФАПСИ в прямую - нет, но регулятор лицензии спрашивает.

43. Система, я так понимаю, облачная? Там хранятся ПДн, да ещё и дистрибутивы можно хранить... Как ваша организация защищает ПДн своих пользователей? Есть ли сертификаты на данное ПО? Аттестована ли она? Где организованы хранилища?

    Решение ставится на мощностях заказчика, и задача шифрования канала также лежит на нем. Spacebit предоставляет инструмент для работы.

44. Если в организации изолированная сеть, X-Control способен работать автономно?

    Да, такая возможность есть.

45. Многие пользователи путаются - скачивают несертифицированные сборки, возможно ли реализовать две кнопки: 1. Сертифицированная версия 2. Актуальная версия?

    В системе X-Control есть модуль по скачиванию дистрибутивов самообслуживания, где указывается номер версии. Решить эту проблему можно внесением изменения в номер с указанием актуальной.
    В ближайших релизах добавлять кнопки не планируем, но при получении достаточной количества запросов от пользователей готовы пересмотреть решение.

46. Распространение дистрибутивов ПО третьим лицам, не нарушает лицензионные требования вендоров?

    КриптоПРО не запрещает распространять дистрибутивы шифровальных средств третьим лицам, поэтому лицензионный договор это не нарушает.

47. Открытые ключи пользователей хранятся в системе X-Control и как-то парсятся? Или дату истечения для оповещения руками указываем?

    Сами ключи в системе не хранятся, только информация о них. Её можно получать из УЦ или Excel файла.

48. Есть ли в X-Control контроль использования в сети новых токенов/смарт-карт? Как отследить новый сертификат и можно ли поймать пользователя?

    Такая функциональность есть в планах к реализации в течение года.

49. X-Control предназначен для автоматизации инструкции 152, а сам этот софт требует какой-то регистрации у пользователя или учёта?

    Нет, регистрации или учёта не требуется.

50. Как собирается информация т.е. что устанавливается на ПК пользователя (агенты, WMI или вручную)?

    Планируем собирать информацию с помощью агентов. Доработка запланирована к следующему релизу.

51. Согласно п. 29 152 ФАПСИ, обладатель конфиденциальной информации может разрешить передачу СКЗИ, ключевых документов, между допущенным к СКЗИ лицам по актам без обязательной отметки в журнале поэкземплярного учёта. Пример, в организации руководитель передаёт свою ЭП другому сотруднику для работы, который имеет допуск к СКЗИ. Достаточно ли при этом оформить акт передачи и не вносить никакие записи в журнал поэкземплярного учёта?

    Как уже указано в самом вопросе, Инструкция допускает не заносить сведения о передачи СКЗИ между допущенным лицам. Выдачу прав можно оформить только по акту.

52. В системе X-Control учитывать можно разные СКЗИ?

    Да, учитывать можно любые СКЗИ.

53. А VIpNet CSP вместо Cryptopro CSP поддерживается?

    К сожалению, нет.

54. В системе X-Control есть ли у пользователя СКЗИ свой интерфейс. С помощью которого можно, например, сменить пин, создать запрос на сертификат?

    На данный момент такой функционал не реализован. Но он запланирован для развития системы в ближайших релизах.

55. Предположим, что пришла проверка, а ваше ПО, X-Control, не загрузилась. Какие журналы мы покажем регулятору?

    Обычно о проверке уведомляют заранее, поэтому есть время подготовиться и распечатать журналы заранее.
    Дополнительной страховкой для компании может стать отказоустойчивый кластер.

56. Насколько отказоустойчивая у вас система X-Control? может ли теоретически злоумышленник (хакер, или внутренний нарушитель) повалить систему и слить её в общедоступные источники (условно). Станет ли отказ в обслуживании системы потерей для каждой организации, использующей X-Control? как хранятся персональные данные организации?

    Поскольку X-Control ставится на мощностях заказчика, многое зависит от уровня ИБ его компании. В качестве обеспечения дополнительного уровня безопасности в системе есть парольные политики, которые можно задать - требования к паролю, сессии и т.д.

57. Какие технические требования к X-Control (сервер, ОС, ДБ и т.п.)?

    Отправьте запрос на почту info@spacebit.ru, и мы направим всю необходимую документацию.

58. Что делать если нужно вести ЖУ СКЗИ по внешним пользователям (не в локальной сети)? Интеграция с web ресурсами по АО возможна?

