Приложение №1
к приказу от «25» 10 2024 г. № 213

ИНСТРУКЦИЯ
по обращению со средствами криптографической защиты информации в информационных системах СПбГИПСР

1. Термины и определения

1.1. Закрытый ключ – криптоключ, который хранится пользователем системы в тайне.

1.2. Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

1.3. Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

1.4. Ключевой документ – физический носитель определенной структуры, содержащий ключевую информации.

1.5. Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.

1.6. Компрометация криптоключа – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

1.7. Контролируемая зона – территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа.

1.8. Криптографический ключ (криптоключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

1.9. Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

1.10. Пользователь СКЗИ – физическое лицо, непосредственно допущенное к работе со средствами криптографической защиты информации.

1.11. Режимные помещения – помещения, где установлены средства криптографической защиты информации или хранятся ключевые документы к ним.

1.12. Средство криптографической защиты информации – криптосредства, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну:

- средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;
- средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;
- средства электронной цифровой подписи - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

- средства кодирования - средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;
- средства изготовления ключевых документов (независимо от вида носителя ключевой информации);
- ключевые документы (независимо от вида носителя ключевой информации).

2. Общие положения

2.1. Инструкция по обращению со средствами криптографической защиты информации (далее – Инструкция) в информационных системах (далее – ИС) СПбГИПСР (далее – Учреждение), определяет порядок обращения, размещения, хранения, учета и уничтожения сертифицированных ФСБ России шифровальных (криптографических) средств защиты информации (далее – СКЗИ), а также лиц, ответственных за эксплуатацию СКЗИ.

2.2. Инструкция разработана в соответствии со следующими документами:

- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России №66 от 9 февраля 2005г.;
- Приказ ФАПСИ при Президенте РФ от 13 июня 2001г. №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ ФСБ России от 10 июля 2014г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

2.3. Пользователи допускаются к работе с СКЗИ согласно «Перечню работников, допущенных к работе со средствами криптографической защиты информации», утверждаемому приказом ректора Учреждения, после ознакомления под подпись с настоящей Инструкцией и обучения правилам работы с СКЗИ.

2.4. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности информации ограниченного доступа, и не исключает обязательного выполнения их требований.

2.5. Аппаратные средства, с которыми осуществляется штатное функционирование криптосредств, а также аппаратные и аппаратно-программные криптосредства должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы).

2.6. Место опечатывания (опломбирования) криптосредств, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

2.7. Передача закрытых криптоключей по техническим средствам связи не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

2.8. По всем вопросам организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ, защищаемой ИОД Учреждение обязано обращаться к организации-лицензиату ФСБ РФ и выполнять его требования.

3. Ответственные лица

3.1. В Учреждении ответственность за эксплуатацию сертифицированных СКЗИ несут:

- ответственный за защиту информации в информационных системах (далее – ИС), на которого возлагаются обязанности по:
  - обеспечению корректного и безопасного функционирования СКЗИ;
  - обеспечению корректной и безопасной эксплуатации СКЗИ;
  - выработке соответствующих инструкций и ознакомление с ними пользователей СКЗИ;
  - контролю работоспособности и соблюдения правил эксплуатации СКЗИ;
  - обеспечению режима сохранности СКЗИ, эксплуатационной и технической документации.
- пользователи СКЗИ, на которых возлагаются задачи по:
  - соблюдению правил корректной и безопасной эксплуатации СКЗИ;
  - обеспечению режима сохранности СКЗИ и ключевых документов, переданных им.

4. Обязанности ответственного за защиту информации

4.1. Ответственный за защиту информации в ИС осуществляет:

- разработку мероприятий по обеспечению функционирования и безопасности, применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;
- ознакомление лиц, использующих СКЗИ, правилам работы с ними с получением подписи о прохождении ознакомления;
- поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;
- учет лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности информации ограниченного доступа (далее – ИОД) в ИС (пользователей СКЗИ);
- контроль за соблюдением условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к ним;
- расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

5. Обязанности пользователей

5.1. Обязанности пользователей СКЗИ:

