ПРИНЯТО
Педагогическим советом
МОАУ «СОШ 65»
Протокол 1 № от 30.08.2023 г.

«УТВЕРЖДАЮ»
врио директора МОАУ «СОШ 65»
_____ Н.Н. Чернышова
Приказ № 229 от 01.09.2023 г.

ПОЛОЖЕНИЕ ОБ ОРГАНИЗАЦИИ И ПРОВЕДЕНИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В МОАУ «СОШ № 65»

Список сокращений и обозначений АВС — антивирусные средства
АРМ — автоматизированное рабочее место АС — автоматизированная система
АСЗИ — автоматизированная система в защищенном исполнении
ИСПДн — информационная система персональных данных КОИ — криптографически опасная информация
ЛВС — локальная вычислительная сеть МЭ — межсетевой экран
ОС — операционная система ПДн — персональные данные
ПМВ — программно-математическое воздействие ПО — программное обеспечение
ПЭМИН — побочные электромагнитные излучения и наводки САЗ — система анализа защищенности
СЗИ — средства защиты информации
СЗПДн — система (подсистема) защиты персональных данных СКЗИ — средства криптографической защиты информации СОВ — система обнаружения вторжений
ТС — техническое средство
УБПДн — угрозы безопасности персональных данных

1. Общие положения

1.1. Положение об организации и проведению работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных (далее – Положение) разработано в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «Оперсональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», методическими рекомендациями ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

1.2. Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условийхранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в пределы границы контролируемой зоны.

1.3. При обеспечении безопасности персональных данных в ИСПДн с использованием криптографических средств защиты информации все сотрудники образовательной организации обязаны выполнять требования приказа ФСБ России от 21.02.2008 № 149/6/6-622 «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных».

2.Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн

2.1. Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании приказа, который издается руководителем общеобразовательной организации, и в соответствии со списком лиц, допущенных к работе в ИСПДн. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн руководителем образовательной организацией назначается администратор безопасности с целью контроля выполнения необходимых мероприятий по обеспечению безопасности ответственный за защиту информации.

2.2. Пользователь имеет право в отведённое ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. Полномочия пользователей (роли пользователей) к информационным ресурсам определяются в матрице доступа, утверждаемой руководителем образовательной организации. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтённые в журнале учёта машинных носителей.

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

2.4. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

2.5. Запись информации, содержащей ПДн, осуществляется пользователем на съёмные машинные носители информации, соответствующим образом учтённые в журнале учёта машинных носителей.

2.6. При работе со съёмными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить использование зараженных носителей и действовать в соответствии с требованиями данного Положения.

2.7. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несёт персональную ответственность за свои действия и обязан:

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

– знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;

– хранить в тайне свой пароль (пароли). В соответствии с п.п. 8.5., 8.6. данного Положения и с установленной периодичностью менять свой пароль (пароли);

– хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

– выполнять требования по организации антивирусной защиты в полном объёме.

Немедленно известить ответственного за защиту информации и (или) администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа, rutoken и т.д.) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

– нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данным защищаемым СВТ;

– 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 ПЭВМ 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;

– записывать и хранить конфиденциальную информацию (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);

– оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

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

– размещать средства ИСПДн так, чтобы с не существовало возможности визуального считывания информации.

2.8. Администратор безопасности (ответственный за защиту информации) обязан:

– знать состав основных и вспомогательных технических систем, и средств (далее – ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее – ПО) в ИСПДн;

– контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;

– производить необходимые настройки подсистемы управления доступом, установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:

– реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

– вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;

– своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

– своевременно вносить изменения и дополнения в список сотрудников, допущенных к работе в ИСПДн;

– проводить инструктаж сотрудников – пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;

– контролировать своевременное (не реже чем один раз в течение 360 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;

– обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;

– осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

– настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;

– вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;

– проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;

– организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации. Сопровождать подсистемы обеспечения целостности информации в ИСПДн;

– периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;

– восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;

– вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;

– контролировать отсутствие на магнитных носителях остаточной информации по окончании работы пользователей;

– периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования;

– проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

– сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств ИСПДн;

– контролироватьсоответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;

– обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);

– присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

– поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положений в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

– докладывать ответственному за защиту информации, ответственному за эксплуатацию ИСПДн о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

– вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

2.9. Администратор безопасности и ответственный за защиту информации имеют право:

– требовать от сотрудников – пользователей ИСПДн – соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;

– инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;

– требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

– участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

3. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и СЗИ определяет действия, связанные с функционированием ИСПДн, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачи:

– определение мер защиты от потери информации;

– определение действий восстановления в случае потери информации.