    Возможна кастомная доработка системы под нужды заказчика. Сделайте запрос на info@spacebit.ru, и мы детально проработаем задачу.

59. Решение облачный токен - насколько сейчас законно? в части хранения квалифицированных сертификатов

    КриптоПРО DSS сейчас поддерживает мобильную подпись - когда ключ подписи хранится в смартфоне. В этом случае никаких вопросов по законности не возникает.
    В других случаях есть нюансы, связанные с толкованием 63-ФЗ «Об электронной подписи», истекшими сертификатами ФСБ на DSS и продолжающим действовать положительным заключением.

60. Каким образом в системе X-Control можно автоматизировать работу сотрудников ОКЗ и выдачу автоматически (допустим 100 установок) пронумерованных актов ввода в эксплуатацию (с заранее предустановленными серийными номерами АРМ), заключения о допуске пользователями? То есть, некая пакетная обработка документов, а не поштучная выдача?

    Пакетные операции в системе уже реализованы. Но на данный момент реквизиты АРМов проставляются именно в момент установки: есть заявка от организации, ОКЗ

готовит пакетные документы и идёт на установку с уже готовыми документами, которые позже будут подписаны.

61. Когда ждать КриптоПро УЦ на linux?

    В конце года ожидается положительное заключение на КриптоПРО УЦ 2.0 на Astra Linux.

62. Для КриптоПРО csp 5.0 подходят ключи лицензии от 4.0. Как учитывать 5.0 с введённым ключом от 4.0?

    Учитывать в журнале стандартно - КриптоПРО CSP 5.0., серию и номер лицензии, который будет введён в это СКЗИ.

63. По теме работы CSP с Apache - Где описаны изменения, которые не требуют проведения контроля встраивания СКЗИ?

    Для примера возьмем последнее сертифицированное СКЗИ линейки КриптоПро CSP – СКЗИ «КриптоПро CSP» 5.0 R2 класса КС1.
    Что касается необходимости работ по оценке влияния (он же - контроль встраивания)– см. документ «ЖТЯИ.00101-02 95 01. Правила пользования». Далее в этом документе читаем Раздел 4.
    В части этого раздела, начинающегося со слов «Исследования СФ не требуются…» - находим про Apache. В примечаниях указано, при соблюдении каких условий не нужно делать оценку влияния среды функционирования (СФ) на СКЗИ (идёт отсылка на Руководство администратора безопасности Linux).

64. Что будет с сертификатом соответствия на hsm после 01.03.2023?

    Если положительное заключение будет действовать после 01.03.2023, то сертификат соответствия будет продлён. В противном случае будем работать над новой версией HSM и сертифицировать.

65. Во многих пунктах 152 ФАПСИ указано, что какие-либо действия совершаются с согласия органа КЗИ. Т.е. на практике это выглядит как разрешение оформленное, например, на бумаге. В то же время ОКЗИ обязателен в организации, которая обрабатывает гос. тайну, а в организации с конфиденциальной информацией носит рекомендательный характер. Если в организации не создавался ОКЗИ, то допускается выполнять пункты приказа без получения каких-либо разрешений, т.е. фактически положения приказа о получении разрешений ОКЗИ можно опустить?

    Да, если в организации не было принято решение о формировании органа криптозащиты, то обычно всю ответственность на себя берет генеральный директор согласовывает вопросы, связанные с учётом СКЗИ.

66. Будет ли поддержка у HSM и УЦ под другие linux-based ОС?

В ближайших планах разработка HSM и УЦ на Astra Linux. Что касается ответных частей HSM, то на подключённых серверах может использоваться любая операционная система, где работает КриптоПРО CSP 5.0.

67. Когда ожидаются заключения на новые HSM?

За три месяца до окончания срока действия сертификата инициируется процедура продления заключений или оформление новых заключений и сертификатов.

68. Уц 2.0 продлите сертификат?

Сертификат на УЦ 2.0 был продлён недавно.

69. Как вести поэкземплярный учёт электронных подписей (ЭП), если приходится делать копии ЭП руководителя на сотрудников для работы в различных информационных системах, которые требуют только подпись руководителя? Как это правильно отражать на бумаги?

В настоящий момент сертификаты, которые создаются на руководителя в ФНС России, формируют ключи подписи в не экспортируемом виде. Это значит, что копировать их нельзя.
Если рассмотреть общий случай, где копирование возможно, то учитывать ключи подписи или шифрования необходимо именуя их в части экземпляров – экземпляр №1, экземпляр №2.

