Министерство образования
Оренбургской области
Государственное казенное
общеобразовательное учреждение
«Специальная (коррекционная)
школа № 10» г. Орска

П Р И К А З

« 09 » августа 2023 г. № 66

«Об утверждении должностного регламента администратора безопасности»

Во исполнение требований Федерального закона 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФАПСИ от 13 июня 2001 года № 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», приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 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 уровня защищенности»,

ПРИКАЗЫВАЮ:

1. Утвердить должностную инструкцию администратора информационной безопасности согласно приложению № 1 к данному приказу.
2. Утвердить Инструкцию для пользователей информационных систем персональных данных согласно приложению № 2 к данному приказу.
3. Утвердить Инструкцию по порядку использования и организации работы со средствами криптографической защиты информации согласно приложению № 3 к данному приказу.
4. Утвердить журнал регистрации пользователей СКЗИ согласно приложению № 4 к данному приказу.
5. Контроль за исполнением приказа оставляю за собой.
6. Приказ вступает с момента подписания.

Директор школы: С.П. Онищенко

Ознакомлен: Смирнов А.А

Приложение № 1
к приказу
от 09.08.2023 г. № 66

Должностная инструкция
администратора информационной безопасности

Настоящая инструкция определяет общие функции, права и обязанности администратора информационной безопасности по вопросам обеспечения информационной безопасности при подготовке и обработке персональных данных на автоматизированных рабочих местах (далее – АРМ), входящих в состав информационной системы персональных данных (далее – ИСПДн).

Администратор информационной безопасности назначается из числа специалистов Учреждения и обеспечивает правильное использование и функционирование установленных средств защиты информации (далее – СЗИ) от несанкционированного доступа (далее – НСД).

Администратор информационной безопасности информации имеет все права администратора СЗИ от НСД.

Настоящая инструкция разработана на основании действующих нормативных документов по защите персональных данных.

1. Основные функции администратора безопасности

1.1. Контроль за выполнением требований, действующих нормативных и руководящих документов по защите персональных данных, при проведении работ на АРМ.

1.2. Работа с учетными записями пользователей ИСПДн (удаление, регистрация новых пользователей), их правильная настройка и разграничение прав доступа пользователей к защищаемым ресурсам ИСПДн согласно разрешительной системе доступа.

1.3. Своевременная корректировка разрешительной системы доступа:

- изменение списка постоянных пользователей ИСПДн (ввод или удаление пользователя из ИСПДн);
- изменение прав доступа к защищаемым программным ресурсам или портам ввода-вывода ИСПДн.

1.4. Корректировка разрешительной системы доступа осуществляется на основании служебной записки пользователя, согласованной с ответственным за эксплуатацию объекта и утвержденной Руководителем Оператора.

1.5. Контроль доступа пользователей к работе на АРМ (в соответствии с перечнем должностей, замещение которых предусматривает данный доступ), выдача внешних носителей информации и соблюдения пользователями требований нормативных и руководящих документов.

1.6. Организация и проведение работ по ежеквартальной смене паролей пользователей для доступа к АРМ.

1.7. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе на АРМ, в том числе и в части периодического контроля за установленными правилами и политиками, учетом машинных носителей.

1.8. Сопровождение системы обеспечения целостности информации при обработке на АРМ:

- соблюдение установленных правил антивирусной защиты;

- контроль соблюдения пользователями установленных правил по информационной безопасности.

1.9. Контроль срока действия сертификатов соответствия ФСТЭК России и ФСБ России.

2. Администратор безопасности имеет право:

2.1. Требовать от специалистов ГКОУ «С(к)ш №10» г. Орска соблюдения требований Политики информационной безопасности, нормативно правовых актов Учреждения по информационной безопасности и исполнения настоящей инструкции.

2.2. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и расследования инцидентов информационной безопасности и фактов (попыток) несанкционированного доступа.

2.3. Требовать от пользователей прекращения обработки информации в ИСПДн в случае:

- нарушение установленного порядка работ;
- нарушение работоспособности средств и систем защиты информации или окончания срока действия сертификатов соответствия ФСТЭК России и ФСБ России.

3. Администратор информационной безопасности обязан:

3.1. Обеспечивать правильное функционирование и поддерживать работоспособность средств СЗИ от НСД в пределах, возложенных на него функций.

