Министерство общего и профессионального образования
Свердловской области

Государственное бюджетное профессиональное образовательное учреждение
Свердловской области «Красноуфимский аграрный колледж»

УТВЕРЖДЕНО
Приказом ГБПОУ СО «КАК»
От «14» февраля 2017 г.
№ 01-11/44

Положение об организации и проведении работ в ГБПОУ СО «Красноуфимский аграрный колледж» по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных

1. Общие положения

1.1. Положение об организации и проведению работ в ГБПОУ СО «Красноуфимский аграрный колледж» по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных (далее – Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и иных нормативных актов в сфере защиты информации 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.

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

2.1. Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании приказа, который издается директором ГБПОУ СО «Красноуфимский аграрный колледж» (далее - директор), и в соответствии со списком лиц, допущенных к работе 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, утверждаемой директором. 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 к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

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

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

хранить в тайне свой пароль (пароли);

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

выполнять требования положений по организации антивирусной защиты в полном объеме.

2.8. Немедленно известить ответственного за защиту информации 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, 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.

2.10. 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 них существовала возможность визуального считывания информации.

2.11. В целях обеспечения безопасности персональных данных пользователи должны соблюдать следующую инструкцию при работе с персональными данными:

2.11.1. Обеспечение безопасности перед началом обработки персональных данных: перед началом обработки персональных данных необходимо убедиться в том, что:

- в помещении, в котором ведется работа с персональными данными, отсутствуют посторонние лица;
- носители персональных данных не повреждены;
- к персональным данным не был осуществлен несанкционированный доступ;
- технические средства автоматизированной обработки и защиты персональных данных находятся в исправном состоянии.

2.11.2. Обеспечение безопасности во время обработки персональных данных: во время обработки персональных данных необходимо обеспечить:

- недопущения воздействия на технические средства автоматизированной обработки персональных данных, способного нарушить их функционирование;
- недопущение нахождения в помещении, в котором ведется работа с персональными данными, посторонних лиц;
- постоянный контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- недопущение несанкционированного доступа к персональным данным;
- конфиденциальность персональных данных.

2.11.3. Обеспечение безопасности в экстремальных ситуациях:

1) при модификации или уничтожения персональных данных, вследствие несанкционированного доступа к ним необходимо обеспечить возможность их незамедлительного восстановления.

2) при нарушении порядка предоставления персональных данных пользователям информационной системы необходимо приостановить их предоставление до выявления и устранения причин нарушений.

3) при обнаружении несанкционированного доступа к персональным данным необходимо немедленно прервать этот доступ.

4) в случае несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных необходимо произвести разбирательство и составление заключений по данным фактам, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

5) обо всех экстремальных ситуациях необходимо немедленно поставить в известность директора образовательного учреждения.

2.11.4. Обеспечение безопасности при завершении обработки персональных данных: после завершения сеанса обработки персональных данных необходимо обеспечить:

- исключение возможности несанкционированного проникновения или нахождения в помещении, в котором размещены информационные системы и ведется работа с персональными данными;
- работоспособность средств защиты информации, функционирующих при отсутствии лиц, допущенных к обработке персональных данных.

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

3.1. К использованию, для создания резервной копии в ИСПДн, допускаются носители, только зарегистрированные в «Журнале учета машинных носителей».

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

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

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

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

3.6. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль.

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

3.8. 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 не обходимые записи в журналах убрать носитель в хранилище.

3.9. Хранение отчуждаемого носителя с резервной копией защищаемой информации осуществляется в специальном металлическом хранилище совместно с ключевой и аутентифицирующей информацией.

3.10. 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 специальном хранилище.

3.12. При необходимости ремонта технических средств, с них удаляются опечатывающие пломбы и по согласованию с администратором безопасности, ответственным за защиту информации и, при условии проведенной аттестации информационной системы, представителем организации, проводившей аттестацию, оборудование передается в сервисный центр производителя. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению. Работа с использованием неисправных технических средств запрещается.

3.13. 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.

3.14. 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.

3.15. 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.

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

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

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

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения кроме настоящего раздела регулируется «Инструкцией о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных…» (приложение 1.8 к настоящему Положению).

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 ГБПОУ СО «Красноуфимский аграрный колледж», 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.

4.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн ГБПОУ СО «Красноуфимский аграрный колледж» 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 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 либо в соответствующих журналах учета результатов контроля.

4.7. Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее - предпосылка).

4.8. По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию руководителя или ответственного за защиту информации проводится расследование

4.9. 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.

4.10. 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 безопасности и(или) ответственного за защиту информации, в соответствии с утвержденным планом или по согласованию с руководителем.

