муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа №4»

«Утверждаю»

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 559047816AA68482C7B61BED8707504A22833ED8A
Владелец: Орищенко Ольга Алексеевна
Действителен: с 03.02.2022 по 03.05.2023

Директор МБОУ «СОШ №4 »
_____ О.А. Орищенко
Приказ № 25-од от 13.01.2022г

Положение
об обеспечении безопасности персональных данных при помощи средств криптографической защиты информации

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Целью разработки данного положения является описание работы со Средствами криптозащиты информации (СКЗИ), в соответствии с действующим законодательством Российской Федерации, по обязательной защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (шифровальных средств), при ее обработке, хранении и передаче по каналам связи.

1.2. Настоящее Положение определяет порядок организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в МБОУ «СОШ №4» (далее - Оператор).

1.3. Настоящее Положение разработано на основании требований Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ « О персональных данных», Типовых требований ФСБ от 21.02.2008 № 149/6/6-622

2. ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБРАБОТКИ С ИСПОЛЬЗОВАНИЕМ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Криптографические средства должны быть установлены и введены в эксплуатацию в соответствии с эксплуатацией и технической документацией к этим средствам.

2.2. Список лиц (пользователей), допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационных системах, оформляются документально. Перечисленные должностные лица должны пройти обучение по работе с криптосредствами.

2.3 Пользователи криптосредств обязаны:

Не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты.

Соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

Сообщать о ставших им известными попытках посторонних лиц получать сведения об используемых криптосредствах или ключевых документах к ним.

Немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документах к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

Сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящими Требованиями, при увольнении или отстранении от исполнения.

2.4. Оператором назначается ответственный за эксплуатацию криптосредств из числа штатных сотрудников, который осуществляет контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним.

2.5. Ответственный пользователь криптосредств должен иметь функциональные обязанности.

2.6. Ответственных пользователь криптосредств заводит и ведет на каждого пользователя криптосредств лицевой счет, в котором регистрирует числящихся за ним криптосредств, эксплуатационную и техническую документацию к ним, ключевые документы.

2.7. Ответственный обязан контролировать:

- Соблюдение пользователями криптосредств конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых криптосредств в ключевых документах к ним.

-Точное выполнение пользователями криптосредств требований к обеспечению безопасности персональных данных.

-Надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения.

-Своевременное выявление попыток посторонних лиц получить сведения о защищаемых персональных данных, об используемых криптосредствах или ключевых документах к ним.

-Немедленное применение мер по предупреждению разрешения защищаемых персональных данных, а также возможностей их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

2.8. Лица, оформленные на работу в качестве ответственных пользователей криптосредств, должны быть ознакомлены с документами, регламентирующими организацию и обеспечение безопасности персональных данных при их обработке в информационных системах, под расписку и несут ответственность за несоблюдение ими требований указанных в соответствии с законодательством Российской Федерации.

2.9. Передача техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств.
Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

3. ОРГАНИЗАЦИЯ ЭКСПЛУАТАЦИИ СКЗИ
3.1. ВВОД В ЭКСПЛУАТАЦИЮ СКЗИ

3.1.1. На каждое рабочее место, оснащение СКЗИ, оформляется акт о вводе в эксплуатацию (Приложение 2). Акт может храниться у ответственного пользователя СКЗИ или у лица, ответственного за эксплуатацию СКЗИ.

3.1.2. Организация централизованного (количественного) поэкземплярного учета компонентов СКЗИ осуществляется пользователем.

3.1.3 СКЗИ, эксплуатационная и техническая документация подлежит поэкземлярному учету. Учет ведется в Журнале учета. (Приложение 3).

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

3.1.4.Программные СКЗИ учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

Все полученные СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть, выданы по расписку в соответствующем журнале поэкземплярного учета пользователем СКЗИ, несущим персональную ответственность за их сохранность.

3.1.5. Если эксплуатационной и технической документации в 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 журнале (Приложение 4), ведущемся непосредственно ответственным 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).

3.1.6. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ по расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями СКЗИ должна быть санкционирована ответственным пользователей СКЗИ.

3.2. ВЫВОД ИЗ ЭКСПЛУАТАЦИИ СКЗИ

3.2.1. Вывод из эксплуатации СКЗИ оформляется актом (приложение 5).

3.2.2. Ключевые документы уничтожаются либо пользователями криптосредств, либо ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземлярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи криптосредств должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) ответственного пользователя криптосредств для списания уничтоженных документов с их лицевых счетов.

