Приложение № 1
к приказу «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах отдела образования администрации городского округа Вичуга
от 29.12.2017г. № 254

Макарова Вера Витальевна

Подписано цифровой подписью: Макарова Вера Витальевна
Дата: 2025.03.21 12:38:31 +03'00'

Положение
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах отдела образования администрации городского округа Вичуга

Оглавление

Термины и определения

Автоматизированная система	Система, состоящая из работников (лиц, состоящих в трудовых отношениях с _____ *(указать название организации)*) и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций
Администратор безопасности информации	Должностное лицо (работник), ответственный за защиту информации, он же может быть ответственным за обеспечение безопасности персональных данных в информационной системе (работник, назначенный приказом руководителя), ответственный за защиту информационных систем персональных данных от несанкционированного доступа к информации
Администратор информационной системы	Администратор автоматизированной системы, администратор локальной вычислительной сети, администратор баз данных, администратор информационного ресурса - ответственный за функционирование информационной системы персональных данных в установленном штатном режиме работы (работники назначенные приказом руководителя)
Блокирование персональных данных	Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
Обладатель информации (информационного ресурса)	Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам. Структурное подразделение _____ *(указать название организации)*, реализующее полномочия владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами. Обладатель устанавливает в пределах своей компетенции режим и правила обработки информации, зашиты информационного ресурса, доступа к информационному ресурсу, условия копирования и тиражирования информационного ресурса (в распоряжении на создание информационного ресурса или в виде отдельных регламентов)
Доступ к информации	Возможность получения информации и ее использования
Информационная система персональных данных (ИСПДн)	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Инцидент информационной безопасности	Появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации операций и создания угрозы информационной безопасности (отказ в обслуживании, сбор информации, несанкционированный доступ и т.д.)
Контролируемая зона	Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание работников и посетителей

	организации, а также транспортных, технических и иных материальных средств
Конфиденциальность персональных данных	Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания
Несанкционированный доступ (несанкционированные действия)	Доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам
Обработка персональных данных	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных
Оператор	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (в настоящем Положении - _____ *(указать название организации)*.
Организационно-распорядительная документация ИСПДн	Документация, регламентирующая деятельность работников в области защиты конфиденциальной информации и персональных данных, а также требования к ИСПДн в соответствии с требованиями законодательства Российской Федерации
Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Предоставление персональных данных	Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
Распространение персональных данных	Действия, направленные на раскрытие персональных данных неопределенному кругу лиц
Руководящие документы по безопасности информации	Нормативно-правовые и методические документы ФСТЭК России и ФСБ России, регулирующие деятельность в области защиты информации
Субъект доступа (субъект)	Лицо или процесс, действия которого регламентируются правилами разграничения доступа
Технические средства, позволяющие осуществлять обработку персональных данных	Средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления

	базами данных и т.п.), средства защиты информации, применяемые в информационной системе
Трансграничная передача персональных данных	передача персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу
Угроза безопасности персональных данных	Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных
Уничтожение персональных данных	Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных

Перечень сокращений

АРМ	- автоматизированное рабочее место
АС	- автоматизированная система
ЗИ	- защита информации
ИБ	- информационная безопасность
ИР	- информационный ресурс
ИС	- информационная система
ИСПДн	- информационная система персональных данных
ИТ	- информационная технология
МЭ	- межсетевой экран
НСД	- несанкционированный доступ
ОС	- операционная система
ПДн	- персональные данные
ПО	- программное обеспечение
Положение	- Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн
СВТ	- средство вычислительной техники
СЗИ	- средство защиты информации
СЗПДн	- система защиты персональных данных
СКЗИ	- средство криптографической защиты информации
СТР-К	- «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденные приказом Гостехкомиссии России от 30 августа 2002 г. № 282
ТС	- техническое средство
ФСБ	- Федеральная служба безопасности
ФСТЭК	- Федеральная служба по техническому и экспортному контролю

1. Общие положения

Настоящее Положение регламентирует вопросы обеспечения безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) и иной, охраняемой законами Российской Федерации информации в отделе образования администрации городского округа Вичуга (далее отдел обазования, также – Учреждение) и определяет порядок организации работ по созданию и эксплуатации системы защиты персональных данных (СЗПДн).

Настоящее Положение разработано на основании следующих основных нормативных правовых актов и документов в области обеспечения безопасности ПДн:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России № 21 от 18 февраля 2013 года «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (зарегистрированный Минюст России, рег. № 28375 от 14 мая 2013 года);
- НМД «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), утвержден приказом Гостехкомиссии России от 30 августа 2002 года № 282 (извещения о корректировке № 1-2005 от 5.08.2005г., № 1-2006 от 24.03.2006г., № 1-2008 от 4.04.2008г.);
- НМД «Сборник руководящих документов по защите информации от несанкционированного доступа», Гостехкомиссия России, Москва, 1998 года;
- Приказ ФСТЭК России № 17 от 11 февраля 2013 года «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (зарегистрированный Минюст России, рег. № 28608 от 31 мая 2013 года).

Действие настоящего Положения распространяется на информационную систему отдела образования администрации городского округа Вичуга ИС «АРМ Государственная (итоговая) аттестация выпускников" в составе ИСПДн:

Действие настоящего Положения не распространяется на вопросы, связанные с обработкой ПДн, осуществляемой без использования средств автоматизации. Правила обработки ПДн, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами отдела образования администрации городского округа Вичуга, определяются в отдельном документе с учетом требований Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденных постановлением Правительства Российской Федерации от 15.09.2008 № 687.

2. Порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн

Под организацией работ по обеспечению безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности мероприятий, осуществляемых на всех стадиях жизненного цикла ИСПДн, согласованных по цели, задачам, месту и времени, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн, восстановление нормального функционирования ИСПДн после нейтрализации угрозы с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.

Организация работ по защите ПДн предусматривает формирование:

- перечня ПДн и конфиденциальной информации, обрабатываемых в информационных системах отдела образования администрации городского округа Вичуга;
- порядка классификации ИС как ИСПДн;
- порядка разработки, ввода в действие и эксплуатации ИСПДн в части реализации мероприятий по обеспечению безопасности ПДн;
- порядка взаимодействия между ответственными за обеспечение безопасности ПДн и эксплуатирующими подразделениями (пользователями) по вопросам обеспечения безопасности ПДн;
- порядка привлечения специализированных сторонних организаций к разработке и эксплуатации СЗПДн, их задачи и функции на различных стадиях создания и эксплуатации ИСПДн в соответствии с требованиями Руководящих документов по безопасности с учетом механизмов, предусмотренных Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;
- ответственности должностных лиц за обеспечение безопасности ПДн, своевременность и качество формирования требований по защите информации, за качество и научно-технический уровень разработки СЗПДн;
- порядка контроля обеспечения требуемого уровня защищенности ПДн.

Согласование подключений сторонних организаций к сети Учреждения осуществляется после согласования схемы подключения, подписания договора на использование ИР между отделом образования администрации городского округа Вичуга и сторонней организацией и соглашения о взаимодействии между такой сторонней организацией и Учреждением.

Для разработки и осуществления мероприятий по организации и обеспечению безопасности конфиденциальной информации и ПДн при их обработке в ИСПДн соответствующим приказом начальника отдела образования администрации городского округа Вичуга назначается должностное лицо (работник) ответственный за обеспечение безопасности информации и ПДн – Администратор безопасности информации.

Непосредственно исполнение работ по защите информации (ПДн) в ИСПДн с использованием средств автоматизации возлагается на ответственных за развитие и использование (эксплуатацию) ИСПДн.

Для проведения классификации ИСПДн соответствующим приказом начальника отдела образования администрации городского округа Вичуга назначается специальная внутренняя комиссия (рабочая группа). В состав этой комиссии (группы) включаются представители подведомственных организаций - обладателей информационных ресурсов ИСПДн.

Проведение обследования ИСПДн, разработка и реализация СЗПДн могут осуществляться как работниками Учреждения, так и на договорной основе с другими специализированными организациями, имеющими соответствующие лицензии на деятельность по технической защите конфиденциальной информации в соответствии с требованиями Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Научно-техническое и методическое руководство, непосредственная организация работ по созданию (модернизации) СЗПДн и контроль за эффективностью использования предусмотренных мер возлагается на специалиста по информационной безопасности в соответствии с требованиями постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

В случае разработки СЗПДн или ее отдельных компонентов специализированными организациями специалист по информационной безопасности (Администратор безопасности информации) отвечает за организацию и проведение мероприятий по защите информации.

Разработка, внедрение и эксплуатация СЗПДн осуществляются во взаимодействии разработчика с Администратором безопасности информации.

Контроль за реализацией проектных решений возлагается на начальника отдела образования администрации городского округа Вичуга

2.1. Порядок определения защищаемой информации и классификации ИСПДн

Внутренней комиссией (рабочей группой), образованной приказом начальника отдела образования администрации городского округа Вичуга, для каждой ИСПДн определяется перечень ПДн, уточняются цели и основание обработки ПДн, а также срок хранения и условия прекращения обработки.