4.11. 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.

4.12. 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.

4.13. 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.

4.14. 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.

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.

5.2. Пользователи должны продемонстрировать администратору безопасности и(или) ответственному за защиту информации 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 ГБПОУ СО «Красноуфимский аграрный колледж» 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.

6. Порядок проверки электронного журнала обращений к ИСПДн

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

6.2. Право проверки электронного журнала обращений имеют: администратор безопасности; ответственный за защиту информации; директор.

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

6.4. Проверке подлежат все электронные журналы ИСПДн.

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

6.6. Факты проверок электронных журналов отражаются в специальном «Журнале учета проверок электронных журналов». После каждой проверки Администратор безопасности делает соответствующую отметку в журнале и ставит свою роспись.

7. Правила организации антивирусной защиты

7.1. На рабочих местах ИСПДн может использоваться программное и аппаратное обеспечение, необходимое только для выполнения служебной деятельности.

К использованию в ИСПДн допускаются только лицензионные антивирусные средства, имеющие соответствующий сертификат ФСТЭК по защите персональных данных.

7.2. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности в соответствии с инструкцией по установке и эксплуатации производителя соответствующего средства антивирусного контроля.

7.3. Регулярное обновление антивирусных программ осуществляется автоматически и контролируется администратором безопасности. В случае получения пользователем на рабочем месте сообщения о невозможности (сбое) автоматического обновления, необходимо оповестить об этом администратора безопасности.

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

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

Полная антивирусная проверка компьютера должна включать проверку всех жестких дисков, всех сменных дисков и устройств, почтовых ящиков, резервного хранилища системы. Она должна проводиться регулярно, не реже одного раза в месяц и может регламентироваться и контролироваться сервером администрирования антивирусной защиты ИСПДн.

7.6. Обязательному постоянному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, запоминающих устройств USB, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо «чистой» (не зараженной вирусами) и защищенной от записи системной дискеты, - на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

7.7. 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.

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

7.9. Установка (изменение) системного и прикладного ПО осуществляется на основании инструкции по установке и эксплуатации ПО и аппаратных средств ИСПДн данного производителя. 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.

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

7.11. 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.

7.12. 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 (при необходимости для выполнения данных требований привлечь администратора);

по факту обнаружения зараженных вирусом файлов составить служебную записку администратору безопасности, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

В случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, администратор безопасности должен связаться организацией - разработчиком антивирусного ПО.

Ответственность за организацию и проведение мероприятий антивирусного контроля в ИСПДн, а также за соблюдением установленного порядка антивирусного контроля возлагается на администратора безопасности.

8. Правила организации парольной защиты

8.1. Данный раздел 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:

обеспечение конфиденциальности пароля;

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 содержать последовательных идентичных символов и состоять из полностью числовых или полностью буквенных групп;

при смене пароля новое значение должно отличаться от предыдущего, должно быть исключено повторное или цикличное использование старых паролей.

пароль не должен быть подвержен легкому угадыванию или вычислению с использованием персональной информации, связанной с владельцем пароля (имен, номеров телефонов, дат рождения, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

пользователь не имеет права сообщать личный пароль другим лицам.

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 предприятия 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 восстановлению парольной защиты

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

8.10. Должно быть исключено коллективное использование индивидуальных паролей.

8.11. Запрещается включать пароли в автоматизированный процесс регистрации (например, с использованием хранимых макрокоманд или функциональных клавиш).

8.12. Пароли никогда не следует хранить в компьютерной системе в незащищенной форме.

9. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн, внесения изменений в конфигурацию средств защиты информации

9.1. Настоящий раздел 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 конкретной ИСПДн.

9.3. Право внесения изменений в конфигурацию аппаратно-программных средств, защищенных ИСПДн предоставляется:

в отношении системных и прикладных программных средств – администратору безопасности по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн;

в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты – администратору безопасности по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн.

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, а также средств защиты информации 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);

изменение настроек средств защиты информации;

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 директор, 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 по согласованию с органом по аттестации (в случае, если проводилась аттестация), проводившим аттестацию данной ИСПДн. Работы производятся в присутствии ответственного за эксплуатацию данной ИСПДн.

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 работе информационных систем персональных данных, выполнения профилактических работ, установки и модификации программных средств на компьютерах информационных систем персональных данных», делает отметку о выполнении (на обратной стороне заявки) и в «Техническом паспорте».

9.14. Порядок оформления «Журнала учета нештатных ситуаций в работе информационных систем персональных данных, выполнения профилактических работ, установки и модификации программных средств на компьютерах информационных систем персональных данных» устанавливается в приложении 1.5. к настоящему Положению.