Действие настоящего Положения распространяется на всех пользователей образовательной организации, имеющих доступ к ресурсам ИСПДн, а также основным системам обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

– системы жизнеобеспечения;

– системы обеспечения отказоустойчивости;

– системы резервного копирования и хранения данных; – системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

Ответственным работником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, и за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, является Администратор безопасности.

Происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации (далее – Инцидент), может произойти в результате:

– непреднамеренных действий пользователей.

– преднамеренных действий пользователей и третьих лиц.

– нарушения правил эксплуатации технических средств ИСПДн.

– возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование работником в «Журнале учета нештатных ситуаций»

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники образовательной организации предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

Все критичные помещения образовательной организации (помещения, в которых размещаются элементы ИСПДн и средства защиты) при необходимости должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции могут подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

– локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

– источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

– дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

– резервные линии электропитания в пределах комплекса зданий;

– аварийные электрогенераторы.

Системы обеспечения отказоустойчивости включают технологии:

– кластеризации;

– избыточных массивов независимых жестких дисков RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель

(жесткий диск, оптический диск и т.п.).

Резервное копирование и хранение данных должно осуществляться на периодической основе:

– для обрабатываемых персональных данных – еженедельное резервное копирование с сохранением копий на файловом сервере или роботизированной библиотеке LTO с постоянным хранением не менее четырех последних версий резервных копий;

– для технологической информации – не реже 1 раза в 6 месяцев;

– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже 1 раза в 6 месяцев, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Съемные носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения (по возможности в здании, территориально удалённом от здания в котором размещается ИСПДн).

Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на администратора безопасности.

Ответственность за проведение мероприятий по восстановлению средств защиты информации (далее – СЗИ) возлагается администратора безопасности.

4. Порядок контроля защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий

4.1. Контроль защиты информации в ИСПДн – комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

4.2. Основными задачами контроля являются:

–проверка организации выполнения мероприятий по защите информации в образовательной организации, учёта требований по защите информации в разрабатываемых плановых и распорядительных документах;

–выявление демаскирующих признаков объектов ИСПДн;

–уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

–проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

–проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

–проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

–проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;

–оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;

–разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

4.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн Учреждения, и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации. Перечень каналов утечки устанавливается в соответствии с моделью угроз.

4.4. В ходе контроля проверяются:

–соответствие принятых мер по обеспечению безопасности персональных данных (далее – ОБ ПДн);

–своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;

–полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

–эффективность применения организационных и технических мероприятий по защите информации;

–устранение ранее выявленных недостатков.

Кроме того, могут проводиться необходимые измерения и расчеты приглашенными для этих целей специалистами организации, имеющей соответствующие лицензии ФСТЭК России.

4.5. Основными видами технического контроля являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

4.6. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите

информации администратор безопасности докладывает руководителю для принятия ими решения о прекращении обработки информации и проведения, соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо в соответствующих журналах учета результатов контроля.

4.7. Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее – предпосылка). По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию руководителя или ответственного за защиту информации проводится расследование.

Для проведения расследования назначается комиссия с привлечением администратора безопасности. Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования руководитель принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

4.8. Ведение контроля защиты информации осуществляется путём проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов организации проводятся,как правило, силами администратора безопасности и(или) ответственного за защиту информации, в соответствии с утвержденным планом или по согласованию с руководителем.

4.9. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора безопасности, ответственного за защиту информации, ответственного за эксплуатацию объекта. Для обследования ИСПДн может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

4.10. Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в «Аттестате соответствия» и(или) требованиям по безопасности персональных данных.