- не разглашать защищаемую ИОД, к которой они допущены, рубежи её защиты, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты;
- соблюдать требования к обеспечению безопасности, защищаемой ИОД, требования к обеспечению безопасности СКЗИ и ключевых документов к ним;
- сообщать ответственному за защиту информации в ИС или своему непосредственному руководителю информацию о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- немедленно уведомлять ответственного за защиту информации в ИС или своего непосредственного руководителя о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемой ИОД;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

6. Организация допуска пользователей к работе с СКЗИ

6.1. Обучение пользователей правилам работы с СКЗИ осуществляет ответственный за защиту информации в ИС. Непосредственно к работе с СКЗИ пользователи допускаются после обучения и выдачи «Заключения о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации», форма которого приведена в Приложении 1 к настоящей Инструкции.

7. Учет СКЗИ

7.1. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат учету с использованием индексов или условных наименований и регистрационных номеров в «Журнале поэкземплярного учета средств криптографической защиты информации, используемых в информационных системах», форма которого приведена в Приложении 2 к настоящей Инструкции.

7.2. Программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

7.3. Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

7.4. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в «Журнале поэкземплярного учета средств криптографической защиты информации, используемых в информационных системах» пользователям СКЗИ, несущим персональную ответственность за их сохранность.

7.5. Ответственный за защиту информации в ИС заводит и ведет на каждого пользователя СКЗИ лицевой счет, в котором регистрирует числящиеся за ними СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы.

7.6. Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, форма которого приведена в Приложении 3 к настоящей Инструкции, ведущемся непосредственно пользователем СКЗИ. В техническом (аппаратном) журнале отражают также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на СКЗИ не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к СКЗИ).

8. Передача СКЗИ

8.1. При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования СКЗИ, указанные сообщения необходимо передавать только с использованием СКЗИ.

8.2. Передача криптоключей по техническим средствам связи не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

8.3. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) ответственным за защиту информации в ИС под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями СКЗИ должна быть санкционирована ответственным за защиту информации в ИС.

8.4. Выдача ключевых носителей, ключевых документов, СКЗИ, эксплуатационных и технических документов к СКЗИ работникам Учреждения осуществляется ответственным за защиту информации в ИС на основании списка, утверждаемого ректором Учреждения.

8.5. Факт выдачи пользователю ключевого документа, СКЗИ, эксплуатационного и технического документа к СКЗИ регистрируется в «Журнале поэкземплярного учета средств криптографической защиты информации, используемых в информационных системах», форма которого приведена в Приложении 2 к настоящей Инструкции.

9. Пересылка и получение СКЗИ

9.1. СКЗИ и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными работниками Учреждения из числа пользователей СКЗИ или ответственным за защиту информации в ИС при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ и ключевым документам во время доставки.

9.2. Эксплуатационную и техническую документацию к СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

9.3. Для пересылки СКЗИ и ключевых документов они должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. СКЗИ пересылают отдельно от ключевых документов к ним. На упаковках указывают ответственного за защиту информации в ИС или пользователя СКЗИ, для которых эти упаковки предназначены. На таких упаковках делают пометку «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати. До первоначальной высылки (или возвращения) адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.

9.4. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо, в котором необходимо указать: что посылается и в каком количестве, учетные номера изделий или документов, а также при необходимости назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

9.5. Полученные упаковки вскрывает только ответственный за защиту информации в ИС, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает отправителю. Полученные с такими отправлениями СКЗИ и ключевые документы до получения указаний от отправителя применять не разрешается.

9.6. При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от изготовителя.

9.7. Получение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме. Отправитель обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

9.8. Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов следует производить заблаговременно. Указание о вводе в действие очередных ключевых документов может быть дано ответственным за защиту информации в ИС только после поступления от всех

заинтересованных пользователей СКЗИ подтверждения о получении ими очередных ключевых документов.

9.9. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному за защиту информации в ИС или по его указанию должны быть уничтожены на месте.

