ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ВЛАДИМИРКОЙ ОБЛАСТИ
«ВЛАДИМИРСКИЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ имени Л.И.НОВИКОВОЙ»

УТВЕРЖДЕНО
Ректор института _____ В.В. Андреева
Приказ от 29.05.2014 г. №035-С

ПОЛОЖЕНИЕ
ОБ ОРГАНИЗАЦИИ И ОБЕСПЕЧЕНИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ в ГАОУ ДПО ВО ВИРО

Принято на заседании Учёного совета
Протокол от 29.05.2014 № 30

Владимир
2014

1. Общие положения

1.1. Данное «Положение об организации и обеспечении защиты персональных данных в ГАОУ ДПО ВО ВИРО» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", другими нормативно-правовыми актами РФ, в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2. Положение определяет порядок работы персонала ИСПДн 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 защищаемые помещения.

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

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 ректором государственного автономного образовательного учреждения дополнительного профессионального образования Владимирской области “Владимирский институт развития образования имени Л.И. Новиковой” (далее руководитель), и в соответствии со списком должностей допущенных к обработке ПДн в ИСПДн. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн руководителем назначается администратор безопасности.

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 регламенте разграничения прав доступа, утверждаемым руководителем организации. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в Журнале учета машинных носителей персональных данных.

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 персональных данных.

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.

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

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

3.2. К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные в журнале учета носители.

3.3. Администратор безопасности обязан осуществлять периодическое резервное копирование конфиденциальной информации.

3.4. Еженедельно, по окончанию работы с документами, содержащими персональные данные на компьютере, пользователь, при отсутствии администратора, обязан создавать резервную копию документов, содержащих персональные данные на зарегистрированный носитель (ЖМД, ГМД, CD, DVD – диски, USB накопитель, другие), создавая тем самым резервный электронный архив документов, содержащих персональные данные.

3.5. Носители информации (ЖМД, ГМД, CD-ROM, USB накопитель, другие), предназначенные для создания резервной копии и хранения конфиденциальной информации выдаются установленным порядком руководителем, администратором безопасности. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение администратору безопасности, или руководителю.

3.6. Перед резервным копированием пользователь или администратор безопасности обязан проверить электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель) на отсутствие вирусов.

3.7. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль в соответствии с п. 7 настоящего Положения.

3.8. Запрещается запись посторонней информации на электронные носители (ЖМД, ГМД, CD-ROM, USB накопитель и другие) резервной копии.

3.9. Порядок создания резервной копии:

- вставить в компьютер зарегистрированный электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель, другие) для резервного копирования;
- выбрать необходимый каталог (файл) для создания резервного архива;
- при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;
- выполнить процедуру создания резервной копии;
- произвести копирование на отчуждаемый носитель;
- произвести отключение отчуждаемого носителя и, создав необходимые записи в журналах убрать носитель в хранилище.

3.10. Хранение отчуждаемого носителя с резервной копией файлов, содержащих персональные данные должно осуществляться в хранилище, исключающем несанкционированный доступ к носителю (запираемые шкафы, сейфы).

3.11. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

3.12. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в хранилище, исключающем несанкционированный доступ к дистрибутиву (запираемые шкафы, сейфы).

3.13. При необходимости ремонта технических средств, с них удаляются опечатывающие пломбы и по согласованию с администратором безопасности, при условии проведенной аттестации информационной системы, представителем организации, проводившей аттестацию, оборудование передается в сервисный центр производителя.

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

3.15. 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. Настройку данных средств должен выполнять сотрудник организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

3.16. 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, с помощью встроенных в них функций на зарегистрированный носитель.

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

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

3.19. Ответственность за проведение мероприятий по восстановлению средств защиты информации (далее – СЗИ) возлагается на 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 подразделениях государственного автономного образовательного учреждения дополнительного профессионального образования (повышения квалификации) Владимирской области “Владимирский институт повышения квалификации работников образования имени Л.И. Новиковой” (далее - Организация), учета требований по защите информации в разрабатываемых плановых и распорядительных документах;
- 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 в ИСПДн;
- 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;

4.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн Организации 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 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 проводятся 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.

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 администратора безопасности 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 путем проведения периодических, плановых и внеплановых проверок объектов защиты. Периодические, плановые и внеплановые проверки объектов организации проводятся силами администратора безопасности, 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 организацию обработки персональных данных и специалистов Организации. 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" (если проводилась аттестация) 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;
- помещения, 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. Государственный контроль состояния защиты информации осуществляется Федеральной службы по техническому и экспортному контролю РФ и Федеральной службой безопасности РФ, в рамках их полномочий и 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.

