|  |  |
| --- | --- |
|  | УТВЕРЖДЕНА  приказом № \_\_\_\_\_\_\_\_\_\_\_\_\_\_  от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |

|  |
| --- |
| ИНСТРУКЦИЯ по организации защиты информации  в информационных системах персональных данных |

# Содержание

[Термины и определения 48](#_Toc448304798)

[1. Общие положения 52](#_Toc448304799)

[2. Ответственность за нарушение безопасности информации 52](#_Toc448304800)

[3. Цель и задачи защиты информации 52](#_Toc448304801)

[4. Объекты и мероприятия защиты информации 52](#_Toc448304802)

[5. Основные методы защиты информации 54](#_Toc448304803)

[6. Руководство защитой информации 54](#_Toc448304804)

[7. Задачи Учреждения и должностных лиц 54](#_Toc448304805)

[8. Задачи пользователя 55](#_Toc448304806)

[9. Задачи и мероприятия защиты информации от несанкционированного доступа 56](#_Toc448304807)

[10. Средства защиты информации от несанкционированного доступа 57](#_Toc448304808)

[11. Мероприятия защиты информации от несанкционированного доступа 57](#_Toc448304809)

[11.1 Работа с персоналом 57](#_Toc448304810)

[11.2 Оборудование помещений для размещения средств обработки информации 58](#_Toc448304811)

[11.3 Учет ресурсов и авторизация пользователей 58](#_Toc448304812)

[11.4 Межсетевые экраны 58](#_Toc448304813)

[12. Защита активного сетевого оборудования и рабочих станций 59](#_Toc448304814)

[13. Системы безопасности зданий (помещений) 59](#_Toc448304815)

[13.4 Охранная сигнализация 60](#_Toc448304816)

[13.5 Пожарная сигнализация 60](#_Toc448304817)

[14. Авторизация пользователей 60](#_Toc448304818)

[15. Действия при компрометации аутентификатора или парольной информации 61](#_Toc448304819)

# Термины и определения

**Автоматизированная информационная система (АИС)** – комплекс программных, технических, информационных, лингвистических, организационно-технологических средств и персонала, предназначенный для сбора, (первичной) обработки, хранения, поиска, (вторичной) обработки и выдачи данных в заданной форме (виде) в целях решения разнородных профессиональных задач пользователей системы.

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

**Авторизация** – предоставление доступа к защищаемому ресурсу в соответствии с уровнем полномочий;

**Адаптивность** – способность АИС изменяться для сохранения своих эксплуатационных показателей в заданных пределах при изменениях условий;

**Администратор защиты информации** – лицо, ответственное за выполнение мероприятий защиты информации, обрабатываемой техническими средствами;

**Архивирование** – 1) запись на отчуждаемый носитель данных информационного ресурса со специальным преобразованием в целях сокращения занимаемого ими места на носителе; 2) реализация процесса хранения резервных копий информационных ресурсов в целях исключения потери их функциональности;

**Архивированная копия** – копия ресурса, полученная путем его копирования с архивированием;

**Архивная копия** – копия ресурса, находящаяся на хранении в архиве, специальном хранилище;

**Аутентификация** – процесс проверки принадлежности субъекту доступа предъявленного им идентификатора; т.е. проверка подлинности пользователя с помощью предъявляемого им идентификатора;

**Аутентичность** – свойство данных (информации), выражающееся в том, что они были созданы законными участниками информационного процесса, и что они не подверглись искажениям (случайным или преднамеренным);

**Безопасность информации** – состояние защищенности информации от внешних и внутренних угроз, характеризуемое способностью персонала, технических средств и информационных технологий обеспечить конфиденциальность, доступность и целостность информации при ее обработке.