4.11. В ходе обследования проверяется:

– соответствие текущих условий функционирования обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;

– соблюдение организационно-технических требований помещений, в которых располагается ИСПДн;

– сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;

– соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в настоящем положении;

– выполнение требований по защите информационных систем от несанкционированного доступа;

– выполнение требований по антивирусной защите.

4.12. Для выявления радиоэлектронных устройств и проводов неизвестного назначения, преднамеренного нарушения защитных свойств оборудования, а также не предусмотренных правилами эксплуатации отводов от оборудования и соединительных линий, проложенных в выделенных и защищаемых помещениях, а также других нарушений и способов возникновения каналов утечки информации необходимо:

–тщательно осмотреть мебель, сувениры (особенно иностранного производства), оборудование, установленное в этом помещении, осветительную аппаратуру, ниши отопительных батарей, шторы, оконные проёмы и т.д.;

–вскрыть и осмотреть розетки, выключатели осветительной сети, люки вентиляции и каналы скрытой проводки;

–проверить качество установки стеклопакетов оконных проёмов;

–провести аппаратурную проверку помещения на отсутствие возможно внедренных электронных устройств перехвата информации (при наличии соответствующей аппаратуры), при необходимости для проведения данных видов работ могут привлекаться организации, имеющие соответствующие лицензии ФСБ России.

4.13. Государственный контроль состояния защиты информации осуществляется Федеральной службы по техническому и экспортному контролю России и Федеральной службой безопасности России в рамках их полномочий в соответствии с действующим законодательством Российской Федерации. Доступ представителей указанных федеральных органов исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения сотрудника, а также документа установленной формы на право проведения проверки.

4.14. Классификация нарушений защиты ПДн

Нарушения, связанные с выполнением требований руководящих документов по безопасности информации, с применением средств защиты информации и разграничением доступа, использованием технического, программного обеспечения информационных систем, по степени их опасности целесообразно разделить на:

– нарушения 1 - ой категории; – нарушения 2 - ой категории; – некатегорированные нарушения.

К нарушениям 1-ой категории относятся нарушения, повлекшие за собой разглашение (утечку) защищаемых сведений, утрату бумажных документов и магнитных носителей информации, уничтожение (искажение) информационного и программного обеспечения, выведение из строя технических средств.

К нарушениям 2-ой категории относятся нарушения, в результате которых возникает возможность разглашения (утечки) защищаемых сведений или утраты бумажных документов и магнитных носителей информации, уничтожения (искажения) информационного и программного обеспечения, выведения из строя технических средств.

Остальные нарушения, не вошедшие в первую и вторую категории, относятся к некатегорированным нарушениям.

Нарушения 1-ой категории:

–утрата бумажных документов и магнитных носителей информации, содержащих охраняемые (конфиденциальные) сведения;

–действия работников структурных подразделений, приведшие к искажению или разрушению охраняемых сведений или иных защищаемых ресурсов;

–умышленная разработка, использование и распространение вредоносных программ (программ - вирусов и т. п.), а также непреднамеренные (по халатности) виновные действия, приведшие к

использованию и распространению таких программ;

–несанкционированная корректировка адресной информации маршрутов и путей коммутации технических средств пользователей данных и сообщений в информационных сетях;

–компрометация средств защиты информации;

–несанкционированный доступ к защищаемой информации; –

несанкционированные действия работников, направленные на сбор, накопление и обобщение охраняемых сведений.

Нарушения 2-ой категории:

–компрометация паролей;

–несвоевременная замена паролей и идентификаторов при их компрометации;

–вывод информации, содержащей охраняемые сведения, на неучтенные носители информации и машинные документы;

–несанкционированное внесение изменений в программное информационное обеспечение информационных систем;

–несанкционированное отключение средств защиты информации;

–самовольное отключение средств антивирусной защиты;

–несанкционированное подключение к вычислительной сети нештатных технических средств обработки информации (например, личных портативных компьютеров и т.п.);

–вход в систему в обход системы защиты (загрузка ОС с флэш-карты или загрузочного CD);

–отсутствие разграничения доступа к информации, содержащей охраняемые сведения и обрабатываемой в многопользовательском режиме, при работе по технологии "Клиент-Сервер", а также доступа из других информационно - вычислительных сетей по каналам корпоративной или открытой сети;

– нарушение порядка учета, хранения и обращения со средствами разграничения доступа к информации.