3.2. В случаях отказа СЗИ от НСД принимать меры по восстановлению их работоспособности.

3.3. Проводить инструктаж пользователей по правилам работы на АРМ, в том числе с установленными СЗИ от НСД.

3.4. Немедленно докладывать об инцидентах информационной безопасности руководителю ГКОУ «С(к)ш №10» г. Орска и в отдел информационной безопасности министерства.

3.5. Вносить изменения в нормативно правовые документы ГКОУ «С(к)ш №10» г. Орска по информационной безопасности по необходимости.

3.6. Осуществлять не реже одного раза в неделю обновление баз данных антивирусного программного обеспечения.

3.7. Вводить полномочия специалистов ГКОУ «С(к)ш №10» г. Орска в разрешительную систему доступа, обеспечивать их своевременную корректировку.

3.8. Регистрировать факты выдачи съемных носителей информации в журнале учета выдачи съемных носителей.

3.9. Контролировать действия пользователей по правильности затирания информации на съемных носителях информации.

3.10. Заблокировать учетные пользователей на АРМ в случае окончания срока действия сертификата соответствия ФСТЭК России и (или) ФСБ России на любое СЗИ, их используемых в ИСПДН, до момента его продления.

Приложение № 2
к приказу
от 09.08.2023 г. № 66

Инструкция
для пользователей информационных систем персональных данных

Настоящая инструкция определяет действия пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

Обработка информации и ПДн в ИСПДн осуществляется в рамках технологических процессов. Пользователи должны выполнять свои функциональные обязанности в соответствии с утвержденными регламентами данных процессов.

При сборе информации и ПДн работники должны руководствоваться принципом достоверности и достаточности информации и ПДн для установленных регламентами технологических процессов целей обработки, а также недопустимости обработки персональных данных, избыточных по отношению к заявленным целям. Состав собираемых и обрабатываемых ПДн утвержден в рамках каждого процесса.

С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн в учреждении назначается приказом администратор безопасности; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности ответственный за защиту информации.

Допуск пользователей для работы в ИСПДн осуществляется на основании Заявки на регистрацию.

В заявке указывается:

1. Должность (с полным наименованием подразделения), фамилия, имя и отчество работника, контактные данные работника (телефон, кабинет).

2. Основание для регистрации учетной записи (номер приказа о принятии на работу в учреждение или иного договорного документа.

Заявку подписывает руководитель учреждения, подтверждающий, что указанный работник действительно принят в штат учреждения.

Заявка согласуется с администратором и передается в отдел информационной безопасности министерства.

Процедура предоставления (или изменения) прав доступа пользователя к ресурсам ИСПДн определена заявкой. Если в ходе исполнения должностных обязанностей при работе в ИСПДн необходимо лишить пользователя полномочий или необходимо добавить пользователю полномочия по доступу к ресурсам ИСПДн, то необходимо предоставить администратору безопасности заявку о блокировке. При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение работника) учетная запись должна немедленно блокироваться. Руководитель с момента увольнения сотрудника, должен в 3-х дневный срок направить заявку на блокирование учетной записи в администратору информационной безопасности учреждения.

Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

Для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в Журнале учета машинных носителей.

Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (далее - СВТ), входа в систему и все действия при работе в ИСПДн.

Вход пользователя в систему может осуществляться только под своей учетной записью и по персональному паролю.

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на средствах вычислительной техники. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями Инструкции по антивирусной защите.

Каждый пользователь, участвующий в рамках своих функциональных обязанностей в работе в ИСПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн. Соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с ПДн при ее обработке;

незамедлительно сообщать администратору информационной безопасности и в отдел информационной безопасности министерства об инцидентах информационной безопасности при работе с ИСПДн;

незамедлительно сообщать в отдел информационных технологий министерства о плановых/внеплановых перебоях в системе электроснабжения;

знать и строго выполнять правила работы со средствами защиты информации, установленными на средствах вычислительной техники, с помощью которой производится работа в ИСПДн;

хранить в тайне свой пароль (пароли) в соответствии с Инструкцией по парольной защите;

хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу). При выходе в течение рабочего дня из служебной комнаты (помещения) убирать документы с конфиденциальной информацией (ПДн) и съемные цифровые носители в сейф (металлический шкаф) и запирать их на ключ;

выполнять требования Правил антивирусной защиты в ИСПДн в полном объеме;

немедленно известить ответственного за защиту информации и отдел информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

некорректного функционирования установленных на компьютеры технических средств защиты;

непредусмотренных отводов кабелей и подключенных устройств.