**Вредоносная программа** – специальная компьютерная программа (троянская, вирус, червь, шпион и т.п.), последовательность инструкций или иной специальный код, предназначенные или приспособленные для несанкционированного запуска на вычислительном средстве в целях не предусмотренного технологией авторизованной обработки информации воздействия на доступные этому средству ресурсы. На практике вредоносными программами признаются: компьютерные вирусы, черви, троянские программы, программы-маскировщики (руткиты), сканеры (эксплоиты) уязвимостей, программы-шпионы (spyware-программы);

**Вскрытие корпуса устройства** – разъем конструктивных деталей корпуса устройства, открывающий доступ к накопителю информации;

**Данные** – информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека;

**Дифференциальное (дифференцированное) копирование** – копирование, при котором копируются только данные, измененные co времени последнего создания полной копии. Дифференциальные копии (архивы) имеют меньшие размеры и быстрее создаются. Для восстановления ресурса из дифференциальной копии необходима полная копия;

**Документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

**Доступ к информации** – возможность получения информации и ее использования;

**Доступность информации** – состояние информации, характеризуемое способностью автоматизированной системы обеспечить беспрепятственный доступ к информации субъектов, имеющих на это полномочия;

**Дублирование** – создание (реализация для целей хранения) информационного ресурса аутентичного дублируемому ресурсу, на другом программно-аппаратном комплексе;

**Живучесть АИС** – свойство AИC, характеризуемое способностью выполнять установленный объем функций в условиях воздействий внешней среды и отказов компонентов системы в заданных пределах;

**Защита информации** – принятие правовых, организационных и технических мер, направленных на: обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении информации; соблюдение конфиденциальности информации ограниченного доступа и реализацию права на доступ к информации;

**Идентификатор** – уникальный признак субъекта или объекта доступа;

**Идентификация** – присвоение объектам и субъектам доступа идентификатора и/или проверка наличия предъявляемого идентификатора в перечне присвоенных идентификаторов;

**Имя пользователя** – идентификатор, представляющий последовательность символов установленного формата;

**Инкрементное (инкрементальное) копирование** – копирование, при котором копируются только данные, измененные co времени последнего создания полной или инкрементной копии. Инкрементные копии (архивы) имеют меньшие размеры и быстрее создаются. Для восстановления ресурса из инкрементной копии необходимы все предыдущие инкрементные копии и полная копия;

**Информационно-телекоммуникационная сеть (корпоративная сеть передачи данных)** – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

**Информация** – сведения (сообщения, данные) независимо от формы их представления;

**Контролируемая зона (КЗ)** – пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств. Границей контролируемой зоны могут являться периметр охраняемой территории организации или ограждающие конструкции охраняемого здания или его части;

**Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

**Копирование** – запись данных оригинала информационного ресурса или его фрагмента на съемный (отчуждаемый) носитель информации;

**Копирование с архивированием** – запись данных оригинала информационного ресурса или их фрагментов на съемный (отчуждаемый) носитель информации со специальным преобразованием данных в целях сокращения занимаемого ими места на носителе;

**Копия ресурса** – съемный (отчуждаемый) носитель информации (комплект однотипных носителей), содержащий информацию ресурса, аутентичную по состоянию на момент записи оригиналу (информации хранящейся в АИС);

**Машинный носитель информации (носитель информации, носитель)** – специальный вещественный энергонезависимый объект, предназначенный для записи на него информации и ее хранения (с возможностью последующего чтения) посредством средств вычислительной техники, или конструктивно законченное устройство, содержащее в своем составе такой объект;

**Межсетевой экран** – локальное или функционально распределенное программное (программно-аппаратное) средство, реализующее контроль пакетов, поступающих на компьютер и/или выходящих с него в рамках определенных протоколов;

**Несанкционированный доступ к информации** – 1) получение защищаемой информации субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; 2) доступ к информации или ее носителям с нарушением установленных правил доступа к ним.

**Носитель информации однократной записи** – носитель информации, позволяющий в процессе эксплуатации однократно произвести полнообъемную (т.е. в размере полной заявленной производителем информационной емкости) запись информации;

**Носитель информации ограниченного доступа** – носитель информации, учтенный в «Журнале учета машинных носителей информации» и предназначенный для хранения информации ограниченного доступа (конфиденциальной информации);

**Обработка информации в АС** – совокупность операций (сбор, накопление, хранение, преобразование, отображение, выдача и т.п.) осуществляемых над информацией (сведениями, данными) с использованием средств АС;

**Объект доступа** – информационный ресурс автоматизированной системы, доступ к которому регламентирован;

**Оригинал ресурса** – информационный ресурс, хранящийся в АИС (в памяти аппаратно-программного комплекса);

**Отчуждаемый носитель [информации]** – см. съемный носитель;

**Пароль** – назначаемый (присваиваемый) аутентификатор пользователя, представляющий собой группу символов определенной длины, являющийся секретом пользователя и служащий для подтверждения принадлежности предъявленного идентификатора (имени пользователя) обращающемуся пользователю;

