

Рассмотрено на Совете колледжа
Протокол № 10 от 28.12.2018

УТВЕРЖДАЮ
Директор БПОУ ВО «Вологодский
педагогический колледж»
С.А. Панахова
Приказ № 440 от 29.12.2018

ПОЛОЖЕНИЕ

об организации и проведении работ по обеспечению безопасности персональных данных обрабатываемых в информационных системах персональных данных и/или без использования средств автоматизации.

1. Общие положения.

1.1. Данное «Положение об организации и проведении работ в БПОУ ВО «Вологодский педагогический колледж» (далее – Колледж) по обеспечению безопасности персональных данных при их автоматизированной обработке и/или без использования средств автоматизации в информационных системах персональных данных» (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных 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 (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2. Положение определяет порядок работы пользователей и администраторов ИСПДн, сотрудников, ответственных за техническое обеспечение, а также администратора информационной безопасности, в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения 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 помещения ИСПДн, порядок создания резервных копий ИСПДн, правила хранения и регистрации носителей информации.

1.3. При обеспечении безопасности персональных данных в ИСПДн с

использованием криптографических средств защиты информации все сотрудники обязаны выполнять требования, изложенные в документе «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» (ФСБ России, № 149/6/6-622, 2008).

2. Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации.

Настоящий порядок определяет действия 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 директором и в соответствии со списком лиц, допущенных к работе в ИСПДн. С целью обеспечения ответственности за нормальное функционирование и контроль работы средств защиты информации в ИСПДн директором назначается администратор информационной безопасности; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности назначается ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн.

2.2. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. Полномочия пользователей к информационным ресурсам определяются в матрице доступа, которая создается ответственным за обеспечение безопасности персональных данных при их обработке в ИСПДн и утверждается директором колледжа. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в Журнале учета 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, может, осуществляется пользователем на съемные машинные носители информации, соответствующим образом учтенные в Журнале учета машинных носителей.

2.6. 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 компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование 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 в помещение, в котором производится обработка ПДн, 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;

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

- хранить в тайне свой пароль (пароли) и с установленной периодичностью менять свой пароль (пароли);

- хранить в установленном порядке свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе, или ящике, закрывающемся на ключ;

- выполнять требования Положения по организации антивирусной защиты в полном объеме.

Немедленно известить ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн и (или) администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушения или несоответствия 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.

2.8. Пользователю категорически **запрещается**:

- использовать компоненты программного и аппаратного обеспечения персонального компьютера в неслужебных целях;

- вносить какие-либо изменения в конфигурацию аппаратных 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 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 существовала возможность визуального считывания информации.

2.9. Лица, ответственные за защиту персональных данных в Колледже.

Ответственный за обработку ПДн - штатный сотрудник определяющий уровень доступа и ответственность лиц участвующих в обработке ПДн. Назначается приказом директора.

Ответственный за обеспечение безопасности персональных данных – штатный сотрудник отвечающий за проведение мероприятий, связанных с защитой ПДн (организационных и технических), а также осуществляющий контроль за соблюдением требований по защите ПДн в подразделениях. Назначается приказом директора.

Администратор информационной безопасности – штатный сотрудник, ответственный за защиту автоматизированной системы (АС) от несанкционированного доступа (НСД) к информации. Назначается приказом директора.

2.10. Администратор информационной безопасности (при его отсутствии ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн) 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;
- контролировать доступ лиц в помещение в соответствии со списком 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 60 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 не реже одного раза в месяц;
- 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 совместно с лицами, ответственными за техническое обеспечение.
- 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;

- контролировать соответствие 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;
- вести журнал учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн;
- поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положения;
- в случае отказа средств и систем защиты информации принимать меры по их восстановлению;
- докладывать ответственному за обработку персональных данных о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;
- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

2.11. Администратор информационной безопасности и ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн 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 обработки персональных данных без использования средств автоматизации.

3.1. Обработка персональных данных без использования средств автоматизации может осуществляться в виде документов на бумажных носителях.

3.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

3.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

3.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

3.4.1. типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

3.4.2. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

3.4.3. типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

3.4.4. типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

3.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с

сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

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

4.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

4.2. Резервному копированию подлежат базы данных ПДн, а так же прикладное программное обеспечение, предназначенное для работы с этими базами данных в случае, если оно подвергается модификации со стороны разработчиков ИСПДн.