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, который в свою очередь связывается с сотрудниками органа по аттестации (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкциям. 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 в работе информационных систем персональных данных, выполнения профилактических работ, установки и модификации программных средств на компьютерах информационных систем персональных данных» 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.

10. Порядок учета, хранения, использования и уничтожения средств защиты информации, эксплуатационной и технической документации, в том числе криптографической.

10.1. Технические средства защиты информации являются важным компонентом организации безопасности ПДн.

10.2. Порядок работы с техническими средствами защиты информации (СЗИ) определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как сотрудниками, обрабатывающими конфиденциальную информацию, так и администратором безопасности ИСПДн.

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

директор;

ответственный за эксплуатацию СЗИ;

администратор безопасности.

10.4. Для организации и обеспечения работ по техническому обслуживанию средств защиты информации, приказом учреждения назначается ответственный за эксплуатацию. Ответственный за эксплуатацию средств защиты информации осуществляет:

- текущий контроль, обеспечение функционирования и безопасности средств защиты;

- поэкземплярный учет, эксплуатационной и технической документации к ним;

- контроль за соблюдением условий использования в соответствии с эксплуатационной и технической документацией и настоящей Инструкцией;

- расследование и составление заключений по фактам нарушения условий использования средств защиты информации, которые могут привести к снижению требуемого уровня безопасности информации;

- обучение пользователей правилам работы с средствами защиты информации;

- разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

10.5. Пользователю ИСПДн категорически запрещается обрабатывать конфиденциальную информацию с отключенными СЗИ и менять настройки СЗИ.

Пользователь средств защиты информации обязан:

- не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптографических ключах;

- соблюдать требования к обеспечению безопасности конфиденциальной информации при использовании средств защиты информации;

- сдать средства защиты информации, эксплуатационную и техническую документацию к ним, криптографические ключи ответственному за эксплуатацию СЗИ при прекращении использования средств защиты информации;

- незамедлительно уведомлять ответственного за эксплуатацию средств защиты информации о фактах утраты или недостачи СКЗИ, криптографических ключей, ключей от помещений, ключевых носителей хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

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

10.7. Все действия работы со средствами защиты информации (в т.ч. криптографическими СЗИ) осуществляются в соответствии с технической и эксплуатационной документацией на них, а также в соответствии с правилами пользования ими.

10.8. Учет и хранение СЗИ.

10.8.1. Используемые или хранимые оператором СЗИ, эксплуатационная и техническая документация к ним подлежат поэкземплярному учету в журнале поэкземплярного учета СЗИ, эксплуатационной и технической документации к ним (форма – в приложении 1.1. к настоящему Положению).

10.8.2. Учет СЗИ, эксплуатационной и технической документации к ним осуществляется ответственным за эксплуатацию СЗИ или иным уполномоченным лицом.

10.8.3. Программные средства учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СЗИ учитываются также совместно с соответствующими аппаратными средствами.

.10.8.4. Единицей поэкземплярного учета криптографических ключей, ключевых носителей, считается отчуждаемый ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптографических ключей, то его каждый раз следует регистрировать отдельно.

10.8.5. При необходимости пользователю выдается документация по эксплуатации средств защиты информации в электронном виде.

10.8.6. Дистрибутивы средств защиты информации на носителях, эксплуатационная и техническая документация к ним, инструкции хранятся у ответственного за эксплуатацию средств защиты информации. Криптографические ключи, электронно-цифровая подпись и ключевые носители хранятся у пользователей средств защиты информации. Хранение осуществляется в закрываемых на замок металлических хранилищах пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение или в опечатанном пенале (тубусе).

Металлические шкафы должны быть оборудованы внутренними замками с двумя экземплярами ключей.

10.8.7. Пользователи средств защиты информации могут осуществлять хранение рабочих и резервных криптографических ключей, ЭЦП и ключевых носителей предназначенных для применения в случае неработоспособности рабочих криптографических ключей, ЭЦП и ключевых носителей. Резервные криптографические ключи, ЭЦП и ключевые носители могут также находится на хранении у ответственного за эксплуатацию.

10.8.8. Все экземпляры СЗИ, эксплуатационная и техническая документация к ним должны выдаваться пользователям СЗИ, несущим персональную ответственность за их сохранность под роспись в соответствующем журнале.

10.8.9. Аппаратные средства, с которыми осуществляется штатное функционирование СЗИ, должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) должно быть таким, чтобы его можно было визуально контролировать.

10.8.10. Ключевые носители совместно с журналом должны храниться ответственным за эксплуатацию средств защиты информации в сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и журнал совместно с другими документами, при этом ключевые носители и журнал должны быть помещены в отдельную папку.