**Парольная документация** – документы, предназначенные для обеспечения функционирования системы аутентификации пользователей;

**Перезаписываемый носитель информации** – носитель информации, позволяющий многократно (более одного раза) производить полнообъемную (то есть в размере полной заявленной производителем информационной емкости) запись информации;

**Полное копирование** – копирование ресурса в полном объеме его данных;

**Пользователь** – субъект доступа, обращающийся к информационной системе в целях получения информации и/или воздействия на нее;

**Предоставление информации** – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

**Применение носителей информации** – процессы учета, хранения, использования по назначению, списания и уничтожения носителей информации, т.е. стадия жизненного цикла носителя информации от его приобретения до уничтожения (утилизации);

**Профайл** – объект операционной системы серверов iSeries (i5)(AS/400), описывающий уровень полномочий субъекта доступа;

**Распространение информации** – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

**Ресурс [информационный]** – отдельный документ и отдельный массив документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

**Системный администратор** – лицо или подразделение, осуществляющее администрирование (техническое управление) вычислительной системой;

**Субъект доступа** – лицо или процесс, действия которого регламентируются правилами разграничения доступа;

Примечание. Субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может выступать: юридическое лицо; группа физических лиц, в том числе общественная организация; отдельное физическое лицо;

**Съемный носитель [информации]** – носитель информации, технология применения которого предусматривает его включение в работу автоматизированной системы и/или выключение из работы автоматизированной системы без ее остановки, а также носитель, извлекаемый из корпуса устройства без его (корпуса) вскрытия;

**Тиражирование копии** – размножение съемного (отчуждаемого) носителя (комплекта носителей) информации, содержащего копию ресурса, путем копирования этого носителя;

**Тиражирование ресурса** – запись ресурса (или его фрагмента) на съемный носитель с последующим их перемещением в целях обеспечения автоматизированной обработки вне Учреждения.

**Угроза безопасности информации** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее;

**Уровень полномочий** – совокупность прав доступа субъекта доступа;

**Устойчивость** – комплексное свойство автоматизированной системы, характеризуемое ее живучестью, помехоустойчивостью и надежностью;

**Целостность информации** – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения);

**Энергонезависимый объект** – объект, не требующий подвода энергии для обеспечения своих функций по хранению информации или содержащий автономный источник энергии.

# 1. Общие положения

1.1 Настоящая инструкция по организации защиты информации в информационных системах персональных данных (далее – Инструкция) определяет цели и основные задачи защиты информации информационных систем персональных данных, основные требования и единый порядок ее организации в ФГБОУВО «Белгородский государственный технологический университет им. В.Г. Шухова» (далее – Учреждение).

1.2 Нормативной базой Инструкции являются федеральное законодательство, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, а также нормативные документы Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации.

# 2. Ответственность за нарушение безопасности информации

2.1 Инструкция является нормативным документом Учреждения, обязательным для выполнения (в части касающейся) всеми сотрудниками Учреждения.

2.3 Сотрудники, виновные в нарушении безопасности ИСПДн, могут быть привлечены к административной или уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

# 3. Цель и задачи защиты информации

3.1 Целью защиты информации ИСПДн является достижение их безопасности, то есть состояния защищенности информации от внешних и внутренних угроз, характеризуемого способностью персонала, технических средств и информационных технологий обеспечить в процессе обработки ее конфиденциальность, целостность, доступность.

3.2 Защите подлежит вся циркулирующая в ИСПДн информация. Методы и меры защиты ресурсов определяются дифференцированно, исходя из их важности, особенностей реализации и использования. Защита общедоступной информации производится только в целях обеспечения ее целостности, доступности.

3.3 Цель защиты информации ИСПДн достигается решением следующих задач:

* реализация комплекса мер по предотвращению противоправного получения информации или ее несанкционированной передачи (распространения);
* своевременное обнаружение фактов несанкционированного доступа к информации и предотвращение неавторизованного (неполномочного) воздействия на информационные ресурсы;
* недопущение воздействия на технические средства обработки и хранения информации, нарушающего их функционирование;
* предупреждение неблагоприятных последствий нарушения порядка доступа к информации;
* обеспечение восстановления в приемлемые сроки информации после не предусмотренной технологией ее обработки, модификации, в том числе уничтожения.