Целью классификации ИС отдела образования администрации городского округа Вичуга как ИСПДн является определение по её результатам перечня обоснованных организационных и технических мероприятий, позволяющих выполнить требования по обеспечению безопасности ПДн с учётом особенностей конкретной ИСПДн.

Классификация может проводиться на этапе создания ИС или в ходе её эксплуатации (для ранее введенной в эксплуатацию и (или) модернизируемой ИС).

Классификация ИСПДн осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Классификация ИСПДн проводится внутренней комиссией (рабочей группой) и включает в себя следующие этапы:

- сбор и анализ исходных данных по ИС;
- присвоение ИС соответствующего класса и его документальное оформление.

При проведении классификации ИСПДн внутренней комиссией (рабочей группой) определяются:

- заданные Учреждением характеристики безопасности ПДн, обрабатываемых в ИС;
- структура ИС;
- наличие подключений ИС к сетям связи общего пользования и (или) сетям международного информационного обмена;

- режим обработки ПДн;
- режим разграничения прав доступа пользователей ИС;
- местонахождение технических средств ИС.

В случае выделения в составе ИС подсистем, каждая из которых является ИС, ИС в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем, если данные ИС не разделены между собой МЭ.

Предложения комиссии (рабочей группы) по отнесению ИС к определенному классу согласовываются с начальником отдела образования администрации городского округа Вичуга.

Результаты классификации ИСПДн Учреждения оформляются Актом, утверждаемым начальником отдела образования администрации городского округа Вичуга, в соответствии с Приложением № 1 к Специальным требованиям и рекомендациям по технической защите конфиденциальной информации (СТР-К), утвержденным приказом Гостехкомиссии России от 30.08.2002 № 282.

Сформированные по результатам классификации материалы являются неотъемлемой частью организационно-распорядительной документации ИСПДн и относятся к информации конфиденциального характера. Оригиналы организационно-распорядительной документации ИСПДн хранятся у лица, ответственного за организацию работ по защите ПДн.

Класс ИСПДн может быть пересмотрен комиссией (рабочей группой) в установленном порядке в следующих случаях:

- на основе результатов проведенного анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений конкретной ИС;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в ИС.

2.2. Порядок разработки, ввода в действие и эксплуатации СЗПДн

Для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в ИС;
- разработка системы защиты информации ИС;
- внедрение системы защиты информации ИС;
- аттестация ИС и ввод ее в действие;
- обеспечение защиты информации в ходе эксплуатации аттестованной ИС;
- обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации.

2.3. Порядок привлечения структурных подразделений Учреждения и специализированных сторонних организаций к разработке и эксплуатации ИСПДн, их задачи и функции на различных стадиях создания и эксплуатации ИСПДн

Для организации и обеспечения безопасности ПДн при их обработке в ИСПДн соответствующим приказом начальника отдела образования администрации городского округа Вичуга назначается должностное лицо (работник) ответственное за обеспечение безопасности информации, в т.ч. ПДн – Администратор безопасности информации.

Администратор безопасности информации обеспечивает методическое руководство, разработку требований к мерам защиты ИСПДн Учреждения и контроль за эффективностью использования предусмотренных мер защиты информации.

Администратор безопасности информации обеспечивает подготовку предложений по совершенствованию и реализации положений Политики информационной безопасности ИСПДн и контролирует выполнение установленных требований отдела образования администрации городского округа Вичуга

Администратор безопасности информации осуществляет следующие основные функции:

- разрабатывает предложения по определению класса защищенности объектов ИСПДн и автоматизированной системы (АС);
- участвует в организации работ по выявлению актуальных угроз безопасности ПДн;
- осуществляет методическое руководство и участвует в разработке (согласовании) конкретных требований по защите ПДн и разработке технического (частного технического) задания на создание СЗПДн;
- согласовывает выбор конкретных средств обработки ПДн, технических и программных средств защиты;
- осуществляет контроль реализации проектных решений на создание СЗПДн;
- участвует в организации работ по оценке соответствия ИСПДн предъявляемым требованиям по обеспечению безопасности ПДн;
- участвует в организации разработки организационно-распорядительной документации по защите информации в ИСПДн;
- проводит контроль требуемого уровня обеспечения защищенности ПДн при эксплуатации СЗПДн, в том числе контроль соблюдения условий использования СЗИ;
- участвует в организации обучения должностных лиц (работников) – пользователей ИСПДн отдела образования администрации городского округа Вичуга, ответственных за эксплуатацию СЗИ, по направлению обеспечения безопасности ПДн;
- участвует в организации охраны и физической защиты помещений отдела образования администрации городского округа Вичуга, в которых размещаются средства обработки ПДн, исключающих несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности, хищение носителей информации;
- оказывает методическую помощь должностным лицам (работникам) отдела образования администрации городского округа Вичуга.

Администратор безопасности информации разрабатывает правила работы с информацией, техническими средствами и правила использования ПДн в соответствии с возможностями, функциями, предназначением и степени защищенности этих средств, ресурсов и требованиям к защите и доступности ПДн, осуществляет предоставление ИТ - сервисов всем структурным подразделениям Учреждения, отвечает за их целостность и доступность, обеспечивает разграничение доступа к ПДн в процессе их использования, контроль над ходом информационных процессов.

Привлечение для разработки СЗПДн или ее отдельных компонентов сторонних специализированных организаций осуществляется в соответствии с порядком, устанавливаемым нормативными и организационно-распорядительными документами ФСТЭК России и ФСБ России.

В случае привлечения для обеспечения безопасности ПДн сторонних специализированных организаций в соответствии с требованиями Федерального закона от 05.04.2013 № 44-ФЗ «О

контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» рекомендуется выполнение следующих условий:

- наличие у организации лицензии на право проведения работ по технической защите конфиденциальной информации;
- оформление соглашения о неразглашении конфиденциальных сведений;
- проведение инструктажа исполнителей работ по вопросам ИБ;
- другие условия, устанавливаемые соответствующими нормативными и организационно-распорядительными документами.

При привлечении сторонних специализированных организаций работникам следует учитывать следующие функции в техническом задании:

а) формирование требований к защите информации, содержащейся в информационной системе:

- уточнение перечня ПДн, подлежащих защите;
- определение условий расположения ИСПДн относительно границ контролируемой зоны;
- определение конфигурации и топологии ИСПДн в целом, и ее отдельных компонент, физические, функциональные и технологические связи как внутри ИСПДн, так и с другими системами различного назначения;
- определение технических средств и систем, включаемых в состав ИСПДн, условий их расположения, общесистемных и прикладных программных средств;
- определение режимов обработки ПДн в ИСПДн;
- разработка предложений по уточнению класса защищенности ИСПДн;
- уточнение степени участия работников в обработке ПДн, характера их взаимодействия между собой;
- определение (уточнение) угроз безопасности ПДн с учётом конкретных условий функционирования ИСПДн, разработка проекта частной модели угроз;
- участие в разработке (согласовании) конкретных требований по защите ПДн и разработке технического (частного технического) задания на создание СЗПДн.

б) разработка системы защиты информации информационной системы:

- разработка технического проекта на создание СЗПДн в соответствии с требованиями руководящих документов ФСТЭК России и ФСБ России;
- монтажные работы в соответствии с проектной документацией;
- использование сертифицированных технических, программных и программно-технических СЗИ и их установка;
- организация сертификации по требованиям безопасности информации программных СЗИ в случае, когда на рынке отсутствуют требуемые сертифицированные СЗИ;
- разработка разрешительной системы доступа пользователей к ПДн, обрабатываемым в ИСПДн;
- разработка (в согласованном объеме) эксплуатационной документации на СЗПДн.

в) внедрение системы защиты информации информационной системы:

- установка СЗИ;
- предварительные испытания и опытная эксплуатация СЗИ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

- приемо-сдаточные испытания СЗИ по результатам опытной эксплуатации;
- оценка соответствия ИСПДн требованиям безопасности ПДн.

3. Основные требования и правила по обеспечению безопасности ПДн при их обработке в ИСПДн

Обеспечение безопасности ПДн при их обработке в ИСПДн отдела образования администрации городского округа Вичуга достигается применением организационных и технических мер, причем в интересах обеспечения безопасности в обязательном порядке подлежат защите технические и программные средства, используемые при обработке ПДн, и носители информации.

Основными направлениями защиты информации (ПДн) являются:

- обеспечение защиты информации (ПДн) от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет несанкционированного доступа (НСД) и специальных воздействий;
- обеспечение защиты информации (ПДн) от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

Основными мерами защиты информации (ПДн) являются:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к ИР, ИС и связанным с её использованием работам, документам;
- ограничение доступа пользователей в помещения, в которых размещены технические средства (ТС), позволяющие осуществлять обработку ПДн, а также в которых хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к ИР, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа (НСД) и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
- резервирование ТС, дублирование массивов и носителей информации;
- использование СЗИ, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности информации;
- использование защищенных каналов связи;
- размещение ТС, позволяющих осуществлять обработку ПДн в пределах охраняемой территории;
- использование ТС, удовлетворяющих требованиям стандартов по электромагнитной совместимости, безопасности, санитарным нормам, предъявляемым к видеодисплейным терминалам;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах охраняемой территории;
- обеспечение развязки цепей электропитания ТС с помощью защитных фильтров, блокирующих (подавляющих) информационный сигнал;

- обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных ТС и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация;
- размещение устройств вывода (отображения) информации, исключающее её несанкционированный просмотр. Устройствами вывода (отображения) информации являются экраны мониторов автоматизированных рабочих мест пользователей, мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств), видеопанели, видеостены и другие средства визуального отображения защищаемой информации, печатающие устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональные устройства. Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра;
- организация физической защиты помещений и собственно ТС, позволяющих осуществлять обработку ПДн;
- предотвращение внедрения в ИС вредоносных программ (программ-вирусов) и программных закладок.

