Об Инструкции по организации, обеспечению функционирования и безопасности каналов передачи данных в интегрированной информационной системе Евразийского экономического союза

Решение Коллегии Евразийской экономической комиссии от 5 июля 2022 года № 98.

В целях реализации пунктов 23 и 30 Протокола об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза (приложение № 3 к Договору о Евразийском экономическом союзе от 29 мая 2014 года) Евразийская экономическая коллегия **решила**:

1. Утвердить прилагаемую Инструкцию по организации, обеспечению функционирования и безопасности каналов передачи данных в интегрированной информационной системе Евразийского экономического союза.

2. Настоящее Решение вступает в силу по истечении 10 календарных дней с даты его официального опубликования.

Председатель Коллегии
Евразийской экономической комиссии *М. Мясникович*

УТВЕРЖДЕНА
Решением Коллегии
Евразийской экономической комиссии
от 5 июля 2022 г. № 98

ИНСТРУКЦИЯ

по организации, обеспечению функционирования и безопасности каналов передачи данных в интегрированной информационной системе Евразийского экономического союза

Общие положения

1. Настоящая Инструкция разработана в соответствии с Решением Коллегии Евразийской экономической комиссии от 2 июня 2016 г. № 50 (ДСП) и определяет порядок организации, обеспечения функционирования и безопасности защищенных каналов передачи данных между интеграционным и национальными сегментами интегрированной информационной системы Евразийского экономического союза (далее соответственно – интегрированная система, Союз), а также между национальными сегментами интегрированной системы (далее – защищенные каналы передачи данных).

2. Положения настоящей Инструкции направлены на достижение устойчивого функционирования и выполнения заданных функций защищенными каналами передачи

данных в условиях возможного воздействия нарушителем, возможности которого определены моделью угроз безопасности информации и действий потенциального нарушителя, утвержденной Решением Коллегии Евразийской экономической комиссии от 26 сентября 2017 г. № 122 (ДСП).

3. Положения Инструкции распространяются на деятельность в сфере осуществления межгосударственного обмена данными с использованием интегрированной системы, осуществляемую Евразийской экономической комиссией (далее – Комиссия), а также операторами интеграционных шлюзов и доверенных третьих сторон национальных сегментов интегрированной системы.

Определения

4. Для целей настоящего документа используются понятия, которые означают следующее:

"администратор защищенной сети передачи данных" – уполномоченное лицо (лица) Комиссии, осуществляющее управление защищенной сетью передачи данных, в том числе непосредственное конфигурирование и управление компонентами защищенной сети передачи данных в соответствии с настоящей Инструкцией и эксплуатационной документацией на такие компоненты;

"администратор криптошлюзов" – уполномоченное лицо (лица) участника защищенной сети передачи данных, осуществляющее непосредственное конфигурирование криптошлюзов, размещенных у участника защищенной сети передачи данных в соответствии с технической и эксплуатационной документацией на криптошлюзы и настоящей Инструкцией;

"защищенная сеть передачи данных" – виртуальная, наложенная на физические каналы передачи данных защищенная транспортная сеть, обеспечивающая множественные сетевые соединения между криптошлюзами, построенная с использованием технологий межсетевого экранирования и частных виртуальных сетей, использующая для защиты каналов передачи данных криптографический стандарт, утверждаемый Комиссией;

"ключевой блокнот" – оптический носитель информации, содержащий предварительно созданную последовательность случайных чисел (гамму), используемую для генерации криптографических ключей и инициализирующих последовательностей программных датчиков случайных чисел в криптошлюзах;

"ключевой дистрибутив" – файл, формируемый с использованием ключевого центра , предназначенный для инициализации криптошлюза и содержащий комплект криптографических ключей и справочников защищенной сети передачи данных;

"ключевой центр" – программно-аппаратный автономный компонент центра управления защищенной сетью, с использованием которого обеспечивается назначение