4.3. Резервное копирование должно осуществляться в специально отведенный сетевой каталог на файловом сервере, а так же путем записи на отчуждаемый носитель.

4.4. Права доступа к сетевым каталогам должны исключать возможность доступа пользователей к резервным копиям других ИСПДн, хранящихся на сервере, при отсутствии допуска к работе в этих ИСПДн.

4.5. Базы данных и программное обеспечение должны копироваться в разные папки на файловом сервере.

4.6. На файловом сервере, помимо актуального состояния баз данных и программного обеспечения, должны храниться минимум два их исторических состояния.

4.7. Раз в месяц администратор ИСПДн создает резервную копию баз данных и программного обеспечения ИСПДн на отчуждаемый носитель, хранящийся у администратора информационной безопасности в закрывающемся на ключ хранилище.

4.8. К использованию, для создания резервных копии в ИСПДн, допускаются только зарегистрированные в журнале учета носители.

4.9. Резервное копирование на файловый сервер должно осуществляться непосредственно после любого изменения состояния баз данных или программного обеспечения этих баз, но не реже, чем раз в неделю.

4.10. Если программный продукт, на основе которого функционирует ИСПДн, имеет функцию резервного копирования, то администратор ИСПДн создает резервную копию при помощи данной функции.

4.11. Специалист, ответственный за техническое обеспечение учреждения создает резервную копию сетевого каталога, в котором хранятся резервные копии всех ИСПДн не реже чем раз в месяц.

4.12. Специалист, ответственный за техническое обеспечение учреждения, при помощи специализированного программного обеспечения, средств создает образы дисков всех рабочих мест ИСПДн не реже, чем раз в квартал.

4.13. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов либо полного

восстановления системы с образа диска.

4.14. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

4.15. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.

4.16. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных.

4.17. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств на зарегистрированный носитель.

4.18. Ответственность за проведение резервного копирования ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора ИСПДн.

4.19. Ответственность за проведение резервного копирования сетевого каталога хранения резервных копий ИСПДн возлагается на специалистов, ответственных за техническое обеспечение учреждения.

4.20. Мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных организуются и проводятся специалистами, ответственных за техническое обеспечение учреждения, привлечением ответственного пользователя той ИСПДн, функционирование которой было нарушено.

5. 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.

5.1. 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.

5.2. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в Колледже;
- учета 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.

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

5.4. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных (далее – ОБ ПДн) мерам, предписанным законодательством РФ и установленным нормативными документами предприятия;
- 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 проведения организационных и технических мероприятий по защите информации;
- устранение ранее выявленных недостатков.

5.5. 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.

5.6. 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 информационной 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.

5.7. 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 обеспечение безопасности персональных данных при их обработке в ИСПДн проводится расследование.

Для проведения расследования назначается комиссия с привлечением администратора информационной 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.

5.8. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов организации проводятся, как правило, силами администратора информационной безопасности и (или) ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн, в соответствии с утвержденным планом или по согласованию с руководителем.

5.9. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора информационной безопасности, ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн информации, администратор ИСПДн. Для обследования ИСПДн может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

5.10. Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в «Аттестате соответствия» (если

проводилась аттестация) и (или) требованиям по безопасности персональных данных.

5.11. 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.

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

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

6.2. Пользователи должны продемонстрировать администратору информационной безопасности наличие необходимых знаний и умений для выполнения требований настоящего Положения. Администратор информационной безопасности должен вести журнал учета пользователей, допущенных к информационным системам персональных данных.

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

6.4. Ответственным за организацию обучения и оказание методической помощи в Колледже является администратор информационной безопасности.

6.5. 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.

6.6. К работе в ИСПДн допускаются только сотрудники, прошедшие первичный инструктаж по обеспечению безопасности в ИСПДн и показавшие твердые теоретические знания и практические навыки, о чём делается соответствующая запись в Журнале учёта допуска к работе в ИСПДн.

6.7. Администратор информационной безопасности должен 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.

7. Порядок проверки электронного журнала обращений к ИСПДн.

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

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

7.3. Право проверки электронного журнала обращений имеют:

- администратор информационной безопасности;
- ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн;
- директор.