Для обеспечения безопасности информации от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет НСД, заданных характеристик безопасности обрабатываемых ПДн, угроз безопасности ПДн, структуры ИСПДн, наличия межсетевого взаимодействия и режимов обработки ПДн в рамках СЗИ от НСД реализуются функции управления доступом, регистрации и учёта, обеспечения целостности, анализа защищённости, обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений.

Перечень мер по защите информации от утечки по техническим каналам при её обработке, хранении и передаче по каналам связи применяются по решению отдела образования администрации городского округа Вичуга.

Применяемые СЗИ учитываются в Журнале учета СЗИ. В случае проведения аттестации ИСПДн учёт применяемых технических СЗИ ведется в документе «Технический паспорт ИСПДн» в соответствии с требованиями СТР-К.

3.1. Требования по организации разрешительной системы доступа пользователей к обрабатываемой в ИСПДн информации

Данный раздел Положения регламентирует порядок взаимодействия подразделений отдела образования администрации городского округа Вичуга по обеспечению безопасности ПДн при организации разрешительной системы доступа к сервисам и ресурсам ИСПДн.

Разрешительная система доступа к обрабатываемой в ИС информации предусматривает установление единого порядка обращения со сведениями, содержащими ПДн и их носителями, определяет степень ограничения на доступ к данной информации и степень ответственности за сохранность предоставленной информации.

Организация разрешительной системы доступа относится к основным вопросам управления обеспечением безопасности ПДн и включает:

- распределение функций управления доступом к данным и их обработкой между должностными лицами;
- определение порядка изменения правил доступа к защищаемой информации;
- определение порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;
- контроль функционирования разрешительной системы доступа и расследование фактов неправомерного доступа лиц к защищаемой информации, в случае выявления таковых;
- оценку эффективности проводимых мер по исключению утечки информации;
- организацию деятельности должностных лиц, ответственных за подготовку предложений о внесении изменений в должностные обязанности и иные документы, определяющие задачи и функции работников ИСПДн;
- разработку внутренних организационно-распорядительных документов, определяющих порядок реализации и функционирования разрешительной системы доступа.

Основные условия правомерного доступа работников отдела образования администрации городского округа Вичуга к обрабатываемой в ИС информации включают в себя:

- подписание работником отдела образования администрации городского округа Вичуга обязательства о неразглашении конфиденциальной информации;
- наличие у работника Учреждения оформленного в установленном порядке права доступа к ПДн, обрабатываемым в ИСПДн;
- наличие утвержденных в соответствии с трудовым законодательством Российской Федерации, должностных (функциональных) обязанностей работника, определяющих круг его задач и объем необходимой для их решения информации.

Лица, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения трудовых обязанностей, допускаются к соответствующим ПДн на основании Списка должностей работников с указанием методов управления доступом, типа доступа и правил доступа, утвержденного начальником отдела образования администрации городского округа Вичуга.

Для обеспечения персональной ответственности за свои действия каждому пользователю ИСПДн, допущенному к работе с защищаемой информацией в ИСПДн, присваивается уникальное имя (учетная запись пользователя), под которым он регистрируется и осуществляет работу в системе. В случае производственной необходимости пользователю ИСПДн могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими работниками при работе в ИСПДн одного и того же имени пользователя («группового имени») запрещается.

В информационной системе должна обеспечиваться идентификация и аутентификация пользователей, являющихся работниками.

При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

К внутренним пользователям в целях настоящего документа, относятся должностные лица (пользователи, администраторы), выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ИС в соответствии с утвержденными должностными регламентами (инструкциями) и которым в

ИС присвоены учетные записи.

В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования информационной системы (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами отдела образования администрации городского округа Вичуга и которым в информационной системе также присвоены учетные записи.

Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации.

В информационной системе должен быть установлен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации.

Разрешение действий пользователей до прохождения ими процедур идентификации и аутентификации осуществляется, в том числе, при предоставлении пользователям доступа к общедоступной информации (веб-сайтам, порталам, иным общедоступным ресурсам). Также администратору разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, иных средств или в случае многофакторной (двухфакторной) аутентификации – определенной комбинации указанных средств.

В информационной системе должна осуществляться однозначная идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей), или процессов, запускаемых от имени этих пользователей.

В ИС должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

При регистрации и назначении прав доступа пользователей ИС Учреждения выполняются следующие требования:

- каждому пользователю присваивается уникальный идентификатор пользователя, по которому его можно однозначно идентифицировать;
- учётные записи всех пользователей привязываются к конкретным автоматизированным рабочим местам (АРМ), за исключением учетных записей технического персонала, обслуживающего компоненты ИСПДн;
- при регистрации пользователей проводится проверка соответствия уровня доступа возложенным на пользователя задачам (вмененным обязанностям);
- назначенные пользователю права доступа документируются;
- пользователь знакомится под роспись с предоставленными ему правами доступа и порядком его осуществления;
- в ИСПДн предусматривается разрешение доступа к сервисам только аутентифицированным пользователям;

- при внесении нового пользователя разрабатывается и обновляется формальный список всех пользователей, зарегистрированных для работы в ИСПДн;
- при изменении должностных обязанностей (увольнении) пользователя проводится немедленное исправление (аннулирование) прав его доступа;
- исключается возможность повторного использования идентификатора пользователя и (или) устройства в течение установленного периода времени;
- идентификатор пользователя блокируется после установленного времени неиспользования;
- Администратором информационной системы проводится удаление всех неиспользуемых учетных записей.

Администратор информационной системы является лицом, ответственным за создание, присвоение и уничтожение идентификаторов пользователей.

Предусмотренные в системе запасные идентификаторы недоступны другим пользователям.

В информационной системе должно быть исключено повторное использование идентификатора пользователя в течение одного года.

В информационной системе должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования не более 90 дней.

В информационной системе устанавливаются и реализуются функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в информационной системе:

- изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы;
- выдача средств аутентификации пользователям;
- генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);
- установление характеристик пароля:
  - задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов (длина пароля не менее шести символов, алфавит пароля не менее 30 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут, смена паролей не более чем через 180 дней);
  - задание минимального количества измененных символов при создании новых паролей;
  - задание максимального времени действия пароля;
  - задание минимального времени действия пароля;
  - запрет на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей;

- блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;
- назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);
- обновление аутентификационной информации (замена средств аутентификации) с периодичностью, установленной оператором;
- защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

В информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после установленного времени его бездействия (неактивности) в информационной системе или по запросу пользователя.

Блокирование сеанса доступа пользователя в информационную систему обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к информационной системе (без выхода из информационной системы).

Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

Блокирование сеанса доступа пользователя в информационную систему должно сохраняться до прохождения им повторной идентификации и аутентификации.

Администратор информационной системы является лицом, ответственным за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками«*», «□» или иными знаками.

Использование дополнительных типов устройств, необходимых для использования в информационной системе возможно, только после утверждения руководителем _____ *(указать полное название организации)*» перечня типов устройств, подлежащих идентификации и аутентификации, до начала информационного обмена.

Контроль выполнения требований разрешительной системы доступа к ПДн возлагается на Администратора безопасности информации.

В информационной системе должны быть установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

- определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей);
- объединение учетных записей в группы (при необходимости);
- верификация пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;

- заведение, активация, блокирование и уничтожение учетных записей пользователей;
- пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой оператором;
- порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;
- оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;
- уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;
- предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

В информационной системе должно быть обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

В Учреждении должны быть однозначно определены и зафиксированы в организационно-распорядительных документах по защите информации (задокументированы) роли и (или) должностные обязанности (функции), также объекты доступа, в отношении которых установлен наименьший уровень привилегий.

В информационной системе для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные оператором методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа.

Правила разграничения доступа реализуются на основе установленных оператором списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в информационную систему, доступом к техническим средствам, устройствам, внешним устройствам, а также к объектам, создаваемым общесистемным (общим) программным обеспечением.

В информационной системе должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).

Доступ к ИР ИСПДн сторонних организаций (правоохранительных органов, судебных органов, органов статистики, органов исполнительной и законодательной власти субъектов Российской Федерации) регламентируется законодательством Российской Федерации, приказами и распоряжениями министерств и служб, законодательно наделенных полномочиями на получение информации, а также настоящим Положением.