Перечень категорированных нарушений должен ежегодно корректироваться и доводиться до всех работников, работающих с защищаемыми ресурсами.

4.15. Оперативная реакция на нарушения режима безопасности

Работники обязаны немедленно уведомлять непосредственных руководителей и ответственного за обеспечение безопасности ПДн лица о случаях нарушения защиты или об обнаруженных уязвимостях (слабостях) в информационных системах и средствах защиты.

Функции своевременной и адекватной реакции на выявленные нарушения защиты ПДн, требующих оперативного реагирования, например, таких как обнаружение и нейтрализация вторжений хакеров или внедрение программных вирусов, возлагаются на Администратора ИСПДн и Администратора безопасности ИСПДн. Эти работники должны быть доступны в течение рабочего времени (лично, по телефону или электронной

почте).

Работники образовательной организации должны обращаться к ним при обнаружении признаков нарушения защиты ПДн в соответствии с установленной процедурой.

4.16. Расследование инцидентов, связанных с нарушениями защиты ПДн

По каждому инциденту, связанному с нарушением защиты ПДн в образовательной организации, должно проводиться расследование. Ответственность за проведение расследования возлагается на лиц ответственных за обеспечение безопасности ПДн.

В результате расследования необходимо определить:

–нарушителя (нарушителей) защиты ПДн;

–категорию нарушения и величину нанесенного ущерба (если он есть);

–причины, приведшие к нарушению;

–меры и средства, необходимые для ликвидации нежелательных последствий;

–меры и средства, необходимые для ликвидации или ослабления причин, приведших к нарушению, чтобы подобные нарушения не повторялись в будущем.

Результаты расследования должны оформляться документально. Вид нарушения, если такового не было ранее, должен быть включен в перечень категорированных нарушений по защиты ПДн.

5.Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных

5.1. Перед началом работы в ИСПДн пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации под роспись.

5.2. Пользователи должны продемонстрировать администратору безопасности и (или) ответственному за защиту информации наличие необходимых знаний и умений для выполнения требований настоящего Положения. Администратор безопасности должен вести журнал учета проверок знаний и навыков пользователей.

5.3. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего положения, к работе в ИСПДн не допускаются.

5.4. Ответственным за организацию обучения и оказание методической помощи в Учреждении является администратор безопасности.

5.5. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов ИСПДн, организаций-лицензиатов ФСТЭК России и ФСБ России.

5.6. К работе в ИСПДн допускаются только сотрудники, прошедшие

первичный инструктаж ОБ (основы безопасности) в ИСПДн и показавшие твердые теоретические знания и практические навыки, о чём делается соответствующая запись в Журнале учёта пользователей, допущенных к информационным системам персональных данных.

5.7. Администратору безопасности рекомендовано иметь профильное образование (либо дипломы о повышении квалификации) в области защиты информации. Рекомендуется прохождение администратором специализированных курсов по администрированию средств защиты информации, используемых в ИСПДн.

6.Порядок проверки электронного журнала обращений к ИСПДн

6.1. Настоящий раздел Положения определяет порядок проверки электронных журналов обращений к ресурсам ИСПДн.

6.2. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к защищаемой информации в ИСПДн.

6.3. Право проверки электронного журнала обращений имеют:

– администратор безопасности;

– ответственный за обеспечение безопасности ПДн; – руководитель образовательной организации.

6.4. На технических средствах ИСПДн, на которых установлены специализированные средства защиты информации (далее – СЗИ) проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

6.5. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлены случаи НСД к информации конфиденциального характера, то вступает в силу п.п. 4.6., 4.7. данного Положения.

6.6. Проверке подлежат все электронные журналы ИСПДн.

6.7. Проверка должна проводиться не реже, чем один раз в неделю с целью своевременного выявления фактов нарушения требований настоящего Положения.