7.4. На технических средствах ИСПДн, на которых установлены специализированные средства защиты информации (далее – СЗИ) типа «Страж», «Secret Net», DallasLock и другие, проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

7.5. Если в ходе периодических, плановых или внеплановых проверок ИСПДн выявлены случаи несанкционированного доступа (далее-НСД) к информации конфиденциального характера, то вступает в силу п.п. 3.7., 3.8. данного Положения.

7.6. Проверке подлежат все электронные журналы ИСПДн.

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

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

8. Правила антивирусной защиты.

8.1. На каждом компьютере ИСПДн должны быть установлены лицензионные антивирусные средства, сертифицированные ФСТЭК РФ.

8.2. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется специалистами, ответственными за техническое обеспечение информационных систем учреждения.

8.3. Специалисты, ответственные за техническое обеспечение информационных систем учреждения, осуществляют периодическое обновление антивирусных пакетов и контроль их работоспособности.

8.4. Установку и удаление средств антивирусной защиты также может осуществлять администратор информационной безопасности.

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

8.6. 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 съемный носитель).

Настройку средств антивирусной защиты выполняет администратор информационной безопасности, либо специалисты, ответственные за техническое обеспечение учреждения, по согласованию администратором информационной безопасности.

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

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

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

8.10. 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 информационной 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 информационной 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.

8.11. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора информационной безопасности.

8.12. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на специалистов по техническому обеспечению,

администратора информационной безопасности и всех пользователей данной ИСПДн.

9. Правила парольной защиты.

9.1. 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.

9.2. 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 информационной безопасности.

9.3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями объекта вычислительной техники 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.

9.4. Администратор ИСПДн передает свои аутентификационные данные для запуска прикладного ПО БД ИСПДн на бумажном носителе в опечатанном конверте администратору информационной безопасности, который в свою очередь хранит их в закрывающемся на ключ хранилище.

9.5. В случае имеющейся служебной необходимости, продиктованной возникновением нештатных ситуаций или других форс-мажорных факторов, при условии отсутствия на рабочем месте пользователя ИСПДн, руководитель подразделения оформляет в письменном виде заявку на сброс пароля отсутствующего пользователя и направляет ее ответственному за обеспечение безопасности персональных данных при их обработке в ИСПДн. В заявке должно быть изложено обоснование необходимости сброса пароля, указаны Ф.И.О. пользователя, чей пароль необходимо сбросить, Ф.И.О., должность специалиста, который будет осуществлять обработку ПДн от имени отсутствующего пользователя, а так же временной отрезок, в течение которого им будет производиться обработка ПДн.

9.6. В случае, если основания, указанные в заявке, являются достаточными для сброса пароля, ответственный за защиту информации поручает администратору информационной безопасности сбросить,

установленный в СЗИ от НСД, личный пароль указанного в заявке пользователя.

9.7. В случае, если прикладное ПО БД ИСПДн обладает системой аутентификации, пароль для запуска прикладного ПО сбрасывает администратор ИСПДн, либо ответственный пользователь, по той же заявке, в случае их отсутствия пароль имеет право сбросить администратор информационной безопасности, воспользовавшись для входа в систему управления аутентификационными данными администратора ИСПДн.

9.8. После выполнения необходимых работ все пароли изменяются и на бумажных носителях в опечатанных конверте, передаются пользователям ИСПДн. После этого пользователи устанавливают себе новые пароли.

9.9. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 60 дней.

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

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

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

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

10. Правила обновления и конфигурирования программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн.

10.1. Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления и конфигурирования программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн.

10.2. Все изменения программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн, должны производиться администратором информационной безопасности и/или лицами ответственными за техническое обеспечение учреждения (при согласовании с администратором информационной безопасности), на основании заявки администратора ИСПДн, направляемой ответственному за обработку персональных данных.

10.3. Обновление и конфигурация программного обеспечения, не используемого для непосредственной обработки ПДн и не являющегося ПО

СЗИ, а также аппаратной составляющей элементов ИСПДн, осуществляется сотрудниками отдела технического обеспечения учреждения в обычном порядке.

10.4. В случае если АРМ проходил аттестацию соответствия требованиям защиты информации, изменение аппаратно – программной составляющей ИСПДн также производится основании заявки.

10.5. Изменение конфигурации программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных сотрудников *запрещено*.

10.6. Процедура внесения изменений в конфигурацию программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн, инициируется заявкой администратора ИСПДн.

10.7. 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).