10.8.11. На время отсутствия ответственного за эксплуатацию средств защиты информации должен быть назначен сотрудник его замещающий.

10.8.12. При необходимости криптографические ключи, ЭЦП и ключевые носители сдаются на временное хранение ответственному за эксплуатацию.

10.9. Использование СЗИ:

10.9.1. Средства защиты информации используются для обеспечения конфиденциальности, авторства и целостности электронных документов и т.п.

10.9.2. При выявлении сбоев или отказов пользователь обязан сообщить о факте их возникновения ответственному за эксплуатацию.

10.9.3. Пользователю запрещается:

- осуществлять несанкционированное копирование средств защиты информации; использовать ключевые носители и ЭЦП для работы на других рабочих местах для шифрования и подписи электронных документов;
- разглашать содержимое средств защиты информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;
- вставлять носители криптографических ключей, ЭЦП и ключевые носители в устройства считывания в режимах, не предусмотренных штатным режимом работы средств защиты информации, а также в устройства считывания других ПЭВМ;
- записывать на носители с криптографическими ключами, ЭЦП и ключевыми носителями постороннюю информацию;
- подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные в штатной комплектации;
- работать на ПЭВМ, если во время ее начальной загрузки не проходят встроенные тесты, предусмотренные в ПЭВМ;

- вносить какие-либо изменения в программное обеспечение средств защиты информации.

10.10. Действия при компрометации криптографических ключей и ЭЦП

10.10.1. К обстоятельствам, указывающим на возможную компрометацию криптографических ключей и ЭЦП, но не ограничивающим их, относятся следующие:

- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами или ЭЦП;
- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами или ЭЦП с последующим их обнаружением;
- увольнение сотрудников, имевших доступ к рабочим и/или резервным криптографическим ключам или ЭЦП;
- возникновение подозрений относительно утечки информации или ее искажения;
- нарушение целостности печатей на сейфах (металлических шкафах) с ключевыми носителями с рабочими и/или резервными криптографическими ключами, ЭЦП, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них ключевых носителей с рабочими и/или резервными криптографическими ключами, ЭЦП;
- временный доступ посторонних лиц к ключевым носителям, а также другие события, при которых достоверно не известно, что произошло с ключевыми носителями.

10.10.2. В случае возникновения обстоятельств, указанных в п. 10.10.1 настоящего раздела, пользователь обязан незамедлительно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей, по телефону информировать администратора безопасности о факте компрометации используемых закрытых криптографических ключей, ЭЦП.

10.10.3. Решение о компрометации криптографических ключей принимает администратор безопасности на основании письменного уведомления пользователя о компрометации, с приложением, при необходимости, письменного объяснения пользователя по факту компрометации его криптографических ключей, ЭЦП.

10.10.4. Уведомление должно содержать:

- идентификационные параметры скомпрометированного криптографического ключа, ЭЦП;
- фамилию, имя, отчество пользователя средств защиты информации, который владел скомпрометированным криптографическим ключом, ЭЦП;
- сведения об обстоятельствах компрометации криптографического ключа, ЭЦП;
- время и обстоятельства выявления факта компрометации криптографического ключа, ЭЦП.

10.10.5. После принятия решения о компрометации криптографического ключа, ЭЦП принимаются меры о его изъятии из обращения в соответствии с требованиями эксплуатационной и технической документации на средства защиты информации

10.10.6. Дата, начиная с которой сертификат ключа подписи считается недействительным, устанавливается равной дате формирования списка отозванных сертификатов, в который был включен отзываемый сертификат ключа подписи.

10.10.7. Использование средства защиты информации может быть возобновлено только после ввода в действие другого криптографического ключа, ЭЦП взамен скомпрометированного.

10.11. Уничтожение криптографических ключей, ЭЦП и ключевых носителей.

10.11.1. Неиспользованные или выведенные из действия криптографические ключи, ЭЦП и ключевые носители подлежат уничтожению.

10.11.2. Уничтожение криптографических ключей, ЭЦП на ключевых носителях производится ответственным за эксплуатацию средств защиты информации.

10.11.3. Криптографические ключи, ЭЦП находящиеся на ключевых носителях, уничтожаются путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на средства защиты информации.

10.11.4. При уничтожении криптографических ключей, ЭЦП находящихся на ключевых носителях, необходимо:

- установить наличие оригинала и количество копий криптографических ключей, ЭЦП;
- проверить внешним осмотром целостность каждого ключевого носителя;
- установить наличие на оригинале и всех копиях ключевых носителей реквизитов путем сверки с записями в журнале поэкземплярного учета;
- убедиться, что криптографические ключи, ЭЦП находящиеся на ключевых носителях, действительно подлежат уничтожению;
- произвести уничтожение ключевой информации на оригинале и на всех копиях носителей.