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, инструкцией пользователя информационных систем персональных данных, настоящим Положением, под роспись.

5.2. Пользователи должны продемонстрировать администратору безопасности наличие необходимых знаний и умений для выполнения требований настоящего Положения.

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 Организации является администратор безопасности и ответственный за организацию обработки персональных данных.

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

5.6. К работе в ИСПДн допускаются только сотрудники прошедшие первичный инструктаж ОБ в ИСПДн и показавшие твердые теоретические знания, и практические навыки. Допуск к работе в ИСПДн оформляется приказом руководителя организации.

5.7. Администратору безопасности, желательно 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. Функции проверки электронного журнала обращений возлагается на администратора безопасности.

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. Проверке подлежат все электронные журналы ИСПДн.

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

7. Правила антивирусной защиты

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

7.2. К использованию на компьютерах допускаются только сертифицированные антивирусные средства, закупленные у разработчиков (поставщиков) указанных средств.

7.3. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности, либо специалистами организаций-лицензиатов ФСТЭК России и ФСБ России.

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 съемный носитель).

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

7.7. 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.

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 администратора безопасности.

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 ИСПДн 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 передавать на хранение администратору безопасности. Запечатанные конверты с паролями исполнителей должны храниться в защищённом хранилище у администратора безопасности.

8.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 90 дней.

8.6. 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 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 предприятия и другие обстоятельства) администратора безопасности.

8.8. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по смене пароля пользователя и проверке электронного журнала обращений к ИСПДн.

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 мотивированных запросов в письменной форме от пользователей ИСПДн.

9.3. В запросе 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).

9.4. Также в запросе указывается наименование ИСПДн, согласно акту классификации ИСПДн. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанного компьютера.

9.5. Запрос пользователя, в котором требуется произвести изменения конфигурации, рассматривает руководитель, визирует его, утверждая тем самым необходимость проведения указанных в запросе изменений.

После чего запрос передается администратору безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера указанного в запросе.

9.6. Право внесения изменений в конфигурацию аппаратно-программных средств защищенных ИСПДн в отношении системных и прикладных программных средств, аппаратных средств, а также в отношении программно-аппаратных средств защиты предоставляется администратору безопасности по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн;

9.7. Изменение конфигурации аппаратно-программных средств ИСПДн без согласования с администратора безопасности запрещено.

9.8. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн, тестирование 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 по согласованию с органом по аттестации (в случае, если проводилась аттестация), проводившим аттестацию данной ИСПДн.

9.9. Установка и обновление ПО (системного, тестового и т.п.) на компьютерах, входящих в состав ИСПДн, 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.

9.10. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность.

9.11. После установки (обновления) ПО, администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки, делает отметку о выполнении (на обратной стороне запроса).

9.12. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом администратору безопасности, который в свою очередь связывается с сотрудниками органа по аттестации (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкции. 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 у администратора безопасности.

9.13. 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.

9.14. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом уничтожения персональных данных по установленной форме.

10. Правила регистрации нового пользователя ИСПДн, а так же изменения прав доступа к подсистемам ИСПДн

10.1. 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 запись пользователя), под которым он будет регистрироваться и работать на данном компьютере.

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

10.3. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется запросом пользователя.

В запросе 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).

10.4. Запрос рассматривает ответственный за организацию обработки персональных данных, визируя его, утверждая тем самым необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в запросе задач ресурсам ИСПДн. Затем запрос передается администратору безопасности.

10.5. В случае, если необходимость допуска сотрудника к ИСПДн устанавливается впервые, то допуск к ИСПДн оформляется приказом руководителя Организации.

10.6. На основании запроса, 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 запросе.

10.7. 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 запросе делается отметка о выполнении задания за подписью исполнителя – администратора безопасности.

10.8. 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).

10.9. Исполненные запросы (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

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 персональные данные, так и администратором безопасности ИСПДн.

11.4. Обязанность проверки соблюдения условий использования средств защиты информации возлагается на администратора безопасности.

11.5. Пользователю ИСПДн категорически запрещается:

- обрабатывать персональные данные 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, без согласования с этой организацией.

12. Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации

12.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие персональные данные, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие персональные данные, 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.

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

12.3. 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.

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

12.5. По факту уничтожения или стирания носителей составляется акт, согласно установленной форме.

13. Заключительные положения

13.1. Требования настоящего Положения обязательны для всех сотрудников обрабатывающих персональные данные в ИСПДн.

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