10.8. Заявку администратора ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает руководитель, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений, после чего заявка передается администратору информационной безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера указанного в заявке самостоятельно или с привлечением сотрудников, ответственных за техническое обеспечение учреждения.

10.9. 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 информационной безопасности по согласованию с органом по аттестации (в случае, если проводилась аттестация), проводившим аттестацию данной ИСПДн. Работы производятся в присутствии администратора ИСПДн.

10.10. Установка или обновление подсистем ИСПДн должны проводиться в соответствии с технологией проведения модификаций программных комплексов данных подсистем, указанной в технической документации, если таковая имеется.

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

10.12. ПО средств защиты информации устанавливается с носителей, обладающих специальной голографической наклейкой, подтверждающей их подлинность, если иное не указано в документации к данному ПО.

10.13. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также на совместимость с установленным программным обеспечением и операционной системой.

10.14. После установки (обновления) ПО, администратор информационной безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера, проверить работоспособность ПО и правильность их настройки и произвести соответствующую запись в «Журнале учета нештатных ситуаций в ИСПДн, выполнения профилактических работ, установки, модификации программных средств на компьютерах ИСПДн», делает отметку о выполнении (на обратной стороне заявки) и в «Техническом паспорте».

10.15. Формат записей «Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» устанавливается приказом руководителя Организации.

10.16. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за обеспечение безопасности персональных данных при их обработке в ИСПДн, который в свою очередь связывается с сотрудниками органа по аттестации (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкций. При этом администратор информационной 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 обеспечение безопасности персональных данных при их обработке в ИСПДн.

10.17. Копии заявок могут храниться у администратора информационной 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

10.18. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора информационной безопасности и администратора ИСПДн.

11. Управление учетными записями пользователей.

11.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должна быть создана уникальная учетная запись пользователя.

11.2. Работу в ИСПДн сотрудник должен осуществлять только с использованием своего уникального имени пользователя. Работа в ИСПДн под чужой учетной записью, кроме случаев, описанных в п.9.5, *запрещена*.

11.3. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой администратора ИСПДн по прилагаемой форме к настоящему Положению.

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).

11.4. 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 информационной безопасности на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.

11.5. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор информационной 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 60 дней.

11.6. После внесения изменений в списки пользователей администратор информационной 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 информационной безопасности.

11.7. Исполненные заявка и задание хранятся у администратора информационной безопасности.

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.

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

12.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее - СЗИ).

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

12.3. 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 информационной безопасности.

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

- руководитель;
- ответственный за обработку персональных данных;
- администратор информационной безопасности.

12.5. Пользователю ИСПДн категорически запрещается:

- отключать СЗИ;
- производить обработку конфиденциальной информации в случае неработоспособности средств ее защиты (СЗИ);
- менять настройки СЗИ.

12.6. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлено нарушение требования п. 10.5. то подлежат применению п.п. 3.7., 3.8. данного Положения.

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

13. Порядок охраны и допуска посторонних лиц в защищаемые помещения.

13.1. Данный раздел Положения устанавливает порядок охраны помещений ИСПДн.

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

Список сотрудников, имеющих право вскрывать и закрывать помещения утверждается руководителем и передаётся на пост охраны.

13.3. При отсутствии сотрудников, ответственных за вскрытие помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа. Комиссией составляется акт вскрытия.

13.4. При закрытии помещений сотрудники, ответственные за помещения, проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы, на которых содержится конфиденциальная информация, убирают для хранения в опечатываемый сейф (металлический шкаф).

13.5. Ключ от помещения сдаётся на пост охраны.

13.6. Сотрудник, имеющий право на вскрытие помещений:

- производит проверку исправности замка;
- вскрывает помещение.

13.7. При обнаружении нарушений целостности замков или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается директору и (или) ответственному за обеспечение безопасности персональных данных при их обработке в ИСПДн.

Одновременно принимаются меры по охране места происшествия и до прибытия должностных лиц в помещение никто не допускается.

13.8. Директор, лицо, ответственное за обеспечение безопасности персональных данных при их обработке в ИСПДн, администратор информационной безопасности организуют проверку ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации.

14. Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации.

14.1. В обязательном порядке уничтожению подлежат поврежденные, 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.

14.2. 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).

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

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

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

14.6. Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: администратор ИСПДн, ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн, администратор информационной безопасности.