3.2.3.Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию криптосредств. В акте указывается, что уничтожается и в каком количестве. В конце акта итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтоженных ключевых документов, инсталлирующих криптосредства 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.

3.2.4. 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).

3.2.5. 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 исключения применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

3.2.6. Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключей 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).

3.2.7. 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.

3.2.8. 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).

3.2.9. 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 журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключами; хранящихся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

3.2.10. 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 журнале.

3.3. КОНТРОЛЬ СОБЛЮДЕНИЯ УСЛОВИЙ ЭКСПЛУАТАЦИИ И РАБОТОСПОСОБНОСТИ СКЗИ

3.3.1. Контроль соблюдения условий использования СКЗИ осуществляет ответственный пользователь СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, настоящим Положением, а также иными нормативно - методическими документами по эксплуатации.

3.3.2. Ответственный пользователь СКЗИ также осуществляет контроль выполнения требований по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

3.3.3. Контроль может быть плановым и внеплановым.

Внеплановый контроль осуществляется в случае установления фактов нарушения условий эксплуатации или работоспособности СКЗИ.

В ходе контроля оцениваются:

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

-достигнутый уровень криптографической защиты конфиденциальной информации:

-условия использования СКЗИ.

3.3.4. По результатам контроля оформляется Протокол проверки в двух экземплярах.

3.3.5. Сведения о контроле заносятся в Журнал контроля соблюдения условий эксплуатации и работоспособности СКЗИ (Приложение 6).

3.3.6. Если при контроле обнаружены недостатки, т делаются записи в Журнал замечаний по результатам контроля (Приложение 7). На каждое замечание назначается лицо, ответственное за его устранение, а также срок устранения. По результатам работы над замечанием, в Журнале замечаний по результатам контроля делается запись о статусе устранения замечания, которая заверяется подписью лица, ответственного за устранение замечания.

3.3.7. Пользователи криптосредств обязаны принять меры по устранению вскрытых недостатков и выполнению рекомендаций, изложенных в Журнале замечаний по результатам контроля.

3.3.8. Если в ходе контроля выявлены серьезные нарушения в эксплуатации СКЗИ, из-за чего становится реальной утечка конфиденциальной информации, ответственный пользователь СКЗИ вправе дать указание о прекращении использования СКЗИ до устранения причин выявленных нарушений.

4. УСТАНОВКА СКЗИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ПЭВМ

4.1. Установка и настройка общесистемного ,прикладного ПО и дополнительных средств защиты на ПЭВМ с СКЗИ производится в соответствии с правилами установки и настройки СКЗИ и ПО, изложенными в эксплуатационной и технической документации.

4.2. Установка СКЗИ осуществляется ответственным пользователем СКЗИ или другим подготовленным специалистом под его контролем. До установки СКЗИ должны быть осуществлены:

-проверка работоспособности технических средств и их соответствия требованиям технической и эксплуатационной документации;

-исключение из состава ПЭВМ все оборудование, которое может создавать угрозу безопасности;

-проверка ОС на отсутствие вирусов;

-проверка и настройка ОС в соответствии с требованиями технической и эксплуатационной документации;

4.3. К установке и настройке СКЗИ и ПО предъявляются следующие общие требования:

-устанавливаемое ПО не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществить несанкционированный доступ к системным ресурсам;

- устанавливаемое ПО должно быть лицензированным;

- устанавливаемое ПО и СКЗИ, а также диски для их инсталляции должно подвергаться периодическому контролю целостности в соответствии с технической и эксплуатационной документации;

-устанавливаемое ПО должно устанавливаться совместно с антивирусным ПО, базы которого должны своевременно и регулярно обновляться;

-устанавливаемое ПО не должно содержать возможностей, позволяющих модифицировать системные ресурсы (области памяти, программный код), передавать управление несанкционированным подпрограммам, повышать предоставленные привилегии, использовать недокументированные разработчиками возможности ОС).