Порядок доступа к ИР ИСПДн сторонних организаций, выполняющих работы на договорной основе, определяется в договоре на выполнение работ (оказание услуг) в соответствии с требованиями Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Обязательным условием договора является заключение соглашения об обеспечении безопасности персональных данных и их конфиденциальности.

3.2. Требования к проведению мероприятий по размещению, специальному оборудованию, охране и режиму допуска в помещения, где размещены средства ИСПДн

Данный раздел Положения содержит общие требования к проведению мероприятий по размещению, специальному оборудованию, охране и режиму допуска в помещения, в которых размещены ИСПДн:

1. Обеспечивается контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств.

Границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

Для одной информационной системы (ее сегментов) может быть организовано несколько контролируемых зон.

Организуется контроль доступа работников и посетителей в помещения отдела образования администрации городского округа Вичуга, в которых установлены ТС ИСПДн и осуществляется обработка ПДн, а также хранятся носители ПДн.

2. Доступ работников Учреждения и посетителей в эти помещения осуществляется в сопровождении ответственных должностных лиц.

3. Для защиты помещений, в которых расположены ТС ИСПДн, принимаются меры для минимизации воздействий огня, дыма, воды, пыли, взрыва, химических веществ, а также кражи.

4. ТС ИСПДн и размещенное совместно с ними вспомогательное оборудование подвергаются регулярным осмотрам с целью выявлений изменения конфигурации средств электронно-вычислительной техники (замки на коммутационных шкафах, использование специальных защитных знаков, пломбирование, опечатывание и др.).

5. Обеспечивается размещение устройств вывода информации средств вычислительной техники, дисплеев АРМ ИСПДн таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей ПДн.

6. Определение интерфейсов средств вычислительной техники, которые, могут использоваться для ввода (вывода) информации, разрешённых и (или) запрещенных к использованию в ИС.

7. Работникам отдела образования администрации городского округа Вичуга запрещается подключать к сети неучтенные информационно-телекоммуникационные средства.

3.3. Правила обеспечения безопасности ПДн при использовании съемных носителей информации

В Учреждении должны обеспечиваться регламентация и контроль использования в информационной системе мобильных технических средств, направленные на защиту информации в информационной системе.

В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

Регламентация и контроль использования мобильных технических средств должны включать:

- установление (в том числе документальное) видов доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа), разрешенных для доступа к объектам доступа информационной системы с использованием мобильных технических средств, входящих в состав информационной системы;
- использование в составе информационной системы для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации;
- ограничение на использование мобильных технических средств в соответствии с задачами (функциями) информационной системы, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств;
- мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа информационной системы;
- запрет возможности запуска без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством.

3.3.1. Правила обращения со съемными носителями информации

В информационной системе допускается использование только учтённых, установленным порядком, съемных носителей информации.

При этом должны соблюдаться установленные правила управления доступом к объектам доступа, методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа в соответствии с функциональными обязанностями (решаемыми задачами).

При обращении со съемными носителями информации выполняются следующие основные правила:

- носители информации учитываются и выдаются пользователям под роспись и защищены;
- носители информации, срок эксплуатации которых истек, уничтожаются установленным порядком;
- для выноса носителей информации за пределы объектов отдела образования администрации городского округа Вичуга дается специальное разрешение, а факт выноса фиксируется;
- все носители информации хранятся в безопасном месте в соответствии с требованиями по их эксплуатации;
- мониторинг за использованием съемных носителей информации осуществляется постоянно руководителями структурных подразделений, в которых установлены ресурсы ИСПДн, Администратором безопасности информации и Администратором информационной системы.

Администратор информационной системы обеспечивает запрет запуска без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия со съемным носителем информации.

Ответственным за хранение, учет и выдачу съемных носителей ПДн является Администратор безопасности информации.

3.3.2. Порядок учёта носителей информации

Все находящиеся на хранении и в обращении машинные носители информации поэкземплярно учитываются в Журнале учета машинных носителей конфиденциальной информации и персональных данных.

Учёту подлежат:

- съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
- портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жёстких дисках).

Учёт машинных носителей информации включает присвоение регистрационных (учетных)

номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учёта, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

Учёт встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учёта в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

Регистрационные или иные номера подлежат занесению в журналы учёта машинных носителей информации или журналы материально-технического учёта с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

Раздельному учёту в журналах учёта подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш-накопители, съёмные жесткие диски).

Каждый носитель, с записанными на нём ПДн, имеет этикетку, на которой указывается метка съёмного носителя и гриф.

Пользователи ИСПДн для выполнения работ получают учтённый съёмный носитель от ответственного работника отдела образования администрации городского округа Вичуга. При получении делаются соответствующие записи в Журнале учёта.

После окончания работ пользователь ИСПДн сдает машинный носитель ответственному работнику отдела образования администрации городского округа Вичуга для хранения, о чем делается соответствующая запись в Журнале учёта.

При наличии личного сейфа у пользователя ИСПДн допускается хранение учтённых съёмных машинных носителей в личных сейфах (металлических шкафах), опечатанных печатью пользователя ИСПДн.

Хранение съемных машинных носителей персональных данных осуществляется в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

3.3.3. Порядок доступа к машинным носителям информации

Порядок доступа к машинным носителям информации в отдела образования администрации городского округа Вичуга заключается в определении должностных лиц, имеющих физический доступ к машинным носителям информации, а именно к следующим:

- съёмным машинным носителям информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
- портативным вычислительным устройствам, имеющим встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые

камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

- машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жёстких дисках);
- предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций).

3.3.4. Порядок уничтожения машинных носителей информации

Уничтожение (стирание) информации на машинных носителях обеспечивается при их передаче между пользователями, в сторонние организации для ремонта или утилизации и должно исключать возможность восстановления защищаемой информации.

Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съёмных и несъёмных машинных носителях информации.

В Учреждении должны быть обеспечены регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации.

Должны применяться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:

- перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием.

Носители ПДн, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению.

Уничтожение носителей ПДн осуществляется комиссией по уничтожению, назначенной руководителя Учреждения.

Уничтожение магнитных, оптических, магнитооптических и электронных носителей информации производится путем их физического разрушения. Перед уничтожением носителя информация с него стирается (уничтожается), если это позволяют физические принципы работы носителя.

Бумажные носители данных уничтожаются через термическую обработку (сжигание) или с использованием специальных устройств - шредеров.

Перед утилизацией оборудования, участвующего в обработке ПДн, Администратором информационной системы осуществляется проверка всех его компонентов, включая носители информации (жёсткие диски) на отсутствие ПДн и лицензированного программного обеспечения (ПО).

По результатам уничтожения комиссией составляется Акт уничтожения носителей ПДн, который хранится в помещении для хранения носителей ПДн, уничтоженные носители ПДн (утилизированное оборудование) снимается с материального учета.

3.4. Порядок и правила использования паролей пользователей

Организационное и техническое обеспечение смены, прекращения действия паролей в ИСПДн Учреждения, процессов генерации и использования возлагается в пределах своих

полномочий на Администратора безопасности информации и Администратора информационной системы, сопровождающего механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

При использовании паролей в ИСПДн выполняются следующие правила:

- пароли обязаны меняться с установленной периодичностью в соответствии с требованиями, установленными в отделе образования администрации городского округа Вичуга;
- пароль должен иметь не менее 6 символов и содержит буквенные и цифровые символы (алфавит пароля не менее 30 символов);
- обязательно применение индивидуальных паролей;
- применение групповых паролей не допускается;
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток;
- блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут;
- при создании пароля пользователя администратором предусматривается его автоматическое изменение самим пользователем после первого же его входа в ИСПДн;
- для предотвращения повторного использования паролей ведется их учёт (запись) за предыдущие 12 месяцев;
- при вводе пароль не выдается на монитор компьютера в явном виде;
- пароли могут храниться только на АРМ владельца пароля в зашифрованном виде с использованием стойких алгоритмов шифрования. Файл с паролями хранится отдельно от системных приложений;
- рекомендуется использование возможностей операционной системы (ОС) по контролю за периодичностью смены (не реже 1 раза в 180 дней), составу символов и недопущению повторений паролей.

Контроль за действиями пользователей ИСПДн при работе с паролями возлагается на Администратора безопасности информации в пределах своих полномочий.

При использовании паролей запрещается:

- использовать в качестве пароля свои имя, фамилию, дату рождения, имена родственников, кличку собаки и т. п., равно как и обычные слова;
- использовать в качестве пароля русское слово, введенное при нахождении клавиатуры в латинском регистре;
- использовать в качестве пароля легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ), а также общепринятые сокращения;
- использовать в качестве пароля «пустой» пароль, имя входа в систему, а также выбирать пароли, которые уже использовались ранее;
- использовать один и тот же пароль при загрузке АРМ и при работе в ИСПДн;
- записывать пароль на неучтённых бумажных носителях информации;
- разглашать кому бы то ни было свои персональные пароли доступа.

В ИС должно обеспечиваться автоматическое блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем трех неуспешных попыток входа в информационную систему (доступа к

информационной системе) в течение трех минут с возможностью разблокирования только Администратором информационной системы.

В информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после пяти минут его бездействия (неактивности) в ИС или по запросу пользователя.