ключевых блокнотов для криптошлюзов, формирование справочной и ключевой информации защищенной сети передачи данных;

"контролируемая зона" – пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и (или) транспортных средств;

"криптошлюз" – аппаратно-программное средство криптографической защиты информации, выполняющее в составе защищенной сети функции зашифрования, расшифрования и имитозащиты трафика от заданных адресатов, фильтрации сетевых соединений в соответствии с заданной политикой безопасности, трансляции сетевых адресов, автоматической настройки IP-адресов устройств, маршрутизации сетевых пакетов, доставки обновлений ключевой и справочной информации защищенной сети передачи данных, экстренного стирания ключевой информации;

"магистральная телекоммуникационная сеть" – телекоммуникационная IP-сеть поставщика услуг аренды каналов связи, построенная с применением технологии многопротокольной коммутации по меткам пакетов данных (MPLS) и обеспечивающая сетевую связность национальных сегментов интегрированной системы между собой, а также с интеграционным сегментом;

"орган криптографической защиты информации" – уполномоченное структурное подразделение Комиссии, разрабатывающее и осуществляющее мероприятия по организации и обеспечению безопасности хранения, обработки и передачи информации ограниченного доступа с использованием средств криптографической защиты информации, а также безопасности применяемых средств криптографической защиты информации в соответствии с правилами их пользования;

"техническое сопровождение защищенной сети передачи данных" – консультирование участников защищенной сети передачи данных по вопросам работы криптошлюзов;

"участник защищенной сети передачи данных" – Комиссия или оператор интеграционных шлюзов и доверенных третьих сторон национальных сегментов интегрированной системы, подключенные в установленном порядке к защищенной сети передачи данных;

"центр управления защищенной сетью передачи данных" – программно-аппаратный компонент подсистемы информационной безопасности интеграционного сегмента Комиссии интегрированной системы, с использованием которого обеспечивается регистрация криптошлюзов в защищенной сети передачи данных, назначение связей между криптошлюзами, рассылка обновлений ключевой и справочной информации защищенной сети передачи данных.

Организация и обеспечение функционирования защищенной сети передачи данных

5. Защищенная сеть передачи данных состоит из центра управления защищенной сетью передачи данных, размещаемого в помещениях Комиссии, и криптошлюзов,

владельцем которых является Комиссия либо участник защищенной сети передачи данных и устанавливаемых в помещениях по месту размещения участников защищенной сети передачи данных.

6. Криптошлюзы, используемые в защищенной сети передачи данных, должны быть предназначены для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну (государственные секреты) и иметь действующие сертификаты соответствия требованиям к средствам криптографической защиты информации, выданные уполномоченным органом государства нахождения их производителя.

7. Криптошлюзы, владельцем которых является Комиссия, передаются Комиссией участникам защищенной сети передачи данных в безвозмездное временное пользование по их запросу. Финансовое обеспечение передачи, за исключением затрат на импортно-экспортные операции в соответствии с законодательством государства участника защищенной сети передачи данных, осуществляются за счет средств, предусмотренных бюджетом Союза на соответствующий финансовый год, в рамках работ на создание, обеспечение функционирования и развитие интегрированной системы.

8. Криптошлюзы, владельцами которых являются участники защищенной сети передачи данных, должны быть совместимы с центром управления защищенной сетью передачи данных, технологиями передачи данных в защищенной сети передачи данных , ключевой системой защищенной сети передачи данных, а также не должны снижать общий уровень защищенности и надежности защищенной сети передачи данных.

9. Центр управления защищенной сетью и криптошлюзы должны размещаться в пределах контролируемой зоны Комиссии или участников защищенной сети передачи данных соответственно.

10. Ключевые блокноты, ключевые дистрибутивы, криптошлюзы с установленными ключевыми дистрибутивами, устройства аутентификации криптошлюзов относятся к материальным носителям, содержащим информацию ограниченного доступа, и должны быть защищены от несанкционированного доступа к ним третьих лиц.