Пользователю категорически запрещается:

использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;

самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц при работе с ИСПДн;

записывать и хранить конфиденциальную информацию из ИСПДн (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

подключение к структурированной кабельной сети аппаратных средств минуя средства защиты информации, в том числе криптографические;

размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, а именно экраны видеомониторов в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами.

Приложение № 3
к приказу
от 09.08.2023 г. № 66

Инструкция
по порядку использования и организации работы со средствами криптографической защиты информации

1. Общие положения

1.1. Настоящая инструкция устанавливает единые требования по обеспечению безопасности функционирования средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну (далее СКЗИ), и определяет порядок учета, выдачи, хранения, уничтожения СКЗИ, а также действия при компрометации ключей и восстановлении связи.

Порядок применения процедуры электронно-цифровой подписи может дополнительно уточняться заключаемыми со сторонними организациями договорами (соглашениями), при условии соблюдения требований настоящей инструкции.

1.2. В настоящей инструкции использована следующая терминология:

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Безопасность информации - состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системой, от внутренних или внешних угроз

Доступ к информации (доступ) - ознакомление с информацией, ее обработка; в частности, копирование, модификация или уничтожение информации.

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Криптографическая (шифровальная защита) – защита информации от ее несанкционированного доступа и модификации посторонних лиц при помощи алгоритмов криптографического преобразования.

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

Конфиденциальность – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

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

Несанкционированный доступ (НСД) - доступ, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Обработка информации - совокупность операций сбора, накопления, ввода-вывода, приема-передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения, осуществляемых над информацией.

Ответственный пользователь – должностное лицо, назначенное ответственным за обеспечение функционирования и безопасности криптосредств.

Пользователь криптосредств – субъект, наделенный правом применения средства криптографической защиты для выполнения возложенных обязанностей.

Ключевой документ (криптоключ) – сохраняемая в тайне, закрытая информация, используемая криптографичеким алгоритмом при шифровании/расшифровании сообщений, постановке и проверке цифровой подписи, вычислении кодов аутентичности.

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

Шифровальные (криптографические) средства:

а) 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;

б) средства имитозащиты – аппаратные, программные и аппаратно–программные средства, системы 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 открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

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 от вида носителя ключевой информации);

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

2. Организационные требования

2.1. Сотрудники, использующие при работе средства криптографической защиты информации, должны быть ознакомлены с требованиями настоящей

инструкции и другими документами, регламентирующими обеспечение безопасности функционирования криптосредств. Они несут персональную ответственность за несоблюдение требований указанных документов в соответствии с законодательством Российской Федерации.

2.2. Обеспечение функционирования и безопасности СКЗИ, возлагается на ответственного за эксплуатацию криптосредств защиты информации.

На Ответственного пользователя возлагается выполнение следующих обязанностей:

– учет криптосредств, эксплуатационной и технической документации с использованием условных наименований и регистрационных номеров;

– контроль за соблюдением 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 и ключевых документах к ним;

– организация работ по безопасному применению средств криптографической защиты информации;

– надежное хранение резервных ключевых документов, эксплуатационной и технической документации к криптосредствам;

– принятие мер к минимизации возможных последствий при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

– обучение лиц, использующих криптосредства, работе с ними;

– учет лиц, допущенных к работе со средствами криптографической защиты информации (пользователи криптосредств);

– контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

– разбирательства по фактам нарушения условий хранения и использования криптосредств, которые могут привести к нарушению или к снижению уровня защищенности информации;

2.3. К работе с СКЗИ пользователи допускаются решением руководителя учреждения.

Пользователи криптосредств обязаны:

- соблюдать требования по обеспечению безопасности функционирования СКЗИ;
- не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и мерах защиты;
- не допускать снятие копий с ключевых документов;
- не допускать вывод ключевых документов на принтер;
- хранить ключевую информацию в сейфах и помещениях, гарантирующих их сохранность и конфиденциальность;
- не допускать записи на ключевой носитель посторонней информации;
- во время работы не оставлять ключевые документы без присмотра;
- сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;
- немедленно уведомлять администратора информационной безопасности, о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к нарушению безопасности.

- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы администратору информационной безопасности пользователю при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

2.4. Ключевые документы или исходная ключевая информация для выработки ключевых документов изготавливаются ФСБ России на договорной основе или лицами, имеющими лицензию ФСБ России на деятельность по изготовлению шифровальных средств.

3. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним

3.1. Помещения, где установлены СКЗИ или хранятся ключевые документы к ним (далее - режимные помещения), должны быть оборудованы средствами охранно-пожарной сигнализации, связанной со службой охраны здания. Входные двери должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время.

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

3.3. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны.

3.4. Пользователи криптосредств хранят выданные им для использования ключевые документы в сейфах индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. В случае отсутствия индивидуального сейфа по окончании рабочего дня Пользователь обязан сдать СКЗИ Ответственному пользователю.

Хранение эксплуатационной и технической документации к СКЗИ, а также копии сертификатов открытых ключей ЭЦП в бумажном виде, осуществляется Ответственным пользователем.

Хранение криптоключей и инсталляционного ПО СКЗИ допускается в одном сейфе с другими документами при условиях исключающих их непреднамеренное уничтожение или иное, непредусмотренное правилами применение.

4. Порядок учета и выдачи средств криптографической защиты информации

4.1. Должностные лица, допущенные к работе с криптосредствами, заносятся в журнал регистрации пользователей. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, а также ключевые документы подлежат учету в журнале поэкземплярного учета. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.

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

4.2. Все необходимые для работы экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета Пользователям криптосредств, несущим персональную ответственность за их сохранность.

4.3. Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и администратором информационной безопасности под расписку в соответствующих журналах поэкземплярного учета. Передача учтенных СКЗИ без санкции администратора информационной безопасности категорически запрещается.

5. Порядок уничтожения средств криптографической защиты информации

5.1. СКЗИ непригодные для дальнейшего использования, или надобность в использовании которых миновала, уничтожаются (утилизируются).

5.2. 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).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 криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

5.3. Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации.

5.4. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожают путем сжигания или с помощью бумагорезательных машин.

5.5. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам.

5.6. Ключевые документы уничтожаются пользователями совместно с Ответственным пользователем криптосредств под расписку журнале поэкземплярного учета, при этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. Уничтожение большого объема ключевых документов может быть оформлено актом. Уничтожение по акту производит комиссия в составе не менее трех человек из числа лиц, допущенных к пользованию криптосредств. 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 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 журнале поэкземплярного учета.

6. Действия при компрометации или повреждении ключевой информации.

6.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает необходимую защиту информации. Криптоключи, в отношении которых возникло подозрение в компрометации, необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

6.2. К событиям, связанным с компрометацией криптографических ключей, относятся:

– утеря (хищение) носителей ключевой информации, в том числе с последующим их обнаружением;

– увольнение сотрудника, имевшего доступ к ключевой информации;

– передача закрытых ключей по линиям связи;

– нарушение правил хранения или уничтожения криптоключа;

– несанкционированное или безучетное копирование ключевой информации;

– нарушение целостности печати на сейфе с ключевыми носителями;

– вскрытие фактов утечки (искажения или изменения) передаваемой информации;

– все случаи, когда нельзя достоверно установить, что произошло с носителем ключевой информации.

6.3. При наступлении любого из перечисленных случаев, или иных нарушениях, которые могут привести к компрометации криптоключей, пользователь должен прекратить использование СКЗИ и немедленно сообщить о произошедшем администратору информационной безопасности.

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

6.5. В каждом случае, по факту (или предполагаемой) компрометации ключевых документов, специально назначенной комиссией, проводится служебное расследование. Результатом расследования является квалификация или не квалификация данного события как компрометация.

6.6. О факте компрометации ключевой информации пользователями совместно с администратором информационной безопасности производится информирование всех заинтересованных участников информационного обмена.

6.7. Выведенные из действия скомпрометированные ключевые документы после проведения расследования уничтожаются, о чем делается соответствующая запись в журнале поэкземплярного учета.

Приложение № 4
к приказу
от 09.08.2023 г. № 66

Журнал регистрации пользователей СКЗИ

№ п.п.	Должность пользователя	Ф.И.О. пользователя	Дата регистрации	Дата выбытия	Примечание
1	2	3	4	5	6