# 4. Объекты и мероприятия защиты информации

4.1 Защите подлежат:

* техническое и программное обеспечение ИСПДн;
* информационно-телекоммуникационная сеть (КСПД);
* информационные ресурсы, представленные в виде носителей на различной физической основе, информативных физических полей, информационных массивов и баз данных;
* помещения, в которых размещаются носители или средства обработки защищаемой информации;
* все технические средства и системы, размещенные в помещениях, в которых обрабатывается (циркулирует) информация ограниченного доступа;
* система защиты информации.

4.2 Выполнение задач защиты информации в ИСПДн обеспечивается организацией эффективной системы защиты информации – комплексным применением организационных и технических (программно и аппаратно реализуемых) мероприятий:

* созданием системы нормативных (руководящих) документов по организации защиты;
* четким распределением ответственности по обеспечению защиты информации между должностными лицами и работниками;
* установлением персональной ответственности работников за обеспечение безопасности обрабатываемой информации;
* организацией выполнения подразделениями, должностными лицами и работниками требований нормативных документов по защите информации;
* юридической защитой безопасности информации при ее предоставлении сторонним организациям;
* своевременным выявлением угроз безопасности информации и принятием соответствующих мер защиты;
* дифференцированием мер защиты в зависимости от степени угрозы и важности объекта защиты;
* комплексным применением программно и аппаратно реализованных средств защиты информации от несанкционированного доступа к ней и от специальных воздействий на информационные ресурсы в целях их уничтожения, искажения, блокирования или фальсификации;
* регламентированием порядка применения средств ввода-вывода информации и контролем его выполнения;
* содержанием актуальных резервных копий информационных ресурсов;
* применением прикладных программных продуктов, отвечающих требованиям обеспечения защиты информации;
* организацией контроля доступа в помещения и здания Учреждения, их охраной в нерабочее время;
* проведением аттестации ИСПДн на соответствие требованиям по защите информации, установленными государственными регуляторами;
* систематическим анализом безопасности информации и совершенствованием системы её защиты;
* эффективной противопожарной защитой;
* приданием мероприятиям защиты информации характера обязательных элементов производственного процесса, а требованиям по их исполнению – элементов производственной дисциплины;
* глубоким знанием и пониманием работниками требований безопасности информации.

4.3 Применение технических средств защиты информации в Учреждении основано на принципах безопасности, правомочности и эффективности. Используемые средства должны соответствовать требованиям всех указанных принципов.

4.4 Безопасность. Применяемые технические средства защиты должны иметь сертификат компетентных государственных органов (организаций):

отсутствия деструктивного воздействия на защищаемую информацию или возможности их использования для такого воздействия;

обеспечения требуемого уровня защищенности.

4.5 Правомочность. Для обеспечения защиты информации Учреждения используются лицензированные или свободно распространяемые программные средства.

4.6 Эффективность. Защита информации должна обеспечивать положительный результат, соотносимый с затратами ресурсов на ее реализацию.

# 5. Основные методы защиты информации

5.1 В Учреждении комплексно применяются организационные и технические методы защиты информации ИСПДн.

5.2 К числу основных организационных и технических мер защиты информации, применяемых в Учреждении, относятся:

* идентификация и аутентификация субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* защита машинных носителей информации;
* регистрация событий безопасности;
* антивирусная защита;
* контроль (анализ) защищенности информации;
* защита технических средств;
* защита информационной системы, ее средств, систем связи и передачи данных;
* управление конфигурацией информационной системы и системы защиты персональных данных.

# 6. Руководство защитой информации

6.1 В Учреждении ответственность за организацию и выполнение мероприятий по обеспечению защиты информации в ИСПДн возлагается на руководителя Учреждения.

6.2 Методическое руководство, организация мероприятий по защите информации в ИСПДн, эксплуатация технических средств защиты, а также контроль безопасности информации возлагается на ответственного за обеспечение безопасности персональных данных (далее - администратор по защите информации).

6.3 Практическая реализация мероприятий по защите информации в ИСПДн осуществляется работниками в соответствии с их должностными полномочиями и обязанностями.