70. Реализован «Кузнечик» или «Магма» на КриптоПро HSM?

На данный момент нет, но будут реализованы в следующей версии HSM. Для получения более подробной информации рекомендуем создать обращение на портале технической поддержки КриптоПРО (support.cryptopro.ru).

71. Есть дистрибутив удостоверяющего цента для Astra Linux в открытом доступе?

Пока нет. Когда сборка пройдёт все проверки и получит положительное заключение, она будет выложена на сайте КриптоПРО.

72. Будет ли реализован учёт машинных носителей информации (МНИ) в электронной системе X-Control из первого доклада?

Есть возможность зарегистрировать МНИ в системе, как ключевые носители и вести учёт.

73. Скажите ваше мнение по поводу исполнения требований 152 приказа ФАПСИ при использовании КриптоПро HSM (как облачного хранилища закрытых ключей). В частности

– пользователь расписывается в журнале и берет на себя обязанность в сохранности ключа, но доступа к хранилищу не имеет и повлиять на сохранность не может, как не может повлиять и на конфиденциальность ключа (он виртуальный и находится где-то), а ответственность за подписанные документы есть.

В данном случае нужно исходить из требований Инструкции №152 по умолчанию, но понимать, что при виртуальном режиме хранения ключей, документы должны отличаться от текущих. Для пользователей не целесообразно брать в учётных документах ответственность за ключи шифрования, которые хранятся в централизованной системе, поскольку вопрос безопасности относится к оператору информационных систем, который использует HSM, и к ПО, которое обеспечивает надёжное хранение ключей пользователей.

74. У СКЗИ КриптоПро CSP 5.0 13.08.2022 закончился сертификат соответствия рег. номер СФ/114-3726 от 13.08.2019г. Планируется ли продление данного сертификата соответствия?

    На данный момент сертификат продлён.

75. Что делать если в бумаге более 10.000 записей не переносить же вручную? В X-Control есть функционал по импорту скан копий есть, или будет разрабатываться? А импорт из Excel?

    В X-Control функционала по импорту скана записей пока нет, но уже реализован перенос данных из Excel.

76. Как правильно вести учёт ключей, хранящихся в реестре АРМ или на жёстком диске? Какими документами регламентируется этот учёт?

    Если ключи шифрования подписи хранятся на жёстком диске, то учёту подлежит сам жёсткий диск, т.е. системный блок компьютера. Его можно учитывать, как и другие ключевые носители и документы.

77. Лицензия Крипто-про CSP 5.0 — СКЗИ? Её нужно учитывать ли только дистрибутив?

    В Инструкции ФАПСИ №152 про лицензии не говорят, только про экземпляры СКЗИ. В законе есть понятия «учётные номера» и «учётные индексы», которые предоставляются только на дистрибутивы. Однако, мы рекомендуем учитывать и лицензии, и дистрибутивы.

    Если полностью отказаться от учёта лицензий, то регулятор и пользователь системы получат данные не соответствующие действительности: получатся разные значения по учёту дистрибутивов и по количеству непосредственно эксплуатируемых экземпляров СКЗИ, которые развёрнуты на рабочих местах пользователя. Поэтому учитывать необходимо всё для своего же удобства.

78. Обязательно ли исполнять требования формуляров СКЗИ организацией, если обрабатываемая с использованием СКЗИ информация не подлежит защите на основании законодательства?

    В данной ситуации все зависит от цели использования СКЗИ:

    - Если сертифицированный СКЗИ используется для защиты конфиденциальности информации и это необходимо делать в силу закона, то необходимо выполнять требования Положения ПКЗ 2005 и Инструкции ФАПСИ №152.
    - Если организация самостоятельно приняла решение защищать информацию, которую в силу закона защищать не обязательно, и определяет используемые средства, то ответственность по выполнению требований полностью лежит на этой организации.
    - Если рассматривать применения квалифицированной электронной подписи, где также используются сертифицированные шифровальные средства, то необходимо соблюдать требования Инструкции, предъявляемые к формулярам и документации для шифровально-криптографических средств.

79. Не вяжутся понятия "Добираться до ключа" и "сохранять конфиденциальность". Кто ответственный за ключ в облаке?