10. Хранение СКЗИ

10.1. Пользователи СКЗИ хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

10.2. Пользователи СКЗИ предусматривают раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

10.3. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у работника, ответственного за хранилище. Дубликаты ключей от хранилищ работники хранят в сейфе ответственного за защиту информации в ИС. Дубликат ключа от хранилища ответственного за защиту информации в ИС в опечатанной упаковке должен быть передан на хранение ректору Учреждения под расписку в «Журнале учета ключей от режимных помещений, карт для доступа в режимные помещения, хранилищ, личных печатей от хранилищ», форма которого приведена в Приложении 4 к настоящей Инструкции.

11. Уничтожение СКЗИ

11.1. Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

11.2. Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

11.3. Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

11.4. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационную и техническую документацию к СКЗИ уничтожают путем сжигания или с помощью любых бумагорезательных машин.

11.5. СКЗИ уничтожают (утилизируют) по решению ответственного за защиту информации в ИС, владеющего СКЗИ, и с уведомлением организации, ответственной в соответствии с ПКЗ-2005 за организацию поэкземплярного учета СКЗИ.

11.6. Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ, и они полностью отсоединены от аппаратных средств.

11.7. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

11.8. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная, и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

11.9. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в СКЗИ или иных дополнительных устройствах уничтожаются пользователями этих СКЗИ самостоятельно под расписку в техническом (аппаратном) журнале.

11.10. Ключевые документы уничтожаются либо пользователями СКЗИ, либо ответственным за защиту информации в ИС под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом, форма которого приведена в Приложении 5 к настоящей Инструкции. При этом пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи СКЗИ должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) ответственным за защиту информации в ИС для списания уничтоженных документов с их лицевых счетов.

11.11. Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию СКЗИ. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учета.

12. Режимные помещения

12.1. Размещение, специальное оборудование, охрана и организация режима в режимных помещениях (далее – РП) должны обеспечивать сохранность СКЗИ и ключевых документов к ним. При оборудовании РП должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

12.2. РП выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. РП должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна РП, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в РП посторонних лиц,

необходимо оборудовать металлическими решетками или ставнями или охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению в РП.

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

12.4. Режим охраны РП, в том числе правила допуска работников и посетителей в рабочее и нерабочее время, устанавливает ответственный за защиту информации в ИС по согласованию с ректором Учреждения. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются.

12.5. Двери РП должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода работников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают работникам, имеющим право допуска в РП, под расписку в «Журнале учета ключей от режимных помещений, карт для доступа в режимные помещения, хранилищ, личных печатей от хранилищ», форма которого приведена в Приложении 4 к настоящей Инструкции. Дубликаты ключей от входных дверей таких РП следует хранить в сейфе ответственного за защиту информации в ИС.

12.6. Дубликат ключа от сейфа ответственного за защиту информации в ИС в опечатанной упаковке должен быть передан на хранение ректору Учреждения под расписку в «Журнале учета ключей от режимных помещений, карт для доступа в режимные помещения, хранилищ, личных печатей от хранилищ», форма которого приведена в Приложении 4 к настоящей Инструкции

12.7. Для предотвращения просмотра извне РП их окна должны быть защищены ставнями, жалюзи и т.п.

12.8. РП по возможности должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять ответственным за защиту информации в ИС совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

12.9. По окончании рабочего дня РП и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале ответственному за защиту информации в ИС или уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

12.10. Ключи от РП, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих РП. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей СКЗИ, ответственных за эти хранилища.

12.11. При утрате ключа от хранилища или от входной двери в РП замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный за защиту информации в ИС.

12.12. В обычных условиях РП, находящиеся в них опечатанные хранилища, могут быть вскрыты только пользователями СКЗИ или ответственным за защиту информации в ИС.

12.13. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти РП или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за защиту информации в ИС. Прибывший ответственный за защиту информации в ИС должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять при необходимости меры к локализации последствий компрометации ИОД и к замене скомпрометированных криптоключей.

12.14. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа

посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

12.15. На время отсутствия пользователей СКЗИ указанное оборудование при наличии технической возможности должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с ответственным за защиту информации в ИС необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами.

13. Компрометация действующих ключей к СКЗИ

13.1. К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

- явная компрометация ключей:
  - потеря ключевых носителей;
  - потеря ключевых носителей с их последующим обнаружением;
  - увольнение работников, имевших доступ к ключевой информации;
  - нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;
- неявная компрометация ключей:
  - возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
  - нарушение печати на сейфе с ключевыми носителями;
  - случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

13.2. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием ИОД, пользователи СКЗИ обязаны сообщать ответственным за защиту информации в ИС.