6.8. Факты проверок электронных журналов отражаются в специальном журнале проверок электронных журналов. После каждой проверки Администратор безопасности делает соответствующую отметку в журнале и ставит свою роспись.

7.Правила антивирусной защиты

7.1. Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения (ПО), компьютерных вирусов и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение. Настоящие правила распространяются на все объекты ИСПДн образовательной организации.

7.2. К использованию на компьютерах допускаются сертифицированные антивирусные средства, централизованно закупленные у

разработчиков (поставщиков) указанных средств.

7.3. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности.

7.4. Администратор безопасности осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

7.5. Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

7.6. Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съёмный носитель).

Настройки средств антивирусной защиты должны быть выполнены в соответствии с требованиями безопасности персональных данных определенными для данной ИСПДн уровня защищенности. Настройку средств антивирусной защиты выполняет администратор безопасности.

7.7. Файлы, помещаемые в электронный архив на электронных и магнитных носителях, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

7.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором безопасности должна быть выполнена антивирусная проверка ИСПДн.

7.9. На компьютеры запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

7.10. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

– приостановить обработку данных в ИСПДн;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также смежные подразделения, использующие эти файлы в работе;

–совместно с владельцем зараженных вирусом файлов провести анализ

возможности, дальнейшего их использования;

–провести лечение или уничтожение зараженных файлов.

7.11. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на ответственного за защиту информации.

7.12. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИСПДн.

8.Правила парольной защиты

8.1. Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.

8.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора безопасности.

8.3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ОВТ самостоятельно с учетом следующих требований:

– пароль должен быть не менее 6 символов;

–в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

–символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;

–пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

–при смене пароля новое значение должно отличаться от предыдущих;

–пользователь не имеет права сообщать личный пароль другим лицам.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

8.4. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей сотрудников (исполнителей) в их отсутствие, сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение руководителю структурного подразделения. Запечатанные конверты (пеналы) с паролями исполнителей

должны храниться в недоступном месте у руководителя структурного подразделения.

8.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 360 дней.

8.6. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри образовательной организации т.п.) должна производиться администратором безопасности (либо новым постоянным пользователем) немедленно после окончания последнего сеанса работы данного пользователя с системой на основании указания начальника отдела.

8.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри образовательной организации и другие обстоятельства) администратора безопасности.

8.8. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по восстановлению парольной защиты.

8.9. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора безопасности.

9.Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн

9.1. Настоящие правила регламентируют обеспечение безопасности информации при проведении обновлении, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

9.2. Все изменения конфигураций технических и программных средств ИСПДн должны производиться только на основании заявок ответственного за эксплуатацию конкретного ИСПДн.

9.3. Право внесения изменений в конфигурацию аппаратно-программных средств защищенных ИСПДн предоставляется в отношении системных и прикладных программных средств – администратору безопасности;

9.4. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных сотрудников и подразделений, запрещено.

9.5. Процедура внесения изменений в конфигурацию системных и прикладных программных средств ИСПДн инициируется заявкой ответственного за эксплуатацию ИСПДн.

9.6. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

– установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности

решения данной задачи в данной ИСПДн;

– обновление (замена) на компьютере(ах) программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);

– удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

9.7. Также в заявке указывается условное наименование ИСПДн. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанного компьютера.

9.8. Заявку ответственного за эксплуатацию ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает руководитель ИТ подразделения, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

После чего заявка передается администратору безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера, указанного в заявке ИСПДн.

9.9. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производится администратором безопасности.

9.10. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

9.11. Установка и обновление ПО (системного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, прикладного ПО – с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

9.12. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

9.13. После установки (обновления) ПО, администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки и произвести соответствующую запись в «Журнале учета нештатных ситуаций в ИСПДн, выполнения профилактических работ, установки и модификации программных средств

на компьютерах ИСПДн».

9.14. Формат записей «Журнала учёта нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» устанавливается приказом руководителя образовательной организации.

9.15. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за защиту информации. В данном случае администратор безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров с отметками о внесении изменений в состав программных средств, должны храниться вместе с техническим паспортом на ИСПДн и «Журналом учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» у ответственного за защиту информации.