11. Криптошлюзы, установленные у участников защищенной сети передачи данных , должны находиться в работоспособном состоянии 365 дней в году, 7 дней в неделю и 24 часа в сутки, быть доступными для других участников защищенной сети передачи данных при защищенном взаимодействии с использованием магистральной телекоммуникационной сети, за исключением времени проведения плановых профилактических работ.

12. Администрирование и техническое сопровождение защищенной сети передачи данных осуществляется администратором защищенной сети передачи данных самостоятельно либо с привлечением сторонних организаций. Привлекаемые для администрирования и технического сопровождения защищенной сети организации

осуществляют такую деятельность в соответствии с законодательством государства пребывания Комиссии, настоящей Инструкцией и эксплуатационной документацией на компоненты защищенной сети передачи данных.

Функции органа криптографической защиты информации, администратора и участников защищенной сети передачи данных

13. Орган криптографической защиты информации выполняет следующие функции:

а) организует оснащение участников защищенной сети передачи данных криптошлюзами;

б) организует обучение администраторов криптошлюзов правилам работы с криптошлюзами;

в) определяет готовность участника защищенной сети передачи данных к самостоятельному использованию криптошлюзов;

г) ведет поэкземплярный учет криптошлюзов и средств криптографической защиты информации, используемых в составе центра управления защищенной сетью передачи данных, технической и эксплуатационной документации к ним, ключевых блокнотов, материальных носителей ключевых дистрибутивов и иной ключевой информации, используемой для обеспечения функционирования защищенной сети передачи данных;

д) ведет реестр участников защищенной сети передачи данных;

е) обеспечивает своевременное получение ключевых блокнотов и создание ключевых дистрибутивов в центре управления защищенной сетью передачи данных, а также их распределение, рассылку и учет;

ж) принимает решение о вводе в действие очередных серий ключевых блокнотов и заблаговременно информирует участников защищенной сети передачи данных о дате и времени такого ввода;

з) обеспечивает защиту технической и эксплуатационной документации, ключевых блокнотов и ключевых дистрибутивов от несанкционированного доступа третьих лиц в рамках своих полномочий;

и) обеспечивает уничтожение неиспользованных или выведенных из действия ключевых блокнотов и (или) ключевых дистрибутивов;

к) осуществляет контроль за соблюдением условий использования средств криптографической защиты информации, используемых в составе защищенной сети передачи данных, установленных технической и эксплуатационной документации к ним, и настоящей Инструкцией;

л) проводит проверки условий использования криптошлюзов и средств криптографической защиты информации, используемых в составе центра управления защищенной сетью передачи данных, на соответствие требованиям технической, эксплуатационной документации и настоящей Инструкции.

14. Администратор защищенной сети передачи данных выполняет следующие функции:

а) консультирует участников защищенной сети передачи данных по вопросам функционирования этой сети;

б) информирует орган крипторафической защиты информации о потребности в ключевых блокнотах с учетом количества криптошлюзов в составе защищенной сети передачи данных с учетом необходимости минимизации времени простоя защищенной сети передачи данных при смене ключей;

в) обеспечивает хранение холодного резерва криптошлюзов (не менее 3 единиц) для обеспечения оперативной замены неисправных криптошлюзов участников защищенной сети передачи данных;

г) в центре управления защищенной сетью передачи данных осуществляет формирование структуры защищенной сети передачи данных на основании информации о структуре интеграционного сегмента Комиссии интегрированной системы и информации, предоставленной администраторами криптошлюзов;

д) осуществляет формирование ключевых дистрибутивов для криптошлюзов интеграционного сегмента Комиссии интегрированной системы и криптошлюзов национальных сегментов, входящих в состав защищенной сети передачи данных;

е) совместно с администраторами криптошлюзов обеспечивает ввод в действие и вывод из обращения криптошлюзов, ключевых блокнотов и ключевых дистрибутивов;

ж) извещает администраторов криптошлюзов:

о приостановлении работы защищенной сети передачи данных или отдельных ее сегментов для выполнения плановых (регламентных) профилактических и внеплановых ремонтных работ;

о приостановлении работы сети защищенной сети передачи данных или отдельных ее сегментов в случае компрометации ключевой информации;

о возобновлении работы защищенной сети передачи данных или отдельных ее сегментов после реализации мер по восстановлению работоспособности;

з) обеспечивает эксплуатацию центра управления защищенной сетью в составе интеграционного сегмента Комиссии интегрированной системы в соответствии с технической, эксплуатационной документацией и настоящей Инструкцией;

и) обеспечивает администрирование и мониторинг функционирования защищенной сети передачи данных;

к) обеспечивает в рамках своих полномочий, в соответствии с должностной инструкцией защиту центра управления защищенной сетью передачи данных, технической и эксплуатационной документации, ключевых блокнотов и ключевых дистрибутивов от несанкционированного доступа третьих лиц;

л) принимает необходимые меры для поддержания работоспособности защищенной сети передачи данных;

м) приостанавливает по согласованию с участниками защищенной сети передачи данных ее функционирование не более чем на 4 часа в месяц для проведения обслуживания технических средств;

н) принимает меры во взаимодействии с администраторами криптошлюзов по восстановлению работоспособности защищенной сети передачи данных;

о) осуществляет организацию ремонтно-восстановительных работ оборудования защищенной сети передачи данных и контроль за выполнением профилактических работ;

п) осуществляет организацию работ по замене неисправных криптошлюзов, владельцем которых является Комиссия, в случае невозможности их ремонта на месте;

р) подключает к защищенной сети передачи данных новых участников защищенной сети передачи данных в соответствии с настоящей Инструкцией.

15. Администратор криптошлюзов выполняет следующие функции:

а) совместно с администратором защищенной сети передачи данных выполняет ввод в действие криптошлюзов, ключевых блокнотов и ключевых дистрибутивов;

б) обеспечивают контроль за техническим состоянием криптошлюзов;

в) принимает необходимые меры для поддержания работоспособности криптошлюзов 365 дней в году, 7 дней в неделю и 24 часа в сутки;

г) обеспечивает обновление программного обеспечения криптошлюзов по согласованию с администратором защищенной сети передачи данных;

д) осуществляет управление правилами сетевого доступа из защищенной сети передачи данных в национальный сегмент интегрированной системы участника защищенной сети передачи данных;

е) по согласованию и совместно с администратором защищенной сети передачи данных выполняет ввод в действие новых серий ключевых блокнотов;

ж) информирует администратора защищенной сети передачи данных о неисправности криптошлюзов;

з) приостанавливает работу криптошлюзов по согласованию с администратором защищенной сети передачи данных для проведения обслуживания технических средств ;

и) приостанавливает работу криптошлюзов по согласованию с администратором защищенной сети передачи данных для проведения ремонтно-восстановительных работ ;

к) осуществляет контроль за выполнением регламентных профилактических работ;

л) оповещает уполномоченный орган, орган криптографической защиты информации и администратора защищенной сети передачи данных о факте компрометации ключевых блокнотов и ключевых дистрибутивов;

м) приостанавливает работу криптошлюзов по согласованию с администратором защищенной сети передачи данных в случае компрометации ключевых блокнотов, ключевых дистрибутивов;

н) осуществляет организацию работ по восстановлению работоспособности криптошлюзов и защищенной сети передачи данных;

о) обеспечивает в рамках своих полномочий, определенных должностным регламентом, защиту криптошлюзов, технической и эксплуатационной документации, ключевых блокнотов и ключевых дистрибутивов от несанкционированного доступа третьих лиц.