10.11.5. В журнале поэкземплярного учета ответственным за эксплуатацию средств защиты информации производится отметка об уничтожении криптографических ключей.

10.12. Изъятие из употребления СЗИ осуществляется по решению ответственного за эксплуатацию СЗИ, при этом вносятся необходимые изменения в журнал поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним.

10.13. СЗИ считаются изъятыми из употребления, если исполнена предусмотренная эксплуатационной и технической документацией процедура удаления программного обеспечения СЗИ, и они полностью отключены от аппаратных средств.

10.14. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены или хранятся средства защиты информации.

10.14.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены средств защиты информации или хранятся криптографические ключи (далее - режимные помещения), должны

обеспечивать сохранность средств защиты информации, СКЗИ, ключевых документов.

10.14.2. При оборудовании режимных помещений должны выполняться требования к размещению, монтажу средств защиты информации, а также другого оборудования, функционирующего со средствами защиты информации.

10.14.3. Помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к средствам защиты информации. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

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

10.14.5. Режим охраны помещений, в том числе правила допуска работников и посетителей в рабочее и нерабочее время, устанавливает ответственный за эксплуатацию. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей Инструкции.

10.14.6. Двери режимных помещений должны быть постоянно закрыты и могут открываться только для санкционированного прохода работников и посетителей. Ключи от входных дверей находятся у ответственных лиц, имеющих право допуска в режимные помещения. Дубликаты ключей от входных дверей таких помещений следует хранить в специальном сейфе.

10.14.7. Для предотвращения просмотра извне помещений, где используются средства защиты информации, окна должны быть защищены или экраны мониторов должны быть повернуты в противоположную сторону от окна.

10.14.8. Помещения, в которых используются при работе криптографические ключи, ЭЦП как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания. Сотрудникам, ответственным за охрану здания, необходимо проверять периодически исправность сигнализации.

10.14.9. В обычных условиях помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями или ответственным за эксплуатацию.

10.14.10. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за эксплуатацию. Администратор информационной безопасности должен оценить возможность компрометации хранящихся

криптографических ключей и принять, при необходимости, меры к локализации последствий компрометации средств защиты информации и к их замене.

10.14.11. Размещение и монтаж средств защиты информации, а также другого оборудования, функционирующего со средствами защиты информации, в помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена средств защиты информации осуществляются в отсутствие лиц, не допущенных к работе с данными средствами защиты информации.

10.14.12. На время отсутствия пользователей указанное оборудование, при наличии такой возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с администратором информационной безопасности необходимо предусмотреть организационно-технические меры, исключающие возможность использования средств защиты информации посторонними лицами.

10.14.13. В нерабочее время помещения, в которых осуществляется функционирование средств защиты информации, должны ставиться на охрану.

11. Порядок управления учетными записями

11.1. 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.

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

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

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 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 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.

11.6. 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.

11.7. 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.

11.8. Исполненные заявка и задание хранятся у администратора безопасности.

12. Порядок учета и управления машинными носителями информации

12.1. Настоящий раздел регламентирует порядок и устанавливает основные требования к организации учета и использования машинных носителей данных, предназначенных для обработки и хранения персональных данных в ИСПДн.

12.2. Ответственность за организацию учета и использования машинных носителей данных, предназначенных для обработки и хранения персональных данных, возлагается на администратора безопасности.

12.3. Учет машинных носителей информации осуществляется в соответствии с формой учетной документации.

12.4. Все машинные носители данных, используемые при работе со средствами вычислительной техники (СВТ) для обработки и хранения персональных данных, должны обязательно регистрироваться и учитываться. Допускается автоматизированный учет машинных носителей информации.

12.5. Проверка наличия машинных носителей данных, предназначенных для обработки и хранения персональных данных, проводится в сроки, установленные настоящим порядком

12.6. Вынос съемных носителей за пределы контролируемой зоны запрещен. Периодические проверки (не реже одного раза в месяц) наличия всех учтенных носителей в пределах контролируемой зоны проводятся администратором безопасности и(или) руководителем подразделения. В случае выявления факта выноса съемного носителя за пределы контролируемой зоны инициируется служебная проверка. Факт фиксируется в журнале учета нештатных ситуаций ИСПДн.

12.7. Запрещено использование в служебных целях личных, неучтенных носителей информации.