    За ключ в облаке несёт ответственность оператор информационной системы, в которой используется и хранятся средства криптозащиты. Также ответственность лежит на пользователе за сохранение всех ключей и кодов аутентификации, которые применяются для доступа к ключам, хранящимися в ЦОДе.

80. Вопрос по учёту дистрибутивов СКЗИ. СКЗИ - это дистрибутив на носителе с документацией (формуляр, правила пользования). СКЗИ имеет учётный номер производителя. Сейчас КриптоПро, в частности, можно приобретать без покупки дистрибутива - покупая только лицензию. Как в этом случае учитывать СКЗИ?

    Сейчас возможна покупка только лицензии на право использования, однако дистрибутив необходимо получить либо на носителе, либо скачать с сайта. Если скачивать ПО с сайта КриптоПРО, то необходима предварительная регистрация. Далее в личном кабинете отразится информация о дистрибутивах, которые были скачены, и серийных номерах. Этот номер можно учитывать в журналах.

81. Вы пишете, что можно устанавливать КриптоПро csp ставить можно самим, а по требованиям 313 постановления установка СКЗИ лицензируемый вид деятельность. возможно только в п. 20

    Если вы, как сотрудник, устанавливаете на своё рабочее место СКЗИ, то вы никакой вид деятельности не осуществляете. Поэтому тут лицензировать нечего.

82. Приказ ФАПСИ говорит об едином порядке использования средств сертифицированных СКЗИ, сейчас средства сертифицируются ФСБ либо ФСТЭК и получается, что данный порядок де факто не работает?

Порядок работает. ФСБ, как правопреемник ФАПСИ в части применения и использования шифровальных, криптографических средств, несёт все необходимые фискальные функции по контролю применения шифровальных средств.

83. Можно ли интегрировать серверный КриптоПро CSP 5.0 с КриптоПро Cloud CSP в качестве хранилища ключей ЭП, например, вместо HDIMAGE на этом же сервере? Будет ли такое решение архитектурно правильным, согласованным? Будет ли эта интеграция требовать обязательных процедур оценок влияния и проверок корректности?

КриптоПро Cloud CSP, как частичка СКЗИ КриптоПро CSP, работает с ключами только через КриптоПро DSS. Поэтому какая-либо интеграция КриптоПро Cloud CSP с серверным КриптоПро CSP не получится.

84. Если та же КриптоПро CSP используется исключительно для авторизации, например, на госуслугах, требуется ли в таком случае её учёт именно как СКЗИ?

Если авторизация осуществляется с помощью шифровально-криптографических средств, то и требования к их учёту, как и у остальных СКЗИ.

85. Проводилось ли тестирование функционала по шифрованию писем на ГОСТу в почтовых клиентах в ОС AstraLinux, как это сейчас реализовано в MS Outlook?

Вопрос не по профилю компании, лучше переадресовать производителю ОС AstraLinux.

86. 63-ФЗ «Об электронной подписи» написано, что Физ. лицо получает лично в УЦ и использует в организации, каким образом учитывается? Ответственный должен бегать за сотрудниками чтобы учитывать в журнале?

Сотрудник «бегать» ни за кем не должен. Если физ. лицо получило подпись, то оно эти ключи подписи само учитывает, как физ. лицо. Если эти ключи подписи будут использоваться ещё в организации, то необходимо сделать соответствующие доверенности и обеспечить учёт со стороны организации о выдачи этих доверенностей и к каким ключам относится.

87. Продаём СКЗИ в сторонние организации в разные субъекты РФ. Является ли надлежащим подтверждением передачи СКЗИ отметка в Журнале поэкземплярного учёта о передаче СКЗИ по акту-приёма передачи (указываем дату подписания и номер документа)? Физически получить подпись о вручении не представляется возможным.

Если происходит передача дистрибутива и лицензий, то в журналах должна быть отметка в разделе «указание исходящего номера», например, отправки дистрибутива. Если такое не применимо, то у вас должно быть другое подтверждение факта передачи, которое можно зафиксировать в журнале.

88. А в Журнале СКЗИ ведётся учёт только для сертифицированных средств защиты информации или нужно указывать, например, ключи Open SSL?

Обычно ведётся учёт сертифицированных средств защиты информации, но если существует потребность дополнительной регистрации других средств, в том числе и не сертифицированные, то это не ограничивается. Лучше сделать два журнала – один согласно требованиям Инструкции ФАПСИ №152, второй для собственного учёта других средств.

