Часто задаваемые вопросы DiSec-W и МГК-3

1. **Вопрос: Участник обмена получил письмо с приглашением получить СКЗИ. Куда идти?**
   Ответ: Все участники обмена кроме московского региона могут получить СКЗИ в своём ТУ, сроки и порядок получения необходимо уточнить в обслуживающем ТУ.

   Для участников обмена Московского региона, дата и время получения СКЗИ отражена в приложении к информационному письму «О переводе УО на взаимодействие с ТШ КБР через защищённые каналы связи». Выдача СКЗИ клиентам Московского региона будет осуществляться по адресу ул. Свободы, 57, корпус 1, строение 2. При необходимости можно связаться с ЦЭПС ДИТ по телефонам: 8 (495) 987-75-83, 8 (495) 987-75-87 и согласовать иные дату и время получения СКЗИ.

2. **Вопрос: Где почитать информацию про DiSec-w? Как настраивать?**
   Ответ: На сайте Банка России в разделе https://www.cbr.ru/development/mcirabis/Involve_EM/ опубликован «Порядок подключения КБР к ТШ КБР с использование средств криптографической защиты каналов DiSec-W».

3. **Вопрос: Есть ли клиент DiSec-w под линукс?**
   Ответ: Нет, только под Windows.

4. **Вопрос: Когда появится клиент DiSec-w под линукс?**
   Ответ: Не ранее 4 квартала 2023 года.

5. **Вопрос: Может ли DiSec-w работать вместе с Cisco AnyConnect одновременно на одной ПЭВМ?**
   Ответ: Да, может.

6. **Надо ли настраивать что-то ещё кроме DiSec-w?**
   Ответ: Да, надо изменить настройки ПК АРМ КБР-Н/СПФС согласно «Порядку подключения КБР к ТШ КБР с использование средств криптографической защиты каналов DiSec-W», опубликованному на сайте Банка России в разделе https://www.cbr.ru/development/mcirabis/Involve_EM/.

   Обращаем внимание, что при нажатии кнопки "Проверить соединение" в АРМ КБР-Н, КБР-СПФС происходит проверка соединения только с основным сервером. Переключение на резервные сервера происходит только при штатной работе АРМа с ролью Оператора в случае недоступности основного сервера. В протоколе отображается только попытка подключения к основному серверу.

7. **Минимальная версия ОС Windows? Можно ли использовать Windows 7/8/8.1/сервер?**

Ответ: В соответствии с формуляром на СКЗИ DiSec-w должна использоваться операционная система Windows 10, либо Windows Server 2016. Работа на других версиях операционных систем не гарантируется, консультации по работе СКЗИ на таких версиях операционных систем не оказываются. Поддерживается только 64-разрядные версии ОС Windows 10, либо Windows Server 2016.

8. **Может ли участник обмен получить больше/меньше рекомендованного количества СКЗИ?**
   Ответ: в соответствии с направленным информационным сообщением клиент может запросить большее число СКЗИ. Для этого необходимо либо направить письмо в адрес Банка России о выделении дополнительных СКЗИ, либо обратить с соответствующим запросом в ЕСПП, указав желаемое к получению число СКЗИ с обоснованием необходимости. Меньше также получить можно проинформировав через ЕСПП.

9. **Возможна ли установка СКЗИ DiSec-W на одном ПЭВМ с АРМ КБР-Н / АРМ КБР-СПФС, либо необходимо разносить ПО на разные ПЭВМ?**
   Ответ: Установка СКЗИ DiSec-W на одном ПЭВМ с АРМ КБР-Н / АРМ КБР-СПФС возможна. СКЗИ DiSec-W не конфликтует с СКАД «Сигнатура».

10. **Можно ли установить один экземпляр СКЗИ на несколько ПЭВМ?**
    Ответ: Для каждой ПЭВМ используется свой собственный экземпляр СКЗИ DiSec-w, в том смысле, что для каждой установки должен использоваться свой собственный учётный номер СКЗИ.