14. Инструкция по восстановлению связи в случае компрометации действующих ключей к СКЗИ

14.1. Криптоключи, в отношении которых, возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.

14.2. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается по решению ответственного за защиту информации в ИС, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

14.3. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать ответственным за защиту информации в ИС.

14.4. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

14.5. В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

14.6. Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет Учреждение.

14.7. Порядок оповещения пользователей СКЗИ о предполагаемой компрометации криптоключей и их замене устанавливается Учреждением.

15. Регламент проведения контроля соответствия использования СКЗИ

15.1. Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ ИОД в Учреждении осуществляют федеральные органы безопасности или организация-лицензиат. В ходе контроля изучаются и оцениваются:

- организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации;
- достигнутый уровень криптографической защиты конфиденциальной информации;
- условия использования СКЗИ.

15.2. По результатам контроля составляется подробный или краткий акт, справка. С актом под расписку должен быть ознакомлен ректора Учреждения.

15.3. Если в использовании СКЗИ обнаружены недостатки, то Учреждение обязан принять безотлагательные меры по их устранению.

15.4. Ответственный за защиту информации в ИС обязан контролировать выполнение пользователями СКЗИ правил организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ ИОД, а также условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФСБ и Инструкцией.

15.5. Внутренний контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации производится Учреждением 1 раз в год.

15.6. В ходе контроля изучаются и оцениваются:

- организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации;
- выполнение Инструкции.

15.7. С целью оценки обоснованности и достаточности мер, принятых для защиты информации конфиденциального характера, Учреждение вправе обратиться в ФСБ России с просьбой о проведении контроля за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования СКЗИ.

16. Ответственность

16.1. Работники несут личную ответственность за сохранность выданной им ключевой информации, носителей и паролей доступа к ним.

16.2. Все работники, осуществляющие обработку и защиту ИОД в ИС, обязаны ознакомиться с данной Инструкцией под подпись.

16.3. Работники несут персональную ответственность за выполнение требований настоящей Инструкции.

17. Срок действия и порядок внесения изменений

17.1. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.

17.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

17.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом ректора Учреждения.

Приложение 1
к Инструкции по обращению со средствами
криптографической
защиты информации

ФОРМА

ЗАКЛЮЧЕНИЕ
о подготовке и допуске к самостоятельной работе
со средствами криптографической защиты

Пользователи средств криптографической защиты информации (далее – СКЗИ):

№ п/п	Должность	Фамилия Имя Отчество

Дата проведения подготовки «___» _____ 20__ г.

Подготовка проводилась в соответствии с требованиями:

– эксплуатационной и технической документации к_____

_____;

(наименование криптосредства, по которому осуществлялась подготовка)

– Инструкции по обращению со средствами криптографической защиты информации, утверждённой приказом от «__» _____ 20__ г. №_____.

1	С Инструкцией по обращению со средствами криптографической защиты информации	*ОЗНАКОМЛЕНЫ*
2	Ранее подготовку по данному средству криптографической защиты информации	*НЕ ПРОХОДИЛИ*
3	Пройденный материал	*УСВОИЛИ*

Заключение:

Допустить пользователей СКЗИ к самостоятельной работе с *(наименование криптосредства, по которому осуществлялась подготовка).*

С заключением ознакомлен (а):

№ п/п	Должность	Фамилия Имя Отчество	Подпись

Ответственный за защиту информации в ИС:

_____

(ФИО, должность, подпись, дата)

Приложение 2
к Инструкции по обращению со средствами
криптографической защиты информации

Форма
журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов, используемых в информационных системах

Уч. № _____

Начат: «___» _____ 20__г.

Окончен: «___» _____ 20__г.

На _____ листах

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. пользователя СКЗИ, производившего 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. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение 3
к Инструкции по обращению со средствами
криптографической защиты информации

Форма
технического (аппаратного) журнала
учета средств криптографической защиты информации

Уч. № _____

Начат: «___» _____ 20__г.