Периодические проверки (не реже одного раза в месяц) использования личных, неучтенных носителей в пределах контролируемой зоны проводятся администратором безопасности и(или) руководителем подразделения. В случае выявления факта использования личных, неучтенных носителей в пределах контролируемой зоны инициируется служебная проверка. Факт фиксируется в журнале учета нештатных ситуаций ИСПДн, носитель изымается по акту для проведения процедуры принудительного стирания информации, после которой возвращается владельцу полностью отформатированным.

12.8. Учет машинных носителей информации:

12.8.1. К машинным носителям информации относятся:

магнитные ленты в кассетах;

съемные носителя информации всех видов и способов подключения;

несъемные жесткие магнитные диски.

12.8.2. Каждый машинный носитель данных, применяемый при обработке персональных данных в ИСПДн, должен иметь гриф – «конфиденциально».

12.8.3. Персональную ответственность за сохранность полученных машинных носителей данных и предотвращении несанкционированного доступа к записанной на них информации несет сотрудник, получивший эти носители.

12.8.4. Учет машинных носителей данных, предназначенных для записи персональных данных производится в «Журнале учета машинных носителей».

12.8.5. Каждому носителю информации присваивается учетный номер.

12.8.6. Учетный номер и гриф «конфиденциально» наносятся на носитель информации или его корпус. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель. В этом случае учетный номер записывается также на носитель машинным способом.

12.8.7. Хранение их должно осуществляться в условиях, исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации. Хранение съемных машинных носителей должно осуществляться в сейфах (металлических шкафах). В случае, если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном виде с использованием СКЗИ, допускается хранение таких носителей вне сейфов (металлических шкафов). Несъемные носители хранятся на рабочих местах в помещениях, в которых должен быть организован режим обеспечения безопасности в соответствии с утвержденной инструкцией.

12.8.8. Машинные носители данных после стирания с них персональных данных, с учета не снимаются, а хранятся наравне с другими машинными носителями.

12.8.9. В последующем эти носители используются для записи персональных данных. Если носители не пригодны для дальнейшего использования, они подлежат уничтожению по соответствующему акту.

12.8.10. О фактах утраты машинных носителей с грифом «конфиденциально» незамедлительно докладывается руководству и администратору безопасности, проводится служебное расследование.

12.8.11. Машинные носители данных должны пересылаться, по возможности, в металлических коробках, помещаемых в пакет, в упаковках, конвертах тем же порядком, что и конфиденциальные документы. На пакетах,

упаковках, конвертах с носителями делается надпись: «Осторожно, машинные носители информации. Не прошивать».

12.8.12. Машинные носители данных выдаются операторам или другим лицам, участвующим в обработке информации, для работы под расписку в Журнале учета машинных носителей информации. По завершению работы машинные носители данных сдаются ответственному руководителю подразделения за их хранение.

12.8.13. Копирование информации, содержащей персональные данные, с машинных носителей производится с разрешения руководства ГБПОУ СО «Красноуфимский аграрный колледж» по заявке работника.

12.8.14. Машинные носители с персональными данными, утратившими практическое значение или пришедшие в негодность, уничтожаются по соответствующему акту.

12.8.15. При подготовке документов должны соблюдаться следующие особенности учета, хранения и уничтожения машинных носителей данных.

12.8.16. Машинные носители данных, предназначенные для записи персональных данных, выдаются сотрудникам по разрешению руководства ГБПОУ СО «Красноуфимский аграрный колледж» в необходимом для работы количестве под расписку в Журнале учета машинных носителей информации.

12.8.17. Несъемные жесткие магнитные диски закрепляются за сотрудником, ответственным за СВТ, в котором они установлены.

12.8.18. В случае повреждения машинных носителей данных, содержащих персональные данные, сотрудник, в пользовании которого они находятся, обязан сообщить о случившемся администратору безопасности.

12.8.19. В случае необходимости (командировка, отпуск и т. д.) машинные носители с персональными данными, сдаются сотрудником ответственному лицу на постоянное или временное хранение в опечатанном виде. При этом на упаковке указывается срок их хранения, заверенный личной подписью сотрудника. По истечению указанного срока информация может быть уничтожена, а носители могут повторно использоваться.

12.8.20. Копирование персональных данных, с машинных носителей с целью передачи другим сотрудникам производится с разрешения руководителя соответствующего подразделения.

12.8.21. Копирование осуществляется только на тех СВТ, на которых разрешена обработка персональных данных, и только на те носители, которые соответствуют грифу «конфиденциально».

12.8.22. Передача скопированной информации третьим лицам производится по письменному разрешению руководства ГБПОУ СО «Красноуфимский аграрный колледж».