89. По обучению перед допуском в X-Control по факту опрос ведёт один человек, а на выгрузке прописывается комиссия. В чем разница, если будет делаться просто подпись в журнале - пользователь и работник ОКЗ?

Согласно Инструкции, подписывать допуск к работе с СКЗИ должна комиссия, которая состоит, как минимум, из двух человек. Возможно, по факту опрос проведёт один человек, но подтвердить допуск должны двое.

90. У X-Control есть какие-нибудь сертификаты по безопасности (ФСБ или ФСТЭК)?

Компания сейчас находится в процессе получения таких сертификатов.

91. Если у нас ведётся журнал поэкземплярного учёта СКЗИ, в котором и так указывается что именно выдано пользователю, какое СКЗИ, номер лицензии или ключа, то зачем Лицевой счёт, который по факту дублирует информацию из журнала?

Это требование Инструкции ФАПСИ №152, и мы не можем уйти от него.

92. Сложности в заполнении формуляра нет только в том случае, если мало пользователей. Если пользователей 2 000?

В данном случае к формуляру можно приложить страничку с расширенной информацией — где устанавливался, кем использовался и тому подобное, например, добавить всю информацию об установки в X-Control, выгрузить файл Excel с формой, распечатать и приложить к формуляру. Далее заверить все одной подписью.

93. Как учитывать дистрибутив СКЗИ скачанный с официального сайта разработчика?

Касательно КриптоПро CSP – регистрируйтесь в личном кабинете на сайте, скачивайте дистрибутив. В ЛК отразится информация о стачивании, учётный номер и индекс, номер экземпляра. Именно эту информацию можно заносить в учётные документы.

94. Разрешено уничтожать ключевую информацию под две подписи в журнале учёта или только по акту? Если да две подписи, они должны быть сотрудников ОКЗ или сотрудника ОКЗ и пользователя?

Согласно Инструкции ФАПСИ №152, уничтожение большого объёма ключевых документов может быть оформлено актом, подписанным комиссией. Если ключ в единичном экземпляре, то он может быть уничтожен либо пользователем, либо сотрудником ОКЗ под расписку в соответствующих журналах. Также важно смотреть какие требования в технической и эксплуатационной документации на СКЗИ.

95. Если мы передаём СКЗИ, то в 100% мы должны передавать под подпись в журнале? нельзя в журнале сослаться на, то что передано по Бухгалтерскому документу?

Нет, подпись в журнале не обязательна. Можно сослаться на бухгалтерский документ. Тогда в журналах необходимо указать наименование и номер документа, по которому совершена передача.

96. 1) приказом создаётся орган криптографической защиты 2) после этого вся ответственность за целостность и достоверность на них.

Орган криптографической защиты проводит обучение и производит учёт СКЗИ. Ответственность при эксплуатации лежит на лице, который СКЗИ использует.

97. Можно ли передавать формуляр в электронном виде (в поставке с диском СКЗИ)?

Передавать можно, но на формуляре в электронном виде не будет отметок производителя. Поэтому при проверке регуляторов могут возникнуть вопросы к правомерности передачи СКЗИ.
Но если вы легитимно скачиваете дистрибутив с сайта, то полученный формуляр в электронном виде вы можете распечатать и вложить к учётной документации, объяснив цепочку действий.

98. Где разворачивается сервер?

Сервер разворачивается в организации, где осуществляется учёт в соответствии с Инструкцией ФАПСИ №152.

99. ПО (дистрибутивы) - СКЗИ. Считаются ли лицензии СКЗИ? При передаче лицензий нужен ли учёт прм-прд СКЗИ, если да, то почему, ведь сами по себе лицензии (лицензионные ключи) не являются СКЗИ?

В части четвертой гражданского кодекса РФ прописано, что является программным обеспечением, а также как передаются права использования. Дистрибутив – понятие материальное, т.к. можем его потрогать физически. Лицензии соотносятся с тем экземпляром СКЗИ который вы будете использовать, и как бы «введены» в него. Поэтому, учитывать необходимо и дистрибутив, и лицензии.

100. Список носителей, поддерживаемых X-Control?

Можно учитывать информацию о любых носителях.

101. Существует ли у ФСБ положение о сертификации СКЗИ для защиты информации, не составляющей ГОС тайну?