4.4. К ОС, в среде, которой планируется использовать СКЗИ, предъявляются следующие общие требования:

-на ПЭВМ должна быть установлена только одна лицензированная ОС, удовлетворяющая системным требованиям СКЗИ (запрещается использовать нестандартные, измененные или отладочные версии ОС);

-удаленное управление ОС должно быть запрещено или ограничено путем отключения всех служб, реализующих данные механизмы, или путем настроек, запрещающих фильтров для протоколов и портов удаленного управления ОС для всех узлов, кроме специально выделенных для этих целей;

-каждый пользователь должен иметь для входа в ОС свою учетную запись;

-длина пароля учетной записи должна быть не менее 6 символов;

-учетная запись для гостевого входа должна быть отключена;

-правом установки и настройки ОС и СКЗИ должен обладать Администратор ПЭВМ;

-все неиспользуемые ресурсы ОС должны быть отключены (протоколы, сервисы и т.п.);

-режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;

-всем пользователям и группам, зарегистрированным в ОС, права доступа к ресурсам должны быть назначены в объеме, необходимом для выполнения ими своих обязанностей;

-регулярно должны устанавливаться пакеты обновления безопасности ОС, антивирусных баз;

-при подключении ПЭВМ с СКЗИ к сетям связи общего пользования должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VRN сетей и т.п.) и др.

4.5. Ответственный пользователь СКЗИ должен осуществлять периодический контроль выполнения указанных требований, а также требований, приведенных в технической и эксплуатационной документации.

4.6. Не допускается:

-обрабатывать на ПЭВМ, оснащенной СКЗИ, информацию, содержащую государственную тайну;

-осуществлять несанкционированное изменение аппаратной и программной конфигурации ПЭВМ (в том числе несанкционированное вскрытие), СКЗИ, ПО.

5. УСЛОВИЯ РАЗМЕЩЕНИЯ И ОХРАНЫ ПОМЕЩЕНИЙ, В КОТОРЫХ УСТАНОВЛЕНЫ КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА

5.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее - режимные помещения), должны обеспечивать сохранность персональных данных, криптосредств и ключевых документов к ним.

5.2. При оборудовании режимных помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

Перечисленные в настоящем документе требования к режимным помещениям могут не предъявляться, если это предусмотрено правилами пользования криптосредствами, согласованными с ФСБ России.

5.3. Режимные помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные двери с замками, гарантирующими надежное закрытие помещения в нерабочее время. Окна помещений, расположенных на первом или последнем этажах зданий, а также окна, находящихся около пожарных лестниц и других мест, откуда возможно проникновение, в режимное помещение посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимное помещение.

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

5.5. Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее время, устанавливает ответственный пользователь криптосредств по согласованию, при необходимости, с оператором, в помещениях которого установлены криптосредства или хранятся документы к ним. Установленный режим должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящих Требований.

5.6. Двери спецпомещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей входных дверей таких помещений следует хранить в сейфе оператора или ответственного пользователя криптосредствами.

5.7. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.

5.8. Режимные помещения, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверить ответственному пользователю криптосредств совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

5.9. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства 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 сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе ответственного пользователя криптосредств. Дубликат ключа от хранилища ответственного пользователя криптосредств в опечатанной упаковке должен быть передан на хранение оператору по расписку в соответствующем журнале.

5.10. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы по расписку в соответствующем журнале ответственному пользователю криптосредств или уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

5.11. Ключи от режимных помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ режимного помещения, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей по охрану самих режимных помещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за эти хранилища.

5.12. При утрате ключа от хранилища или от входной двери в режимное помещение замок необходимо заменить или передать 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 оператор или ответственный пользователь криптосредств.

5.13. В обычных условиях режимные помещения, находящиеся, а них опечатанные хранилища могут быть вскрыты только пользователями криптосредств, ответственным пользователем криптосредств или оператором.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения и хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю криптосредств или оператору. Прибывший ответственный пользователь криптосредств должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.

5.14. Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами , в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляется в отсутствии лиц, не допущенных к работе с данными криптосредствами.

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

Приложение 1

СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

НСД – Несанкционированный доступ
ОС – Операционная система
ПК – Персональный компьютер
ПО – Программное обеспечение
СКЗИ – Средство криптографической защиты информации
ТС – Технические средства
ЭЦП – Электронная цифровая подпись

Основные термины и определения

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Доступ к информации - возможность получения информации и ее использования.

Информационная система персональных данных - совокупность содержания в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребываниями и действиями лиц и (или) транспортных средств.

Границей контролируемой зоны, может быть: пример охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Криптосрество - шифровальное (криптографические) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В части, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) - средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц предоставлен с согласия субъекта персональных данных или на которые, в соответствии с федеральными законами, не распространяется требование соблюдения конфиденциальности.

Оператор - государственный орган, муниципальный орган, юридическое и физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные (ПДн)- любая информация относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь – лицо, участвующее в эксплуатации криптосредста или использующее результаты его функционирования.

Распределение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародованные персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каких-либо иным способом.