12.8.23. Хранящиеся на магнитных носителях и потерявшие актуальность персональные данные должны своевременно стираться (уничтожаться). Ответственность за это несет владелец информации.

12.9. Порядок уничтожения машинных носителей, содержащих персональные данные:

12.9.1. 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.

12.9.2. 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).

12.9.3. 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.

12.9.4. Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожают путем сжигания.

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

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

13. Порядок учета лиц, имеющих доступ к персональным данным обрабатываемым в информационных системах персональных данных

13.1. Нормы настоящего раздела определяют порядок учета лиц, допущенных к работе с персональными данными в информационных системах, а также ведение «Журнала учета лиц, допущенных к работе с персональными данными в информационных системах».

13.2. Основанием для допуска сотрудника к работе в информационной системе персональных данных (далее – ИСПДн) и со средствами криптографической защиты информации является включение его в список лиц, имеющих доступ к персональным данным, обрабатываемым в информационных системах.

13.3. Включение в список лиц, имеющих доступ к персональным данным, обрабатываемым в информационных системах, осуществляется путем составления соответствующего приказа.

13.4. При допуске к работе с персональными данными (далее - ПДн) определяется перечень информационных систем персональных данных, к работе в которых допущен специалист.

13.5. Прекращение допуска к работе с персональными данными в ИСПДн оформляется в случае увольнения, перевода, отмены обязанностей по работе в данной ИСПДн и др. сотрудника и оформляется приказом директора о внесении изменений в список лиц, допущенных к работе с персональными данными в ИСПДн.

13.6. Согласно приказу о допуске к работе с персональными данными в ИСПДн администратором безопасности ведется «Журнал учета лиц, допущенных к работе в информационных системах персональных данных» (далее – Журнал) в соответствии с типовой формой журнала, указанной в приложении 1.6. к настоящему Положению.

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.

Приложение 1.1 к положению

Типовая форма журнала поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним

№ п/п	Наименование средства защиты информации, эксплуатационной и технической документации и к ним, ключевых документов	Регистрационные номера СЗИ, эксплуатационной и технической документации к ним	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СЗИ			Отметка об изъятии СЗИ из аппаратных средств			Примечание
			От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя	Дата и расписка в получении	Ф.И.О. пользователя, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СЗИ	Дата изъятия (уничто - жения)	Ф.И.О. пользователя СЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1													

Приложение 1.2 к положению

Типовая форма журнала учета машинных носителей

№п.п. п/п	Регистрационный номер	Вид носителя	Тип/емкость носителя	Место установки (хранения, использования)	Ответственное лицо, использующее носитель	Расписка лица, получившего носитель (подпись и дата)	Отметка о возврате носителя (должность кому возвращен носитель, его подпись и дата)	Отметка об уничтожении (стирании) информации	Отметка об уничтожении носителя
1	2	3	4	5	6	7	8	9	10

Приложение 1.3. к положению

Типовая форма журнала учета хранилищ

п/п	Регистрационный (учетный) номер хранилища (ключа)	Вид хранилища (ключа)	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата	Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатации	Примечание
	2	3	4	5	6	7	8

Приложение 1.4. к положению

Типовая форма журнала периодического тестирования средств защиты информации

№ п/п	Наименование средства защиты информации от НСД или криптосредства	Регистрационные номера СЗИ от НСД или криптосредства	Дата тестирования	Фамилия и подпись ответственного пользователя, проводившего тестирование	Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/неуспешный), комментарий	Дата очередного тестирования
1	2	3	4	5	6	7	8

Приложение 1.5 к положению

Типовая форма журнала учета нештатных ситуаций в работе информационных систем персональных данных, выполнения профилактических работ, установки и модификации программных средств на компьютерах информационных систем персональных данных

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО исполнителей и их подписи	ФИО ответственного за эксплуатацию ПЭВМ, подпись	Подпись администратора информационной безопасности	Примечание (ссылка на заявку)
1	2	3	4	5	6	7

Приложение 1.6. к положению

Типовая форма журнала учета лиц,

допущенных к работе в информационных системах персональных данных

№	Фамилия, имя, отчество пользователя ИСПДн	Сведения о допуске к работе с персональными данными в ИСПДн				Сведения о прекращении допуска к персональным данным, обрабатываемым в ИСПДн	
		Наименование ИСПДн	Дата и № приказа о доступе к ИСПДн	Дата и подпись допущенного лица об ознакомлении с Положением об организации и проведении работ в ГБПОУ СО «КАК» по обеспечению безопасности ПДн при их автоматизированной обработке в ИСПДн	Подпись администратора безопасности о готовности пользователя к работе в ИСПДн	Дата и номер документа о прекращении доступа (основание прекращение доступа)	Дата и подпись лица об ознакомлении с документом, прекращающим доступ к работе в ИСПДн
1	2	3	4	5	6	7	8