    При этом для нескольких инсталляций можно использовать один и тот же дистрибутивный комплект (компакт-диск), затем, при запросе на активацию, для каждого установленного экземпляра СКЗИ нужно делать запрос на активацию с индивидуальным номером СКЗИ.

    Активация и использование одного экземпляра СКЗИ DiSec-W одновременно на нескольких ПЭВМ является нарушением правил пользования СКЗИ DiSec-W.

11. **Должен ли токен с закрытым ключом всегда быть присоединен к ПЭВМ?**
    Ответ: Да, извлечение токена с закрытым ключом приведёт к нарушению работы DiSec-W.

12. **Можно ли в акте и доверенности на получение указывать сразу несколько комплектов DiSec-W, или на каждый комплект должен составляться свой акт и доверенность?**
    Ответ: Да, в доверенности можно указать сразу несколько комплектов СКЗИ для получения.

13. **Когда планируется вывод из эксплуатации Cisco Anyconnect? Будет ли Cisco Anyconnect использоваться как резервное решение в случае проблем с СКЗИ DiSec-W ?**
    Ответ: Настоятельно рекомендуется переходить на использование ГОСТ-туннелей в установленные сроки, использование Cisco AnyConnect допускается в качестве резервного способа подключения до 30.06.2023.

14. **Участник обмен решил использовать аппаратное решение (например, Dionis-NX). Нужно ли в таком случае получать DiSec-W.**
    Ответ: Программный продукт DiSec-w распространяется Банком России бесплатно для выполнения требований 747-П. Если клиент самостоятельно и за свой счёт приобрел ПАК Dionis-NX для организации защиты канала, то его можно использовать вместо DiSec-W, соответственно в таком случае участник обмена может отказаться от использования DiSec-w и не получать его вовсе, либо получить в ограниченном количестве, например, для целей резервирования или тестирования. В данном случае решение принимается участником обмена.

15. **При генерации запроса, появляется диалоговое окно «Инициализация выполнена», далее нажимается Ок, однако выбор ключевого носителя не запускается – приложение закрывается. (п.4 Инструкции по изготовлению КИ КБР)**
    Ответ:
    Необходимо выполнить следующие действия:
    - Удалить МГК. Удалить драйвер токена. Перезагрузить АРМ.
    - Установить МГК с правами администратора.
    - Остановить антивирус или добавить путь C:\Program Files (x86) \Factor-TS\Request3 в исключения.
    - Выполнить первый запуск с правами администратора.
    - По инструкции сформировать запрос/ключ на внешний flash носитель

16. **При запуске DiSec-W, иконка не появляется в трее, или исчезает при попытке вызвать всплывающее меню.**
    Ответ:
    Необходимо отключить (перевести в состояние Disable) следующие службы и перезагрузить АРМ:
    - Модули ключей IPSec для обмена ключами в Интернете и протокола IP с проверкой подлинности (IKE and AuthIP IPSec keying Modules).
    - Агент политики IPSec (IPSec Policy Agent)

17. **В логе СКЗИ «DiSec» присутствует фраза "Обновление CRL выполнено с ошибками для сертификата пользователя"?**

    лог имеет вид:

    04-10-2022 13:03:49,760: +++++++++ [[CD-TUZ01]]: УСТАНОВЛЕН ТУННЕЛЬ [8426A8C0 <=> 1B92D50B] +++++++++

    04-10-2022 13:03:49,760: [[CD-TUZ01]]: ВСЕ ТУННЕЛИ для целевых объектов ДОБАВЛЕНЫ

    04-10-2022 13:03:55,619: [[CD-TUZ01]]: Обновление CRL выполнено с ошибками для сертификата пользователя. См. Журнал
    04-10-2022 13:03:55,650: [[CD-TUZ01]]: Начата процедура обновления CRL для сертификата оппонента
    04-10-2022 13:04:05,618: [[CD-TUZ01]]: Обновление CRL выполнено с ошибками для сертификата оппонента. См. Журнал

Ответ: В окне «Настройка PKI пользователя» необходимо убрать галку «Выполнить до установки туннеля» и установить галку «Выполнить после установки туннеля».