Блокирование сеанса доступа пользователя в информационную систему обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к ИС (без выхода из информационной системы).

Для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

Блокирование сеанса доступа пользователя в ИС сохраняется до прохождения им повторной идентификации и аутентификации.

Администратор безопасности информации совместно с Администратором информационной системы обеспечивают в ИС визуальное предупреждение пользователя в виде сообщения («окна») при его входе в ИС (до процесса аутентификации) о том, что в информационной системе реализованы меры защиты информации, а также о том, что при работе в информационной системе пользователем должны быть соблюдены установленные обладателем ИСПДн правила и ограничения на работу с информацией.

До пользователей информационной системы под роспись доводятся требования по организации парольной защиты в отделае образования администрации городского округа Вичуга с проставлением собственноручно подписи в листе ознакомления с соответствующей документированной процедурой и ответственность за использование паролей, не соответствующих установленным требованиям, а также за разглашение парольной информации.

3.5. Обязанности работников, при возникновении инцидентов информационной безопасности

Настоящий раздел регламентирует взаимодействие отдела образования администрации городского округа Вичуга с подведомственными организациями при возникновении нештатных ситуаций.

При возникновении инцидентов ИБ работник, обнаруживший инцидент, немедленно ставит в известность своего непосредственного руководителя и Администратора безопасности информации или Администратора информационной системы.

Администратор безопасности информации или Администратора информационной системы проводят предварительный анализ ситуации.

По факту возникновения инцидента ИБ проводится выяснение причин его возникновения.

Результаты расследования фиксируются в акте. К акту прилагаются (при наличии) поясняющие материалы (копии экрана, распечатка журнала событий и др.). Акт предоставляется начальнику отдела образования администрации городского округа Вичуга.

3.6. Требования к резервированию информационных ресурсов

Резервное копирование защищаемой информации (ПДн) применяется для оперативного восстановления данных в случае утери или по другим причинам.

В состав ИР, подлежащих резервному копированию, в обязательном порядке включаются ИР, являющиеся объектом защиты в отделе образования администрации городского округа Вичуга

При организации резервирования ИР обеспечивается выполнение следующих требований:

- резервное копирование информации на резервные машинные носители информации с установленной периодичностью;
- разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации;
- регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации;
- резервные копии ИР и инструкции по их восстановлению хранятся в специально выделенном месте, территориально отдаленном от места хранения основной копии информации;
- принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность;
- регулярная проверка носителей, на которые осуществляется резервное копирование, на отсутствие сбоев;
- обеспечение производительности, достаточной для сохранения информации, в установленные сроки и с заданной периодичностью;
- регулярная проверка процедур восстановления и практический тренинг работников по восстановлению данных.

Резервное копирование информации осуществляется Администратором информационной системы в соответствии с графиком резервного копирования. Допускается осуществление резервного копирования в автоматизированном режиме.

График резервного копирования составляется для каждого вида информации, подлежащей периодическому резервному копированию. Периодичность проведения резервного копирования устанавливается Графиком резервного копирования не реже одного раза в неделю и может осуществляться ежедневно (в автоматизированном режиме).

Резервное копирование информации производится в соответствии с документацией на используемое ПО.

Программно-аппаратные средства, обеспечивающие проведение резервного копирования и носители, на которые осуществляется резервное копирование, не реже одного раза в месяц проверяются на отсутствие сбоев в соответствии с документацией на программно-аппаратные средства с отметкой в Журнале проверки работоспособности системы резервного копирования.

Резервные копии данных хранятся вместе с инструкцией по восстановлению данных из резервных копий на отдельных (размещенных вне информационной системы) средствах хранения резервных копий и в помещениях, специально предназначенных для хранения резервных копий информации, которые исключают воздействие внешних факторов на хранимую информацию.

Восстановление данных из резервной копии производится Администратором информационной системы на основании заявки начальника структурного подразделения - обладателя ИР, согласованной с Администратором безопасности информации. Заявка может предоставляться в электронной форме.

Восстановление данных из резервных копий осуществляется в соответствии с документацией на используемое ПО в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

Восстановление информации с резервных машинных носителей информации (резервных копий) должно предусматривать:

- определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования информационной системы и доступности информации;
- восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала;
- регистрацию событий, связанных восстановлением информации с резервных машинных носителей информации.

3.7. Правила защиты ИСПДн от вредоносных программ

При использовании в ИСПДн средств антивирусной защиты и защиты от вредоносных программ выполняются следующие организационные меры:

- использование съёмных носителей ПДн пользователя ИСПДн на других компьютерах только с механической защитой от записи;
- запрет на использование посторонних съёмных носителей ПДн при работе в ИСПДн;
- запрет на передачу съёмных носителей ПДн посторонним лицам;
- запрет на запуск программ с внешних съёмных носителей информации при работе в ИСПДн;
- запрет на несанкционированное использование отчуждаемых носителей информации (оптических дисков, флэш-карт и т. п.);
- использование в ИСПДн только дистрибутивов программных продуктов, приобретенных у официальных дилеров фирм-разработчиков этих продуктов;
- обязательная проверка всех программных продуктов;
- проверка всех программных файлов и файлов документов, полученных по электронной почте, специальными антивирусными средствами;
- систематическая проверка содержимого дисков файловых хранилищ обновленными версиями антивирусных программ;
- контроль и обновление списка разрешенных ссылок на веб-ресурсы сети «Интернет».

Реализация антивирусной защиты должна предусматривать:

- применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы);
- установку, конфигурирование и управление средствами антивирусной защиты;
- предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;
- проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);

- проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;
- оповещение Администратора информационной системы в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);
- определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

В информационной системе должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты Администратору безопасности информации.

Ответственность за эксплуатацию средств антивирусной защиты и защиты от вредоносных программ возлагается:

- на Администратора информационной системы в части наличия антивирусного ПО на клиентских рабочих станциях и использования данного ПО пользователями;
- на Администратора безопасности информации в части централизованного управления СЗИ.

Оператором должно быть обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов). Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать:

- получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);
- получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);
- контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

3.8. Требования по обеспечению безопасности при работе в информационно – телекоммуникационных сетях

Доступ к информационно – телекоммуникационным сетям, в т.ч. «Интернет», предоставляется пользователям исключительно в целях повышения эффективности выполнения ими своих трудовых обязанностей.

Организация доступа пользователей ИСПДн к информационно – телекоммуникационным сетям и сети «Интернет» осуществляется Администратором информационной системы на основании мотивированного запроса руководителя организации, подведомственной отделу образования, согласованного с Администратором безопасности информации.

Установка дополнительного оборудования и ПО для осуществления доступа пользователей ИСПДн осуществляется в порядке, установленным настоящим Положением для внесения изменений в ПО и аппаратные средства отдела образования администрации городского округа Вичуга.

В информационной системе должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.

Защита информации обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации.

Администратор безопасности информации и Администратор информационной системы обеспечивают защиту информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

Использование удаленного доступа к информационной системе запрещено.

В отдельных случаях по решению начальника отдела образования администрации городского округа Вичуга, в случае служебной необходимости и наличия технической возможности может быть обеспечен удаленный доступ к информационной системе, но при этом должна быть обеспечена защита требуемого вида доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) которая должна включать. Защита удаленного доступа должна обеспечиваться при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) и включает:

- установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа информационной системы;
- ограничение на использование удаленного доступа в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа;
- предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
- мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной системы;
- контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой (передачи защищаемой информации).

Использование технологий беспроводного доступа к информационной системе запрещено.

В отдельных случаях по решению руководителя _____ *(указать полное название организации)*», в случае служебной необходимости и наличия технической возможности может быть организован беспроводный доступ пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), но при этом дополнительно должны быть обеспечены регламентация и контроль использования технологий беспроводного доступа, направленные на защиту информации в ИС.

Регламентация и контроль использования технологий беспроводного доступа должны включать:

- ограничение на использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) ИС, для решения которых такой доступ

необходим;

- предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
- мониторинг и контроль применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа информационной системы;
- контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИС до начала информационного взаимодействия с информационной системой.

Запрещается использование подключений к сети «Интернет» и каналам связи, использование которых не согласовано с Администратором безопасности информации.

Пользователи ИСПДн могут использовать сеть «Интернет» в качестве:

- транспортной среды при обмене информацией между несколькими территориально разнесенными элементами ИСПДн или другими ИС (транспортная задача);
- средства предоставления открытой общедоступной информации, содержащейся в ИР отдела образования администрации городского округа Вичуга, внешнему абоненту (портальная задача);
- средства получения необходимой пользователям ИСПДн информации, содержащейся в ИР сети «Интернет» или других корпоративных сетей (информационная задача).