9.16. Копии заявок могут храниться у администратора безопасности:

–для восстановления конфигурации ИСПДн после аварий;

–для контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;

–для проверки правильности установки и настройки средств защиты ИСПДн.

9.17. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора безопасности и сотрудника ответственного за эксплуатацию данной ИСПДн.

9.18. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная записьпользователя), под которым он будет регистрироваться, и работать на данном компьютере.

9.19. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя («группового имени») запрещено.

10. Правила регистрации пользователей

10.1. Процедура регистрации (создания учётной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой ответственного за эксплуатацию данной ИСПДн. Форма заявки приведена ниже.

В заявке указывается:

–содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);

–должность (с полным наименованием отдела),

фамилия, имя и отчество сотрудника;

–имя пользователя (учетной записи) данного сотрудника;

–полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

10.2. Заявку рассматривает руководитель, визируя её, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем подписывает задание администратору безопасности на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.

10.3. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор безопасности производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 360 дней.

10.4. После внесения изменений в списки пользователей администратор безопасности должен обеспечить настройки средств защиты, соответствующие требованиям безопасности, указанной ИСПДн. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписью исполнителя – администратор безопасности.

10.5. Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное(ые) значение(ия) пароля(ей), которое(ые) он обязан сменить при первом же входе в систему.

10.6. Исполненные заявка и задание (за подписью администратора безопасности) передаются руководителю на хранение. Они могут впоследствии использоваться:

–для восстановления полномочий пользователей после аварий ИСПДн;

–для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;

–для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

11. Порядок контроля соблюдения условий использования средств защиты информации, в том числе криптографических

11.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее –

СЗИ).

11.2. Технические средства защиты информации являются важным компонентом ОБ ПДн.

11.3. Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как сотрудниками, обрабатывающими конфиденциальную информацию, так и администратором безопасности ИСПДн.

11.4. Право проверки соблюдения условий использования средств защиты информации имеют:

– директор;

– ответственный за защиту информации; – администратор безопасности.

11.5. Пользователю ИСПДн категорически запрещается:

– обрабатывать конфиденциальную информацию с отключенными СЗИ;

– менять настройки СЗИ.

11.6. Администратору безопасности запрещается менять настройки программно-аппаратных СЗИ, предустановленные специалистом организации, имеющей лицензию на деятельность по технической защите информации, бе согласования с этой организацией.

11.7. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлено нарушение требования п. 10.5. то вступает в силу п.п. 4.6., 4.7. данного Положения.

11.8. Криптографические средства защиты информации должны использоваться в соответствии с технической и эксплуатационной документацией на них, а также в соответствии с правилами пользования ими.

12. Порядок охраны и допуска посторонних лиц в пределы границы контролируемой зоны

12.1. Настоящее Положение устанавливает порядок охраны (сдачи под охрану) помещений ИСПДн внутри границы контролируемой зоны.

12.2. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.

12.3. При отсутствии сотрудников, ответственных за вскрытие (сдачу под охрану) помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа, о чем составляется акт.

12.4. При закрытии помещений и сдачей их под охрану сотрудники, ответственные за помещения проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации, на которых содержится конфиденциальная информация, убираются для хранения в опечатываемый сейф (металлический шкаф).

12.5. В соответствии с требованиями данного Положения при обработке защищаемой информации в ИСПДн исключить неконтролируемое пребывание посторонних лиц в пределах границ контролируемой зоны ИСПДн, определенных соответствующим приказом.

13. Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации

13.1. В обязательном порядке уничтожению подлежат повреждённые, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн. Не допускается стирание неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с настоящим порядком.

13.2. Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания, встроенные в сертифицированные средства защиты информации).

13.3. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирание информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.

13.4. Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожают путем сжигания или с помощью любых бумагорезательных машин.

13.5. По факту уничтожения или стирания носителей составляется акт, в журналах учета делаются соответствующие записи.

13.6. Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: ответственный за эксплуатацию ИСПДн, ответственный за защиту информации, администратор безопасности.

14. Заключительные положения

14.1. Требования настоящего Положения обязательны для всех сотрудников, обрабатывающих конфиденциальную информацию (персональные данные).

14.2. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.