Окончен: «___» _____ 20__г.

На _____ листах

№ п/п	Дата	Тип и регистрационные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10

Приложение 4
к Инструкции по обращению со средствами
криптографической защиты информации

Форма
учета ключей от режимных помещений, карт для доступа в режимные помещения, ключей хранилищ, личных печатей от хранилищ

Уч. № _____

Начат: «___» _____ 20__г.

Окончен: «___» _____ 20__г.

На _____ листах

№ п/п	Наименование объекта учета (ключ от помещения/ключ от хранилища/личная печать/карта)	№ помещения/ № хранилища	Информация о выдаче	Информация о получении	Информация о сдаче	Примечание
			Фамилия И.О., подпись, дата	Фамилия И.О., подпись, дата	Фамилия И.О., подпись, дата	
1	2	3	4	5	6	7

Приложение 5
к Инструкции по обращению со средствами
криптографической защиты информации

АКТ

«___» _____ 20___ г. № _____

Уничтожения средств
криптографической защиты информации

Комиссия в составе:

Председатель:

_____ _____

Члены комиссии:

1. _____ _____
2. _____ _____
3. _____ _____

составила настоящий акт о том, что перечисленные в таблице 1 средства криптографической защиты информации уничтожены с предварительным стиранием программного обеспечения средств криптографической защиты информации и произведено стирание информации (которая может оставаться в устройствах памяти оборудования, в принтерах, сканерах)

Таблица 1

№ п/п	Наименование средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера средств криптографической защиты информации, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Примечание

Регистрационные данные на средствах криптографической защиты информации сверены с записями в настоящем Акте, уничтожение средств криптографической защиты информации выполнено способом их стирания (разрушения) по технологии в соответствии с требованиями эксплуатационной и технической документации на соответствующие средства криптографической защиты информации.

Узлы и детали аппаратных средств общего назначения

_____

(не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций средств криптографической защиты информации мониторы, принтеры, сканеры, клавиатура и т.п.)

передать в _____.

Отметку об уничтожении ключевых носителей, ключевых документов в «Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов» произвел _____.

(должность, фамилия, инициалы подпись, дата)

Председатель:

_____ _____

Члены комиссии:

1. _____ _____
2. _____ _____
3. _____ _____

Приложение 6
к Инструкции по обращению со средствами
криптографической защиты информации

ПЕРЕЧЕНЬ
помещений СПбГИПСР, выделенных для установки средств криптографической защиты информации и хранения ключевых документов к ним

№ п/п	Наименование/ номер помещения	Адрес расположения помещения	Допущенные работники (Фамилия И.О., должность)	Ответственный за режим в помещении (Фамилия И.О., должность)
1	Кабинет № 98	192102, Санкт-Петербург, Волковский пр., д. 4, лит. А	– Проректор по учебной работе М.В. Сперанская; – Проректор по молодежной политике и воспитательной деятельности Н.С. Иванова; – Начальник отдела информационных технологий Т.А. Георгиев; – Начальник отдела по работе с абитуриентами и выпускниками О.А Алексеева; – И.о. начальника отдела учебно-методического обеспечения образовательного процесса А.А. Горбачева – Ведущий специалист отдела информационных технологий П.А. Кодра	Начальник отдела по работе с абитуриентами и выпускниками О.А. Алексеева

Приложение 7
к Инструкции по обращению со средствами
криптографической защиты информации

ПЕРЕЧЕНЬ
защищенных хранилищ, предназначенных для хранения средств криптографической защиты информации, ключевых документов, эксплуатационной и технической документации к средствам криптографической защиты информации

№ п/п	Номер хранилища	Номер помещения, где расположено хранилище	Адрес расположения помещения	Ответственный за хранилище (Фамилия И.О., должность)
1.	№ 1	98	192102, Санкт-Петербург, Волковский пр., д. 4, лит. А	Начальник отдела по работе с абитуриентами и выпускниками О.А. Алексеева

Лист ознакомления с «Приказом об обращении со средствами криптографической защиты информации в информационных системах» от "25" 10 2024 г. № 213

Занимаемая должность	И. О. Фамилия	Подпись	Дата ознакомления