16. Участники защищенной сети передачи данных выполняют следующие функции:

а) из числа своих работников назначают администраторов криптошлюзов;

б) информируют орган криптографической защиты информации о вновь назначенных администраторах криптошлюзов, их контактных данных;

в) обеспечивают получение и размещение на своей территории криптошлюзов в соответствии с требованиями настоящей Инструкции, подключение их к источнику бесперебойного электропитания, а также сетевую связность с магистральной телекоммуникационной сетью, интеграционным шлюзом, доверенной третьей стороной и источником точного времени интеграционного сегмента Комиссии интегрированной системы или национального сегмента интегрированной системы;

г) получают доступ к защищенной сети передачи данных в соответствии с условиями подключения согласно разделу V настоящей Инструкции;

д) обеспечивают получение в органе криптографической защиты информации ключевых блокнотов и ключевых дистрибутивов;

е) обеспечивают поэкземплярный учет криптошлюзов, ключевых блокнотов и ключевых дистрибутивов;

ж) обеспечивают возврат неиспользованных или выведенных из действия ключевых блокнотов и ключевых дистрибутивов в орган криптографической защиты информации или по его распоряжению обеспечивают их уничтожение на месте;

з) обеспечивают контроль за техническим состоянием криптошлюзов.

Условия и порядок подключения криптошлюзов к защищенной сети передачи данных

17. Условиями подключения криптошлюзов к защищенной сети передачи данных являются:

а) наличие у участника защищенной сети передачи данных криптошлюзов, соответствующих настоящей Инструкции;

б) наличие у участника защищенной сети передачи данных лиц, ответственных за обеспечение эксплуатации и безопасности криптошлюзов, обученных правилам работы с ними в соответствии с технической и эксплуатационной документацией на криптошлюзы и настоящей Инструкцией;

в) наличие у участника защищенной сети передачи данных помещений для размещения криптошлюзов, соответствующих требованиям настоящей Инструкции;

г) наличие у участника защищенной сети передачи данных условий для обеспечения сохранности криптошлюзов, а также защиты их, ключевых блокнотов и ключевых дистрибутивов от несанкционированного доступа третьих лиц.

18. Передача участникам защищенной сети передачи данных криптошлюзов, владельцем которых является Комиссия, осуществляется на основании договора (соглашения).

Передача криптошлюзов за пределы государства пребывания Комиссии до места получения их участником защищенной сети передачи данных осуществляется организацией – участником внешнеэкономической деятельности Российской Федерации, уполномоченной в установленном порядке на осуществление экспорта товаров двойного назначения.

Оформление импорта криптошлюзов, включая разрешение на ввоз на территорию государства – члена Союза, осуществляется участником защищенной сети передачи данных в соответствии с требованиями законодательства государства – члена Союза.

19. Подключение к защищенной сети передачи данных осуществляется на основании заявления, направляемого участником защищенной сети передачи данных в Комиссию по форме согласно приложению № 1.

20. Настройка и конфигурирование криптошлюзов обеспечивается администратором защищенной сети передачи данных.

21. Подключение к защищенной сети передачи данных оформляется актом, подписываемым администратором и участником защищенной сети передачи данных в 2 экземплярах, по одному для каждой из сторон.

22. Не допускается применение ключевых блокнотов и ключевых дистрибутивов до получения соответствующих указаний администратора защищенной сети передачи данных.

Требования к транспортировке криптошлюзов, ключевых блокнотов и ключевых дистрибутивов

23. Криптошлюзы подлежат транспортировке отдельно от ключевых блокнотов и ключевых дистрибутивов. Не допускается перемещение криптошлюзов с установленными ключевыми дистрибутивами за пределы контролируемой зоны.

24. Криптошлюзы должны быть оборудованы средствами контроля вскрытия их корпуса (опечатывание, опломбирование).

25. Полученные упаковки с криптошлюзами вскрываются непосредственно лицами, ответственными за их эксплуатацию и безопасность.

Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или упаковка и печать их описанию (оттиску), а также если

упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, или обнаружено вскрытие корпуса криптошлюза, составляется акт, который направляется в орган криптографической защиты информации.