Администратор безопасности информации может ограничивать доступ к ресурсам сети «Интернет», содержание которых не имеет отношения к исполнению трудовых обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

При работе с ресурсами сети «Интернет» запрещается:

- разглашение конфиденциальной информации, ставшей известной работнику отдела образования администрации городского округа Вичуга, в связи с исполнением трудовых обязанностей либо иным путем;
- распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;
- публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления НСД, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения НСД к платным ресурсам в сети «Интернет», а также размещение ссылок на вышеуказанную информацию;
- загрузка и запуск исполняемых либо иных файлов без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
- использование анонимных прокси-серверов;

– доступ к ресурсам сети «Интернет», содержащим развлекательную (в том числе музыкальные, видео, графические и другие файлы, не связанные с производственной деятельностью), эротическую или порнографическую информацию.

Вся информация о ресурсах, посещаемых работниками Учреждения, протоколируется.

Администратор информационной системы обязан проводить анализ использования ресурсов сети «Интернет» и в случае необходимости представлять отчет об использовании «Интернет-ресурсов» работниками Администратору безопасности информации.

В случае обнаружения значительных отклонений в параметрах работы средств обеспечения доступа к ресурсам сети «Интернет» от среднестатистических значений немедленно сообщается Администратору безопасности информации для принятия последующих решений.

Руководители подразделений вправе запросить у Администратора безопасности информации отчет об использовании ресурсов сети «Интернет» работниками своего подразделения.

При нарушении работником Учреждения правил работы в сети «Интернет» либо возникновении нештатных ситуаций доступ к ресурсам сети «Интернет» блокируется Администратором информационной системы с последующим уведомлением Администратора безопасности информации.

Электронная почта в отдела образования администрации городского округа Вичуга является средством коммуникации, распределения информации и управления процессами в производственных целях: повышения эффективности труда работников Учреждения и экономии ресурсов.

Корпоративная (внутренняя) электронная почта Учреждения предназначена исключительно для использования в служебных целях.

Использование личной почты в служебных целях запрещено.

Организацией и обеспечением порядка работы электронной почты в Учреждении занимается Администратор информационной системы. Ответственность за использование электронной почты возлагается на работников и руководителей подразделений в рамках их должностных обязанностей.

При работе с корпоративной электронной почтой отдела образования администрации городского округа Вичуга пользователь учитывает следующие принципиальные положения:

– электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;
– внутренняя электронная почта, организованная с применением средств криптографической защиты, является средством передачи информации, обеспечивающим конфиденциальность передаваемой информации. Передача информации ограниченного доступа осуществляется только в зашифрованном или в обезличенном виде.

В Учреждении должно быть обеспечено управление взаимодействием с внешними информационными системами, включающими информационные системы и вычислительные ресурсы (мощности) уполномоченных лиц, информационные системы, с которыми установлено информационное взаимодействие на основании заключенного договора (соглашения), а также с иными информационными системами, информационное взаимодействие с которыми необходимо для функционирования информационной системы.

Управление взаимодействием с внешними информационными системами должно включать:

- предоставление доступа к информационной системе только авторизованным (уполномоченным) пользователям;
- определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;
- определение системных учетных записей, используемых в рамках данного взаимодействия;
- определение порядка предоставления доступа к информационной системе авторизованными (уполномоченным) пользователями из внешних информационных систем;
- определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.

В Учреждении предоставляется доступ к информационной системе авторизованным (уполномоченным) пользователям внешних информационных систем или разрешается обработка, хранение и передача информации с использованием внешней информационной системы при выполнении следующих условий:

- при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;
- при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

3.9. Трансграничная передача персональных данных

При совершении трансграничной передачи персональных данных Учреждение обязано убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

Трансграничная передача персональных данных Учреждением на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

- наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;
- предусмотренных международными договорами Российской Федерации;
- предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;
- исполнения договора, стороной которого является субъект персональных данных;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

3.10. Правила использования ПО и аппаратных средств ИСПДн

Настоящий раздел регламентирует взаимодействие организаций подведомственных отделу образования и отдела образования администрации городского округа Вичуга по обеспечению безопасности информации при проведении модификаций ПО, технического обслуживания и ремонта средств вычислительной техники (СВТ) ИСПДн.

3.10.1. Права на внесение изменений в ПО и аппаратные средства ИСПДн

Все изменения конфигурации ТС и программных средств рабочих станций (АРМ) и серверов ИСПДн, обрабатывающих ПДн, производятся только на основании заявок начальников структурных подразделений, согласованных с Администратором безопасности информации.

Право внесения изменений в конфигурацию программно-аппаратных средств информационных узлов (рабочих станций, серверов) и телекоммуникационного оборудования, обрабатывающего ПДн, предоставляется:

- в отношении системных и прикладных программных средств, а также в отношении аппаратных средств – Администратору информационной системы;
- в отношении программно-аппаратных СЗИ - Администратору безопасности информации и Администратору информационной системы;
- в отношении программно-аппаратных средств телекоммуникаций – Администратору информационной системы.

Изменение конфигурации аппаратно-программных средств защищенных рабочих станций (АРМ) и серверов кем-либо, кроме уполномоченных работников, запрещено.

3.10.2. Порядок внесения изменений в ПО и аппаратные средства ИСПДн

Для внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций ИСПДн начальником структурного подразделения, в котором вносятся изменения, подается заявка на имя Администратора информационной системы, которая им рассматривается и утверждается по согласованию с Администратором безопасности информации.

При необходимости планового проведения изменений (обновлений версий) ПО, заявка выпускается руководителем структурного подразделения и, после согласования с Администратором безопасности информации, направляется Администратору информационной системы.

В заявках могут быть указаны следующие виды необходимых изменений в составе программных и аппаратных средств рабочих станций и серверов подразделения:

- установка в подразделении новой рабочей станции (АРМ) или сервера;
- замена рабочей станции (АРМ) или сервера подразделения;
- изъятие рабочей станции (АРМ) или сервера подразделения;
- добавление устройства (узла, блока) в состав конкретной рабочей станции (АРМ) или сервера подразделения;
- замена устройства (узла, блока) в составе конкретной рабочей станции (АРМ) или сервера подразделения;
- изъятие устройства (узла, блока) из состава конкретной рабочей станции (АРМ) или сервера;

- установка (развертывание) на конкретной рабочей станции (АРМ) или сервере программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данной рабочей станции или сервере);
- обновление (замена) на конкретной рабочей станции (АРМ) или сервере программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);
- удаление с конкретной рабочей станции (АРМ) или сервера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данной рабочей станции).

В заявке указываются условные наименования развернутых рабочих станций (АРМ) и серверов в соответствии с их паспортами. Программные средства указываются в соответствии с перечнем программных средств алгоритмов и программ, которые используются в ИСПДн.

Администратор безопасности информации при согласовании заявки учитывает возможность совмещения решения новых задач (обработки информации) на указанных в заявке рабочих станциях (АРМ) или серверах в соответствии с требованиями по безопасности.

После этого заявка передается Администратору информационной системы для непосредственного исполнения работ по внесению изменений в конфигурацию рабочих станций (АРМ) или серверов ИСПДн.

Руководитель подведомственной организации, в которой установлены аппаратно-программные средства, подлежащие модернизации, допускает Администратора информационной системы и Администратора безопасности информации к внесению изменений в состав аппаратных средств и ПО.

Установка, изменение (обновление) и удаление системных и прикладных программных средств производится Администратором информационной системы.

Если рабочая станция (АРМ) или сервер обрабатывают ПДн, то установка, снятие, и внесение необходимых изменений в настройки СЗИ от НСД и средств контроля целостности файлов на рабочих станциях осуществляется Администратором информационной системы под контролем Администратора безопасности информации. Работы производятся в присутствии пользователя данной рабочей станции.

Подготовка модификаций ПО защищенных серверов и рабочих станций, тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в фонд алгоритмов и программ и другие необходимые действия производится Администратором информационной системы.

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

Модификация ПО на сервере осуществляется Администратором информационной системы по согласованию с Администратором безопасности информации.

После установки модифицированных модулей на сервер Администратор безопасности информации в присутствии Администратора информационной системы устанавливает защиту целостности модулей на сервере (производит пересчет контрольных сумм эталонов модулей на файл-сервере с помощью специальных программных средств, прошедших оценку соответствия).

После проведения модификации ПО на рабочих станциях Администратор информационной системы проводит антивирусный контроль.

Установка и обновление общего ПО (системного, тестового) на рабочие станции (АРМ) и серверы производится с оригинальных лицензионных дистрибутивных носителей (компакт дисков

и др.), полученных установленным порядком, а прикладного ПО - с эталонных копий программных средств, полученных из фонда алгоритмов и программ.

Все добавляемые программные и аппаратные компоненты предварительно проверяются на работоспособность, контроль наличия проверок работоспособности осуществляет Администратор безопасности информации.

После установки (обновления) ПО Администратор информационной системы, а при использовании специализированных СЗИ от НСД - Администратор безопасности информации производят настройку средств управления доступом к данному программному средству и проверяют работоспособность ПО и правильность настройки СЗИ.

После завершения работ по внесению изменений в состав аппаратных средств рабочей станции (АРМ), обрабатывающей ПДн, ее системный блок закрывается Администратором информационной системы на ключ (при наличии штатных механических замков) и опечатывается (пломбируется, защищается специальной наклейкой) с возможностью постоянного визуального контроля за ее целостностью Администратором безопасности информации.