Приложение 1.7. к положению

Типовая форма журнала учета проверок электронных журналов

п/п	Дата проверки	Наименование ИСПДн, компьютера, технического средства	Наименование проверяемого журнал	Выявленные нарушения требований безопасности, нештатные ситуации	Подпись администратора информационной безопасности	Примечание
	2	3	4	5	6	7

Приложение 1.8 к Положению

ИНСТРУКЦИЯ О ПОРЯДКЕ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ РАБОТОСПОСОБНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Инструкция устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в базах данных ГБПОУ СО «Красноуфимский аграрный колледж» (далее – Колледж), а также к резервированию аппаратных средств.

Настоящая Инструкция разработана с целью:

определения категории информации, подлежащей обязательному резервному копированию;

определения процедуры резервирования данных для последующего восстановления работоспособности информационных систем при полной или частичной потере информации, вызванной сбоями или отказами аппаратного, или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

определения порядка восстановления информации в случае возникновения такой необходимости;

упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.

Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности информационных систем персональных данных (ИСПДн) в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

Резервному копированию подлежит информация следующих основных категорий:

персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений) на файловых серверах;

информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн, в т.ч. систем управления базами данных (СУБД) общего пользования и справочно-информационные системы общего использования;

рабочие копии установочных компонентов программного обеспечения общего назначения и специализированного программного обеспечения ИСПДн, СУБД, серверов и рабочих станций;

информация, необходимая для восстановления серверов и систем управления базами данных ИСПДн, локальной вычислительной сети, системы электронного документооборота;

регистрационная информация системы информационной безопасности ИСПДн;

другая информация ИСПДн, по мнению пользователей и администратора безопасности, являющаяся критичной для работоспособности ИСПДн.

Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений.

Резервные копии хранятся вне пределов серверного помещения, доступ к резервным копиям ограничен.

2. ОБЩИЕ ТРЕБОВАНИЯ К РЕЗЕРВНОМУ КОПИРОВАНИЮ

Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования, программный и аппаратный состав которых обеспечивает выполнение требования к резервному копированию.

Система резервного копирования обеспечивает производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью.

Требования к техническому обеспечению систем резервного копирования:

это комплекс взаимосвязанных технических средств, обеспечивающих процессы сбора, передачи, обработки и хранения информации, основывающийся на единой технологической платформе;

имеет возможность расширения (замены) состава технических средств, входящих в комплекс, для улучшения их эксплуатационно-технических характеристик по мере возрастания объемов обрабатываемой информации;

средства вычислительной техники отвечают действующим на момент сертификации российским и международным стандартам и рекомендациям.

Требования к программному обеспечению систем резервного копирования:

лицензионное системное программное обеспечение и программное обеспечение резервного копирования;

программное обеспечение резервного копирования обеспечивает простоту процесса инсталляции, конфигурирования и сопровождения.

Сопровождение системы резервного копирования возлагается программиста колледжа, который обязан следить за работоспособностью программных и аппаратных средств, осуществляющих архивное копирование, в соответствии с их инструкциями по эксплуатации.

Хранение отдельных магнитных носителей архивных копий организуется в отдельном от используемых данных помещении. Физический доступ к архивным копиям строго ограничен. Контроль за физическим доступом возлагается на администратора безопасности.

Доступ к носителям архивных копий имеют только уполномоченные работники подразделений информационных технологий (ИТ) и информационной безопасности (ИБ), которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

Уничтожение отделяемых магнитных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

3. ОТВЕТСТВЕННОСТЬ ЗА СОСТОЯНИЕ РЕЗЕРВНОГО КОПИРОВАНИЯ

Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на программиста колледжа.

Ответственность за контроль над своевременным осуществлением резервного копирования, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на администратора безопасности.

В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается программисту и руководителю.

4. ПЕРИОДИЧНОСТЬ РЕЗЕРВНОГО КОПИРОВАНИЯ

Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

Резервное копирование открытой информации делается не позднее чем через сутки после ее изменения, но не реже одного раза в месяц.

Информация (ПДн), содержащаяся в постоянно изменяемых базах данных, сохраняется в соответствии со следующим графиком:

□□ еженедельно проводится резервное копирование всей базы данных. Носители с еженедельными копиями хранятся в течение месяца;

□□ ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.).

5. ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ РЕЗЕРВНЫХ КОПИЙ

В случае необходимости восстановление данных из резервных копий производится программистом Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.