26. Доставка ключевых блокнотов и ключевых дистрибутивов может осуществляется фельдъегерской связью или уполномоченным представителем участника защищенной сети передачи данных при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

27. Для транспортировки ключевые блокноты и материальные носители ключевых дистрибутивов помещаются в прочную упаковку, исключающую возможность их физического повреждения. Упаковки опечатывают таким образом, чтобы исключить возможность извлечения из них содержимого без нарушения целостности упаковки и оттисков печати или контрольной пломбы.

28. Для пересылки криптошлюзов, технической и эксплуатационной документации к ним, ключевых блокнотов и ключевых дистрибутивов составляется опись вложений, в которой указывается: что посылается и в каком количестве, учетные номера криптошлюзов, ключевых блокнотов и материальных носителей ключевых дистрибутивов, а также при необходимости порядок использования высылаемого отправления. Опись вкладывается в упаковку.

29. Отправление принимается администратором криптошлюзов, осуществляется сверка вложений по описи с последующей регистрацией в журнале поэкземплярного средств криптографической защиты информации учета участника защищенной сети передачи данных.

30. В случае обнаружения администратором криптошлюзов бракованных ключевых блокнотов и (или) ключевых дистрибутивов они возвращаются в орган криптографической защиты информации для уничтожения.

Требования к размещению центра управления защищенной сетью передачи данных и криптошлюзов

31. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены средства центра управления защищенной сетью передачи данных и (или) криптошлюзы (далее – помещения), должны обеспечивать безопасность оборудования и криптографических ключей.

32. При оборудовании помещений должны выполняться требования законодательства государства – члена Союза, в котором находятся помещения, к размещению, монтажу средств криптографической защиты информации, а также другого оборудования, функционирующего совместно со средствами криптографической защиты информации.

33. Помещения выделяют с учетом размеров контролируемых зон, регламентированных технической и эксплуатационной документацией на средства центра управления защищенной сетью передачи данных и (или) криптошлюзы.

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первом и последнем этажах здания, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц , необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

34. Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключать возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

35. Режим охраны помещений должен быть установлен их владельцем и должен предусматривать периодический контроль за состоянием технических средств охраны.

36. Окна помещений должны быть защищены от просмотра извне плотными шторами, жалюзи либо иными средствами, предотвращающими такой просмотр.

37. Размещение и монтаж средств центра управления защищенной сетью передачи данных и криптошлюзов должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена ключевых документов осуществляются в отсутствие лиц, не допущенных к работе с ним.

Учет, хранение криптошлюзов и средств криптографической защиты информации, используемых в составе центра управления защищенной сетью передачи данных, эксплуатационной и технической документации к ним, ключевых блокнотов и ключевых дистрибутивов

38. Криптошлюзы и средства криптографической защиты информации, используемые в составе центра управления защищенной сетью передачи данных, эксплуатационная и техническая документация на них, ключевые блокноты и ключевые дистрибутивы подлежат поэкземплярному учету.

39. Поэкземплярный учет ведется в журнале поэкземплярного учета средств криптографической защиты информации в рамках компетенции органа криптографической защиты информации по форме согласно приложению № 2 и участником защищенной передачи данных по форме согласно приложению № 3.

40. Единицей поэкземплярного учета является техническое средство или материальный носитель. При использовании материальных носителей многократного использования, каждый факт их использования регистрируется отдельно.

41. Все полученные экземпляры криптошлюзов, средств криптографической защиты информации, используемых в составе центра управления защищенной сетью передачи данных, эксплуатационной и технической документации на них, ключевых блокнотов и ключевых дистрибутивов выдаются под расписку в журнале, указанном в пункте 39 настоящей Инструкции лицам, ответственным за их сохранность.

42. Дистрибутивы программного обеспечения на оптических или магнитных носителях, ключевые блокноты и материальные носители ключевых дистрибутивов хранятся у лиц, ответственных за эксплуатацию соответствующих компонентов защищенной сети передачи данных.