18. **Где взять данные для генерации закрытого ключа?**
    Ответ:
    Клиенты московского региона руководствуются «Регламентом взаимодействия Банка России и Клиента (косвенного участника Клиента), Пользователя при управлении криптографическими ключами» опубликованном на сайте Банка России в разделе https://cbr.ru/development/mcirabis/Involve_EM/
    Клиенты ТУ должны руководствоваться локальными регламентами, определяющими их взаимодействие с ТУ в части ключевой информации.

19. **Что делать с канальными/прикладными учётными записями?**
    Ответ:
    Канальные учётные записи использовались для работы ПО Cisco AnyConnect. После перехода на использование СКЗИ DiSec-W необходимость использования канальных учётных записей отпадает.
    При этом Вы можете поддерживать актуальным пароль от канальной учётной записи если хотите сохранять возможность подключения через Cisco AnyConnect на время переходного периода до 30.06.2023
    Обращаем внимание, что в случае использования ПО Cisco Anyconnect необходимо соответствующим образом настроить работу ПК АРМ КБР-Н/СПФС.
    Для промышленного взаимодействия в ПК АРМ КБР-Н/СПФС должен быть указан адрес промышленного прикладного сервера ТШ КБР 172.16.18.211 и порт 7777.
    Для тестового взаимодействия в ПК АРМ КБР-Н/СПФС должен быть указан адрес тестового прикладного сервера ТШ КБР 172.16.19.211 и порт 7777.

20. **После установления туннеля недоступны прикладные порты 7777/1414/9697?**
    Ответ:
    Средствами СКЗИ Disec-W устанавливается одновременно 4 VPN-туннеля до 4-х ЦОД ТШ КБР.
    Личный кабинет ТШ КБР должен быть доступен на TCP-порту 9697 по всем четырём прикладным ip-адресам.

    TCP-порты 7777(http) и 1414(mq) для прикладного взаимодействия ПК АРМ КБР-Н/СПФС доступны **не менее, чем на одном** из четырёх прикладных ip-адресов.

    В АРМ КБР-Н/СПФС для этих целей настраивается основной и резервные прикладные ip-адреса, по которым АРМ осуществляет перебор. Таким образом по TCP портам 7777 и 1414 должен отвечать хотя бы один из четырёх адресов, но не обязательно все.

21. **В логах ПК АРМ КБР-Н / АРМ КБР-СПФС присутствуют ошибки при подключении к узлам ТШ КБР (connection timeout)?**
    Ответ:

В конфигурации ПК АРМ КБР-Н / АРМ КБР-СПФС на вкладке «Настройки СВК/ТШ КБР» должны быть указаны как основной адрес подключения, так и резервные адреса.

Резервные адреса должны быть указаны с номером порта! Например, 172.21.1.58:7777

Сервис должен отвечать хотя бы по одному из четырёх адресов, но не обязательно все. Также необходимо установить таймаут соединения в размере 60 секунд или более.

22. При проверке соединения администратором ПК АРМ КБР-Н/АРМ КБР – СПФС (кнопка «Проверить соединение») возникает ошибка «Невозможно соединиться с удалённым сервером»?

Ответ:

На текущий момент ПК АРМ КБР-Н / АРМ КБР-СПФС проверяет только доступность основного адреса подключения. При этом активный сервис может располагаться в данный момент времени на другом, резервном адресе (см. Вопрос 20). Доработка ПК АРМ КБР-Н / АРМ КБР-СПФС, позволяющая выполнять проверку сразу как основного адреса, так и резервных адресов, будет выполнена в одном из ближайших релизов.

На текущий момент, для проверки соединения средствами ПК АРМ КБР-Н / АРМ КБР-СПФС можно поочередно указывать прикладные ip-адреса ТШ КБР в качестве основного ip-адреса ТШ КБР и нажимать кнопку «Проверить соединение». Если хотя бы один адрес ответил успешно, значит всё настроено правильно.

После проверки соединения необходимо убедиться, что в качестве основного и резервных адресов подключения указаны все четыре разные прикладные ip-адреса ТШ КБР.