Режимные помещения-помещения, где установлены криптосредства или хранятся ключевые документы к ним.

Средство защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Шифровальные (криптографические) – криптосредства средства:

а) средства – шифровальные - аппаратные, программные и аппаратно–программные средства, система 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;

б) средства имитозащиты - аппаратные, программные и аппаратно-программные средства, система и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) 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 отрытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой записи;

г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых документов (независимо о вида носителя ключевой информации);

е) ключевые документы (независимо от вида носителя ключевой информации).

Приложение 2

АКТ
ввода СКЗИ в эксплуатацию

«____» _____20 ___г.

Комиссия в составе председателя комиссии _____
_____, членов комиссии _____

и ответственного пользователя СКЗИ _____ составили акт о том, что (наименование СКЗИ) установлен в _____ по адресу _____ в помещении № _____, в соответствии с эксплуатационно-технической документацией и введен в эксплуатацию.
Состав (наименование СКЗИ):
Системный блок №_____
Программный комплекс:
(наименование СКЗИ) версия _____ сборка _____
Версия операционной системы: _____
Дополнительно установленное ПО (антивирусное ПО, Прокси-сервер, ПО для удаленного администрирования и т. д):_____
Дополнительно установленное оборудование (наименование, назначение, серийный номер и т.д.)_____

Председатель комиссии:

_____	_____	_____
(должность)	(Ф.И.О.)	(подпись)

Члены комиссии:

_____	_____	_____
(должность)	(Ф.И.О.)	(подпись)

_____	_____	_____
(должность)	(Ф.И.О.)	(подпись)

Приложение 3

№	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ эксплутационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров ключевых документов	Отметка о получении		Отметка о выдаче	
				от кого получены	Дата номер сопроводительного письма	ФИО пользователя СКЗИ	Дата и расписка в получении
	1	2	3	4	5	6	7

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключей документов				Примечание
Ф.И.О. сотрудников органа криптогафической защиты пользователя СКЗИ, производивших подключение (установку)	Дата подключения средств, в которые установлены или к которым подключены СКЗИ	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудника органа криптогафической защиты пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении		
8	9	10	11	12	13		14

Приложение 4

№	Дата	Тип и регистра-ционные номера	Запись об обслуживании крипто-средств	Используемые криптоключи			отметка об уничтожении (стирании)		приме чание
				Тип ключевого документа	Серийный криптографический номер и номер экземпляра ключевого документа	Номер разового ключе-вого носителя или зоны крипто-средств, в которую введены крипто-ключи	дата	Подпись пользователя крипто-средствами	
1	2	3	4	5	6	7	8	9	10

Приложени5

АКТ
вывода СКЗИ из эксплуатацию

«_____» _____20 ___г.

Комиссия в составе председателя комиссии _____
_____, членов комиссии _____

и ответственного пользователя СКЗИ _____ и
о том, что установленный (наименование СКЗИ) по адресу _____ в помещении № _____, выведен из эксплуатации.
Состав (наименование СКЗИ):
Системный блок №_____
Программный комплекс:
(наименование СКЗИ) версия _____ сборка _____

Председатель комиссии:

_____ _____ _____
(должность) (Ф.И.О.) (подпись)

Члены комиссии:

_____ _____ _____
(должность) Ф.И.О.) (подпись)

_____ _____ _____
(должность) (Ф.И.О.) (подпись)

Приложение 6

Журнал контроля соблюдения условий эксплуатации и работоспособности СКЗИ

№	Вид контроля (плановый) внеплановый - причина)	Дата контроля	ФИО контролирую -щего	Результат контроля (без замечаний/ с замечаниями - № замечаний по Журналу замечаний)	Подпись контро-лирую-щего	Подпись ответст-венного Органи-зации	№ прото-кола	при ме-ча-ние

Приложение 7

Журнал замечаний по результатам контроля (лист 1)

№ заме ча-ния	Содержа-ние замечания	Ответственный по замечаниям	Дата замеча-ния	Срок устране-ния замеча-ния	Статус замеча -ния	Подпись ответст-венного	Подпись Ответственно го пользователя СКЗИ	Примеч ание

Лист регистрации изменений (лист 2)

№№ п/п	Дата внесения изменений	Наименование документа, фиксирующего изменения	№№ замененных (исправленных) листов	Подпись лица, внесшего изменения
1				
2				
3				
4				

Лист ознакомления с Порядком обеспечения безопасности персональных данных при помощи криптосредств

№ п/п	Должность	Фамилия, инициалы	Подпись, дата
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			