43. Криптошлюзы, аппаратно-программные средства криптографической защиты информации и аппаратные средства, с которыми осуществляется штатное функционирование средств криптографической защиты информации в составе центра управления защищенной сетью передачи данных, должны быть оборудованы средствами контроля за их вскрытием (опломбирование, опечатывание). Место размещения средства контроля должно позволять осуществлять его визуальный контроль.

44. Хранение эксплуатационной и технической документации, ключевых блокнотов и ключевых дистрибутивов осуществляется в надежных металлических хранилищах, оборудованных внутренними замками с 2 экземплярами ключей и приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у лица, ответственного за хранилище.

Способ хранения ключей должен исключать доступ к ним неуполномоченных лиц.

45. По окончании рабочего дня хранилища должны быть закрыты и опечатаны.

Печати, предназначенные для опечатывания хранилищ, должны находиться у лиц, ответственных за эти хранилища.

46. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в хранилище посторонних лиц, о случившемся должно быть немедленно сообщено в орган криптографической защиты информации.

Лица, ответственные за хранение ключевых блокнотов и ключевых дистрибутивов, должны оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять при необходимости меры к локализации последствий компрометации защищаемой информации и к замене скомпрометированных ключевых блокнотов и ключевых дистрибутивов.

Требования к уничтожению ключевых блокнотов, ключевых дистрибутивов, эксплуатационной и технической документации на компоненты защищенной сети передачи данных

47. Материальные носители ключевых блокнотов, ключевых дистрибутивов, эксплуатационной и технической документации на компоненты защищенной сети передачи данных, подлежат физическому уничтожению.

Материальные носители уничтожаются путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления размещенной на них информации.

Ключевые блокноты и ключевые дистрибутивы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации на центр управления защищенной сетью передачи данных. Если такой срок не установлен, то уничтожение должно быть произведено не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета.

48. Ключевые блокноты и ключевые дистрибутивы уничтожаются органом криптографической защиты информации и участником защищенной сети передачи данных с проставлением отметки в соответствующих журналах поэкземплярного учета.

Компрометация ключевых блокнотов и ключевых дистрибутивов

49. К обстоятельствам, указывающим на возможную компрометацию ключевых блокнотов и ключевых дистрибутивов, но не ограничивающим их, относятся:

а) потеря ключевых блокнотов и материальных носителей ключевых дистрибутивов ;

б) потеря ключевых блокнотов и материальных носителей ключевых дистрибутивов с последующим их обнаружением;

в) увольнение лиц, имевших доступ к ключевым блокнотами или ключевым дистрибутивам;

г) утрата ключей от хранилищ с ключевыми блокнотами или ключевыми дистрибутивами;

д) временный доступ посторонних лиц к ключевым блокнотам или ключевым дистрибутивам, а также другие события, при которых неизвестно, что произошло с ключевыми блокнотами или ключевыми дистрибутивами.

50. При возникновении обстоятельств, указанных в пункте 49 настоящей Инструкции, следует информировать орган криптографической защиты информации и администратора защищенной сети передачи данных о факте компрометации, при необходимости приостановить работу криптошлюзов по согласованию с администратором защищенной сети передачи данных, в максимально короткий период осуществить смену скомпрометированной ключевой информации.

51. Решение о компрометации в рамках своей зоны ответственности принимает администратор защищенной сети передачи данных или администратор криптошлюзов. Информация о компрометации (с указанием идентификационных номеров скомпрометированных ключевых блокнотов и (или) ключевых дистрибутивов и сведений об обстоятельствах такой компрометации) должна быть направлена в течение 1 рабочего дня в орган криптографической защиты информации.

52. Орган криптографической защиты информации после проверки достоверности полученной информации дает поручение администратору защищенной сети передачи данных и администраторам криптошлюзов в согласованное с участниками защищенной сети передачи данных время произвести ввод в действие ключевых блокнотов и (или) ключевых дистрибутивов взамен скомпрометированных.