В рамках Положения ПКЗ 2005 ведётся разработка шифровальных, криптографических средств и вводятся основные понятия, которые с этим связаны. Это основной документ в части разработки СКЗИ и проведения тематических исследований СКЗИ, и именно на этом этапе исследуется соответствие СКЗИ каким-либо требованиям (требованиям к средствам ЭП и т.д.). . Результат - положительное заключение ФСБ.
Следующий шаг – оформление сертификата соответствия.
Формально сертификация происходит в рамках системы сертификации (для СКЗИ на сертификате соответствия в самом верху это написано – система сертификации РОСС RU.0001.030001). Если в Яндексе ввести «система сертификации РОСС RU.0001.030001», то в первой десятке выйдет ссылка с текстом этой системы. Может есть документ и свежее, но он чисто формальный. Повторюсь – основное это ПКЗ-2005.

102. Подгружаются ли сканы формуляров в X-Control?

Да, можно подгрузить.

103. Есть опыт интеграции X-Control с DLP и SIEM?

Пока нет, но мы открыты для новых вызовов.

104. Пользователь подписывает своей ЭП в "журнале" X-Control факт установки СКЗИ на свой АРМ и т.п. Получается, всем пользователям СКЗИ нужен веб-доступ к X-Control? И нужны учётки для каждого?

Возможно организовать процесс учёта СКЗИ только за подписью сотрудников ОКЗ, ограничивая доступ сотрудников в систему. В таком случае будет необходимо фиксировать передачу СКЗИ пользователю на бумаге.

105. КриптоПРО HSM и 152 приказ ФАПСИ. Как оформить с точки зрения документов места хранения ключей (фактическое хранение не соответствует требованиям 152 приказа)? Как оформить клонирование ключа (ведь он выпускается не в системе, он туда записывается), что нарушает требования работы с СКЗИ? Юридически пользователь несёт ответственность за подпись этим ключом, однако за бекапы, за систему отвечает ИТ, за сохранность ключей в хранилище, наверное, ИБ или тоже ИТ - теоретически лиц, имеющих доступ к ключам за спиной владельца много, а отвечает за подпись только он. Как на это смотрит 152 приказ?

Согласно приказу ФАПСИ №152 необходимо учитывать СКЗИ, в данном случае КриптоПРО HSM, и ключевые документы, которые находятся в нём. Ключи формируются и хранятся непосредственно в HSM, все криптографические операции

выполняются в системе. Понятия клонирования там не присутствует, поэтому в этой части все легитимно и не противоречит закону.
Что касается разделения ответственности, то она лежит и на операторе ИС, где эксплуатируется HSM, и на пользователе, который должен обеспечить сохранность кодов аутентификации и доступа к своим ключам. Поэтому с точки зрения Инструкции ФАПСИ №152 оператор ИС может учесть своё СКЗИ, КриптоПРО HSM, и все ключи, которые в нем находятся.

106. ЭП это аналог моей собственной подписи. я не могу отпилить руку и отдать бухгалтеру. я могу дать бухгалтеру доверенность и подпись должна быть его (личная). Как раз для нивелирования данной проблемы и выпустили новый 63 ФЗ, появилась машиночитаемая доверенность.

Утверждение, что «ЭП – это аналог моей собственной подписи» сейчас не совсем верно. Такая трактовка была верна в законе об «Электронно-цифровой подписи», где условия равнозначности так и говорили «электронно-цифровая подпись равнозначна собственноручной». Сейчас электронный документ, подписанный электронной подписью, равнозначен электронному документу, подписанному собственноручной подписью. Из-за такого различия и появилась возможность выдавать сертификаты на юридических лиц.

107. Есть ли предположение, когда нельзя будет легитимно использовать КриптоПро УЦ 2.0 на windows? После окончания сертификата соответствия? Есть ли возможность миграции ВСЕХ данных с УЦ windows на УЦ Астра? Какая БД используется в УЦ Астра?

Пока будет действовать сертификат соответствия на Windows, КриптоПро УЦ 2.0 можно будет использовать для автоматизации деятельности аккредитованного удостоверяющего цента. По истечению срока действия сертификата соответствия для выдачи квалифицированных сертификатов использовать ПО будет невозможно. Но уже в конце года должны появиться исполнения для УЦ 2.0, которые будут работать на Astra Linux. Организации, являющиеся удостоверяющими центрами, которые планируют оказывать услуги по выпуску сертификатов будут переходить на УЦ на Astra Linux.