Администратор безопасности информации проводит периодический контроль за опечатыванием узлов и блоков ИСПДн.

На обратной стороне заявки делается отметка о выполнении и исполненная заявка хранится вместе с паспортом данной рабочей станции (сервера).

При изъятии рабочей станции (сервера), обрабатывающей ПДн, из состава рабочих станций (серверов) структурного подразделения ее передача на склад, в ремонт или в другое структурное подразделение для решения иных задач осуществляется только после того, как Администратор безопасности информации снимет с данной рабочей станции (сервера) СЗИ и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется Актом об уничтожении конфиденциальной информации (персональных данных) после затирания остаточной информации, хранившейся на диске компьютера.

Оригиналы заявок (документов), на основании которых производились изменения в составе ТС или программных средств рабочих станций с отметками о внесении изменений в состав программно-аппаратных средств хранятся вместе с оригиналами паспортов рабочих станций (серверов). Они могут быть использованы:

- для восстановления конфигурации рабочих станций (серверов) после аварий;
- для контроля правомерности установки на конкретной рабочей станции (сервере) средств для решения соответствующих задач при разборе конфликтных ситуаций;
- для проверки правильности установки и настройки СЗИ рабочих станций (серверов).

В информационной системе должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе программного обеспечения и (или) его компонентов.

Установка (инсталляция) в информационной системе программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных к установке («белый список»), и (или) перечнем программного обеспечения и (или) его компонентов, запрещенных к установке («черный список»). Указанные перечни программного обеспечения и (или) его компонентов разрабатываются в Учреждении для информационной системы в целом или для всех ее сегментов или устройств в отдельности.

Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов должна осуществляться только от имени Администратора информационной системы.

Администратором информационной системы должен обеспечиваться периодический контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в информационной системе, а также на предмет отсутствия программного обеспечения, запрещенного к установке.

Оператором должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций. Для этого в информационной системе должны быть приняты соответствующие планы по действиям персонала (администраторов безопасности, пользователей) при возникновении нештатных ситуаций.

Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать:

- восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;
- восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;
- возврат информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной системы, определенных оператором, позволяющих решать задачи по обработке информации.

3.11. Требования по обеспечению безопасности при применении средств криптографической защиты информации

Для защиты информации, не содержащей сведений, составляющих государственную тайну, при применении средств криптографической защиты информации (СКЗИ) соблюдаются нормативные требования. Криптографическая защита в ИСПДн отдела образования администрации городского округа Вичуга создаётся на основе сертифицированных СКЗИ, встраивание которых в ИСПДн происходит с выполнением интерфейсных и криптографических протоколов, определенных технической документацией на СКЗИ.

В Учреждении выделяются должностные лица, ответственные за разработку и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ. Вопросы обеспечения функционирования и безопасности СКЗИ отражаются в специально разработанных документах в соответствии с требованиями регуляторов в области защиты информации, утвержденных начальником отдела образования администрации городского округа Вичуга, с учетом эксплуатационной документации на СКЗИ.

К работе с СКЗИ решением начальника отдела образования администрации городского округа Вичуга допускаются работники, обладающие знаниями о правилах его эксплуатации, правилах пользования, об эксплуатационной документации и прошедшие обучение работе с СКЗИ.

Ответственное должностное лицо, уполномоченное на руководство заявленными видами деятельности со средствами СКЗИ, имеет представление о возможных угрозах информации при ее обработке, передаче, хранении, методах и СЗИ.

Охрана и режим в помещениях, в которых размещены СКЗИ (далее помещения), обеспечивают безопасность информации, СКЗИ и криптоключей, сводят к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами.

Порядок допуска в помещения определяется внутренним документом отдела образования администрации городского округа Вичуга.

При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п., окна помещений оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими НСД в помещения. Эти помещения имеют прочные входные двери, на которые устанавливаются надежные замки.

Для хранения криптоключей, нормативной и эксплуатационной документации, инсталлирующих криптосредство носителей, помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Дубликаты ключей от хранилищ и входных дверей хранятся в сейфе ответственного лица, назначаемого начальником отдела образования администрации городского округа Вичуга.

Порядок охраны помещений предусматривает периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.

Размещение и установка СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ. Системные блоки АРМ с СКЗИ оборудуются средствами контроля их вскрытия.

3.12. Регистрация событий безопасности

Для реагирования на события безопасности в информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности.

События безопасности, подлежащие регистрации в информационной системе, должны определяться с учетом способов реализации угроз безопасности для информационной системы. К событиям безопасности, подлежащим регистрации в информационной системе, должны быть отнесены любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов информационной системы, нарушения процедур, установленных организационно-распорядительными документами по защите информации оператора, а также на нарушение штатного функционирования средств защиты информации.

События безопасности, подлежащие регистрации в информационной системе, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИС.

Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в ИС.

Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется Администратором информационной системы исходя из возможностей реализации угроз безопасности информации и фиксируется в Журнале учета мероприятий по контролю режима защиты конфиденциальной информации (персональных данных) и выполнения обязательных процедур.

В информационной системе как минимум подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы;
- подключение машинных носителей информации и вывод информации на носители информации;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;
- попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа.

В информационной системе должны быть определены состав и содержание информации о событиях безопасности, подлежащих регистрации.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее

результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

Сбор, запись и хранение информации о событиях безопасности должен предусматривать:

- возможность выбора Администратором безопасности информации событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности;
- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту);
- хранение информации о событиях безопасности.

Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации, составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

Реагирование на сбои при регистрации событий безопасности должно предусматривать:

- предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
- реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

Администратор безопасности информации и Администратор информационной системы осуществляют мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагируют на них.

Мониторинг (просмотр и анализ) записей регистрации (аудита) проводиться для всех событий, подлежащих регистрации, и с периодичностью, обеспечивающей своевременное выявление признаков инцидентов безопасности в ИС.

В случае выявления признаков ИБ в ИС осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

Администратор информационной системы контролирует синхронизацию системного времени. Применение внутренних системных часов ИС необходимо для получения меток

времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИС.

Информация о событиях безопасности подлежит защите и обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только Администратору безопасности информации и Администратору информационной системы.

3.13. Контроль (анализ) защищенности информации

В Учреждении должны осуществляться выявление (поиск), анализ и устранение уязвимостей в информационной системе. При выявлении (поиске), анализе и устранении уязвимостей в информационной системе должны проводиться:

- выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;
- разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
- анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
- устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;
- информирование должностных лиц оператора (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы. На этапе эксплуатации поиск и анализ уязвимостей проводится с периодичностью, установленной оператором. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в информационной системе.

В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного

обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

В Учреждении должно обеспечиваться использование для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей.

Доступ к функциям выявления (поиска) уязвимостей предоставляется только Администратору безопасности информации.

В Учреждении должен осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода, также должно осуществляться получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

Контроль установки обновлений проводится с установленной периодичностью и фиксируется в соответствующих журналах.

При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты, баз решающих правил систем обнаружения вторжений, баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

В Учреждении должен проводиться контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации, при этом должны осуществляться:

- контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;
- проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации, объем и содержание которой определяется оператором;
- контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;

– восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

При проведении контроля состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация) осуществляется:

– контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;
– контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;
– контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;
– исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляется:

– контроль правил генерации и смены паролей пользователей;
– контроль заведения и удаления учетных записей пользователей;
– контроль реализации правил разграничения доступом;
– контроль реализации полномочий пользователей;
– контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей;
– устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

4. Порядок организации внутреннего обучения работников правилам и мерам защиты ПДн

Решение основных вопросов обеспечения защиты ПДн предусматривает соответствующую подготовку работников. Проведение обучения работников отдела образования администрации городского округа Вичуга позволяет организовать обработку информации в соответствии с требованиями законодательства и нормативно-методических документов в области обеспечения безопасности ПДн при их обработке в ИСПДн и реализовать установленный комплекс организационных и технических мер по защите ПДн.

Систему внутреннего обучения работников в области защиты ПДн составляет:

- проведение инструктажа пользователей ИСПДн;
- самостоятельное изучение работниками Учреждения необходимых для работы документов, средств и продуктов;
- проведение курсов повышения квалификации работников в области защиты персональных данных.

В результате прохождения обучения работники отдела образования получают необходимые знания и навыки в отношении:

- правил использования СЗИ;
- содержания основных нормативных правовых актов, руководящих и нормативно-методических документов в области обеспечения безопасности ПДн при их обработке в ИСПДн;
- основных мероприятий по организации и техническому обеспечению безопасности ПДн при их обработке в ИСПДн.

4.1. Проведение инструктажа пользователей ИСПДн

Пользователи ИСПДн, допущенные к работе с ПДн, обязаны пройти инструктаж по вопросам обеспечения безопасности ПДн с целью подтверждения своих знаний и уяснения своих обязанностей по поддержанию установленного режима защиты ПДн.

Инструктаж представляет собой ознакомление работников отдела образования администрации городского округа Вичуга, допущенных к работе в ИСПДн, с положениями настоящего Положения и действующих нормативных документов по обеспечению безопасности информации при ее обработке в ИСПДн, в том числе и с Инструкцией пользователя ИСПДн.