53. Период использования скомпрометированных ключевых блокнотов и (или) ключевых дистрибутивов должен быть максимально коротким.

Контроль за организацией и обеспечением безопасности защищенной сети передачи данных

54. Контроль за организацией и обеспечением безопасности защищенной сети передачи данных осуществляет орган криптографической защиты информации в рамках осуществляемых им функций.

55. Срок и периодичность контроля определяются Консультативным комитетом по информатизации, информационным технологиям и защите информации, созданным Решением Коллегии Евразийской экономической комиссии от 2 июня 2016 г. № 53, и утверждаются актом Комиссии.

56. Формируемые по результатам контроля заключения по фактам нарушения требований настоящей Инструкции, а также предложения по принятию мер по предотвращению опасных последствий подобных нарушений представляются органом криптографической защиты на рассмотрение Консультативного комитета по информатизации, информационным технологиям и защите информации.

ПРИЛОЖЕНИЕ № 1

к Инструкции по организации, обеспечению функционирования и безопасности каналов передачи данных в интегрированной информационной системе Евразийского экономического союза

(форма)

(Оформляется на бланке участника защищенной сети передачи данных)

Евразийская экономическая комиссия

ЗАЯВЛЕНИЕ

на подключение к защищенной сети передачи данных

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____

(должность, фамилия, имя, отчество)

действующего на основании _____

(организационно-распорядительный документ)

просит изготовить файл ключевого дистрибутива сети, на своего уполномоченного представителя, в соответствии с указанными в настоящем заявлении данными:

Наименование органа или организации	
Место нахождения организации	
Место размещения криптошлюзов	
Ф.И.О уполномоченного представителя	
Должность	
Контактные данные (адрес электронной почты, телефон)	

Настоящим _____

_____

(фамилия, имя, отчество уполномоченного представителя)

паспорт: серия	номер	выдан

_____

(орган, которым выдан паспорт)

"_____" _____ 20__

_____

(дата выдачи паспорта)

уполномочен для получения ключевых блокнотов и ключевого дистрибутива участника защищенной сети передачи данных интегрированной информационной системы Евразийского экономического союза.

Полномочия, указанные в заявлении, действуют в течение срока действия ключевого дистрибутива без права передоверия.

Уполномоченное лицо _____ _____

(подпись) (инициалы, фамилия)

Руководитель организации _____ _____

(подпись) (инициалы, фамилия)

М.П. "____"_____ 20__ г.

ПРИЛОЖЕНИЕ № 2

к Инструкции по организации, обеспечению функционирования и безопасности каналов передачи данных в интегрированной информационной системе Евразийского экономического союза

(форма)

ЖУРНАЛ

поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации на них, ключевых документов (для органа криптографической защиты)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации на них, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации на них, номера серий ключевых документов	Номера экземпляров (криптографи-ческие номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)		
				от кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	кому разосланы (переданы)	дата и номер сопроводи-тельного письма	дата и номер подтверждения или расписка в получении
1	2	3	4	5	6	7	8	9

Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
дата и номер сопроводительного письма	дата и номер подтверждения			дата уничтожения	номер акта или расписка об уничтожении	
10	11	12	13	14	15	16

ПРИЛОЖЕНИЕ № 3

к Инструкции по организации, обеспечению функционирования и безопасности каналов передачи данных в интегрированной информационной системе Евразийского экономического союза

(форма)

ЖУРНАЛ

поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации на них, ключевых документов (для администратора защищенной сети передачи данных и участника защищенной сети передачи данных)

				Отметка о получении		Отметка о выдаче	

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации на них, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации на них ним, номера серий ключевых документов	Номера экземпляров (криптографи-ческие номера) ключевых документов	от кого получены	дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	дата и

							расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	дата подключения (установки) и подписи лиц, произведших подключение (установку)	номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	номер акта или расписка об уничтожении	
9	10	11	12	13	14	15