Ознакомление с положениями нормативной документации работник Учреждения подтверждает своей личной подписью в журнале инструктажа (обучения), что свидетельствует о прохождении инструктажа (обучения).

Контроль проведения инструктажа и периодическая проверка знаний пользователями ИСПДн положений нормативной документации по вопросам обеспечения безопасности ПДн возлагается на Администратора безопасности информации и ответственного за организацию обработки персональных данных в отделе образования администрации городского округа Вичуга совместно с руководителями подведомственных организаций, использующих ИСПДн.

Ответственность за непосредственное проведение инструктажа возлагается на руководителя Учреждения.

Работники отдела образования администрации городского округа Вичуга, не прошедшие инструктаж, к работе в ИСПДн не допускаются. Инструктаж проводится перед началом работы в ИСПДн и вновь принятых на работу работников Учреждения, а также не реже одного раза в год для всех пользователей ИСПДн.

Проверка знаний пользователями ИСПДн положений законодательства Российской Федерации в области персональных данных и нормативных правовых документов по вопросам обеспечения безопасности ПДн проводятся: лицом, назначенным ответственным за организацию обработки персональных данных в отделе образования администрации городского округа Вичуга и Администратором безопасности информации, не реже одного раза в год, а также в ходе периодического контроля, соблюдения режима безопасности информации.

4.2. Самостоятельное изучение

При данном виде подготовки работниками отдела образования администрации городского округа Вичуга, осуществляющими обработку ПДн, самостоятельно изучаются (в части касающейся):

- нормативные правовые документы в области ПДн;
- руководящие и нормативно-методические документы в области обеспечения безопасности ПДн;
- правила (инструкции) по использованию программных и аппаратных СЗИ.
- внутренние положения (локальные акты) отдела образования администрации городского округа Вичуга, устанавливающие порядок обращения с ПДн и их защиты.

Время для самостоятельного изучения определяется начальниками структурных подразделений Учреждения.

5. Ответственность должностных лиц за обеспечение безопасности ПДн, своевременность и качество формирования требований по защите информации, за качество и научно-технический уровень разработки СЗПДн

Ответственность за обеспечение безопасности ПДн распределяется между должностными лицами отдела образования администрации городского округа Вичуга на основании настоящего Положения.

Ответственность за организацию режима обеспечения безопасности ПДн возлагается на руководителя отдела образования администрации городского округа Вичуга и руководителей подведомственных организаций.

Ответственность за своевременность и качество формирования требований по защите ПДн, за качество и научно-технический уровень разработки СЗПДн, а также контроль исполнения правил и требований, направленных на обеспечение безопасности ПДн, возлагается на лицо, ответственное за организацию обработки персональных данных в отделе образования администрации городского округа Вичуга и Администратора безопасности информации.

Ответственность за выполнение обязанностей по обеспечению режима безопасности ПДн, несут начальники соответствующих структурных подразделений, эксплуатирующие ИСПДн,.

Средства информатизации, входящие в состав ИСПДн, закрепляются за ответственными должностными лицами (владельцами). Владельцем средств информатизации может быть начальник структурного подразделения или специально назначаемое должностное лицо. На владельца средств информатизации возлагается ответственность за выполнение установленных мероприятий по защите закрепленных средств информатизации и обрабатываемых ими ПДн.

Должностные лица и работники Учреждения, виновные в нарушении режима защиты ПДн, несут дисциплинарную, гражданскую, административную и уголовную ответственность, предусмотренную законодательством Российской Федерации.

6. Порядок контроля за обеспечением уровня защищенности ПДн и оценки соответствия ИСПДн

Контроль обеспечения требуемого уровня защищенности ПДн заключается в проверке выполнения требований нормативных документов по защите ПДн, а также в оценке обоснованности и эффективности принятых мер. Мероприятия по контролю защищенности ПДн могут проводиться как уполномоченными работниками отдела образования администрации городского округа Вичуга, так и на договорной основе сторонней организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации. Мероприятия по контролю защищенности ПДн и оценке соответствия ИСПДн включают:

- внутренний контроль режима безопасности ПДн (оперативный и периодический);
- обследование защищенности ПДн с привлечением сторонней организации;
- оценку соответствия ИСПДн требованиям безопасности ПДн.

6.1. Внутренний контроль режима безопасности ПДн и оценки соответствия ИСПДн требованиям безопасности ПДн

Внутренний оперативный контроль соблюдения режима безопасности ПДн проводится Администратором безопасности информации ежедневно в режиме «реального времени».

Внутренний контроль заключается в анализе защищенности ПДн посредством используемых в составе ИСПДн программных и программно-аппаратных средств (систем) анализа защищенности.

В ходе проведения контроля соблюдения режима безопасности ПДн Администратор безопасности информации:

- осуществляет анализ лог-файлов, производимых средствами защиты и другими элементами ИСПДн (ОС, прикладные программы);
- просматривает оповещения средств защиты ИСПДн;
- принимает меры по результатам анализа полученных оповещений и лог-файлов.

Внутренний периодический контроль соблюдения режима безопасности ПДн (контрольные обследования защищенности ИСПДн) организуется лицом, ответственным за организацию обработки персональных данных в Учреждении по планам, ежегодно утверждаемым руководителем отдела образования администрации городского округа Вичуга.

По решению руководителя отдела образования администрации городского округа Вичуга внутренний контроль может проводиться во внеочередном порядке в случаях выявления нарушений безопасности ПДн с целью определения причин произошедших нарушений и разработки мер по их устранению.

Внутренний периодический контроль заключается в оценке выполнения требований нормативных документов по обеспечению безопасности ПДн, обрабатываемых в ИСПДн.

В ходе проведения внутреннего периодического контроля проверяются следующие вопросы:

- соответствие состава и структуры программно-технических средств, обрабатывающих защищаемую информацию (ПДн), документированному составу и структуре средств, разрешенных для обработки такой информации;

- знание персоналом руководящих документов, технологических инструкций, предписаний, актов, заключений и уровень овладения персоналом технологией безопасной обработки информации, описанной в этих инструкциях;
- проверка наличия документов, подтверждающих возможность применения технических и программных средств вычислительной техники для обработки ПДн и применения СЗИ (сертификатов соответствия и других документов);
- проверка правильности применения СЗИ;
- проверка выполнения требований по условиям размещения АРМ в рабочих помещениях;
- соответствие реального уровня полномочий по доступу к защищаемой информации (ПДн) различных пользователей установленному в списке лиц, допущенных к обработке ПДн, уровню полномочий;
- знание инструкций по обеспечению безопасности информации пользователями ИСПДн;
- организация хранения носителей ПДн и допуска в помещения, в которых размещены средства обработки и осуществляется обработка ПДн;
- прохождение инструктажа пользователей по вопросам обеспечения безопасности ПДн и выполнение ими установленных требований.

По фактам несоблюдения условий хранения носителей ПДн, использования СЗИ, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, составляется соответствующее заключение, на основе которого впоследствии осуществляется разработка и реализация мер по предотвращению возможных опасных последствий подобных нарушений.

Результаты контроля оформляются Актом, в котором делаются выводы о состоянии обеспечения безопасности ПДн на проверяемом объекте информатизации и приводятся рекомендации по его совершенствованию.

6.2. Обследование защищенности ПДн внешней специализированной организацией

Обследование защищенности ПДн внешней специализированной организацией проводится при создании ИСПДн (формирование требований к защите информации, содержащейся в информационной системе) или при доработке (модернизации) СЗПДн в случае, если:

- изменился состав или структура ИСПДн или технические особенности её построения (состав или структура ПО, ТС обработки ПДн, топологии и т.п.);
- изменился состав угроз безопасности ПДн;
- изменился класс защищённости ИС.

Обследование защищенности ПДн внешней специализированной организацией проводится по решению руководителя отдела образования администрации городского округа Вичуга.

Привлекаемая для проведения обследования внешняя специализированная организация обязана иметь лицензию на деятельность по технической защите информации.

6.3. Порядок оценки соответствия ИСПДн требованиям безопасности ПДн

Оценка соответствия ИСПДн требованиям безопасности ПДн проводится в форме проверки готовности СЗИ к использованию.

Проверка готовности СЗИ к использованию осуществляется в ходе приемо-сдаточных испытаний СЗПДн с составлением протоколов проверки и заключений о возможности их эксплуатации.

Для проверки готовности СЗИ к использованию или для проведения аттестации ИСПДн, привлекается организация, имеющая лицензию ФСТЭК России на право деятельности по технической защите конфиденциальной информации в соответствии с постановлением Правительства Российской Федерации от 03.02.2012 № 79.

Проверка готовности СЗИ к использованию проводится в соответствии с разрабатываемой программой и методикой испытаний соответствующих СЗИ, определяющих порядок проверки выполнения СЗИ заявленных функций защиты.

Аттестация проводится в соответствии с действующими нормативными и методическими документами ФСТЭК России.

Порядок подготовки и проведения аттестации ИСПДн определяется в приказах (распоряжениях) руководителя отдела образования администрации городского округа Вичуга.