# 7. Задачи Учреждения и должностных лиц

7.1 Подразделениями информационных технологий (администратором ИСПДн) обеспечивается:

* внедрение и сопровождение технических и программных (общесистемных и прикладных) средств, удовлетворяющих требованиям безопасности информации;
* выполнение процедур обеспечения целостности информации ИСПДн;
* включение в разрабатываемую проектную документацию ИСПДн разделов по защите информации;
* обеспечение устойчивости и адаптивности ИСПДн, организационной и информационной совместимости ее подсистем и элементов;
* отражение вопросов защиты информации в документации по приемке технологий и приложений в эксплуатацию и при организации фонда алгоритмов и программ Учреждения;
* выбор (разработка) программных средств, удовлетворяющих требованиям настоящей Инструкции и других нормативных документов по защите информации;
* обеспечение соответствия информационно-телекоммуникационной системы Учреждения требованиям безопасности информации;
* содержание фонда алгоритмов и программ Учреждения.

7.2 Администратором по защите информации обеспечивается:

* организация выполнения практических мероприятий по защите информации ИСПДн и информационно-телекоммуникационной сети Учреждения;
* разработка нормативных документов по обеспечению защиты информации;
* организация разграничения допуска и обеспечение доступа работников к защищаемой информации в соответствии с их правами;
* организация и обеспечение криптографической защиты информации;
* организация и обеспечение антивирусной защиты;
* организация защиты конфиденциальной информации от НСД;
* анализ состояния безопасности информации и выработка рекомендаций по совершенствованию системы защиты информации;
* учет защищаемых ресурсов, средств защиты и машинных носителей информации в Учреждении;
* контроль применения машинных носителей информации;
* контроль функционирования средств защиты информации;
* организация закупки средств защиты информации, а также услуг по обеспечению защиты информации в соответствии с бюджетом Учреждения;
* организация и выполнение работ по внедрению технических средств защиты информации;
* организация работ по аттестации ИСПДн, помещений, специальных исследований и специальных проверок технических средств;
* согласование технических решений при проектировании систем охранной и пожарной сигнализации, разграничения, контроля доступа и видеонаблюдения зданий (помещений), участие в приеме в эксплуатацию;
* выявление и блокирование каналов возможной утечки конфиденциальной информации.

# 8. Задачи пользователя

8.1 На пользователя средств и ресурсов ИСПДн возлагается:

* выполнение в объеме должностных полномочий и обязанностей требований нормативных (руководящих) документов по защите информации;
* соблюдение конфиденциальности информации, правил пользования носителями (документами), содержащими конфиденциальную информацию, порядка их учета, хранения и уничтожения, исключение всеми имеющимися средствами доступа к конфиденциальной информации посторонних лиц;
* ознакомление только с той информацией (документами), содержащими конфиденциальную информацию, к которым получен доступ в силу исполнения прямых служебных обязанностей;
* защита целостности и доступности пользовательских информационных ресурсов;
* своевременное информирование непосредственного руководителя о возникновении предпосылок к нарушению конфиденциальности информации и о фактах нарушения, ставших ему известными;
* использование только программных продуктов, включенных в перечень разрешенного для использования прикладного программного обеспечения ИСПДн.

8.2 При работе с конфиденциальной информацией пользователю ЗАПРЕЩАЕТСЯ:

* использовать сведения конфиденциального характера в неслужебных целях, в разговорах с лицами, не имеющим отношения к этим сведениям, либо в других ситуациях, не связанных с выполнением служебных обязанностей;
* выносить документы и другие носители информации, содержащие сведения конфиденциального характера и выполнять работы, связанные со сведениями конфиденциального характера, вне служебных помещений Учреждения без разрешения руководителя структурного подразделения;
* использовать сведения конфиденциального характера при ведении переговоров в телефонной сети и по незащищенным каналам связи (в том числе передавать конфиденциальную информацию по электронной почте без применения средств криптографической защиты);
* использовать сведения конфиденциального характера в открытой переписке, статьях и выступлениях;
* снимать копии с документов и служебной информации, содержащей сведения конфиденциального характера, или производить выписки из них, а также использовать различные технические средства (фото-, видео-, и звукозаписывающую аппаратуру) для записей сведений конфиденциального характера без разрешения руководителя своего структурного подразделения;
* работать с неучтенными машинными носителями информации;
* записывать игровые и обучающие программы на любые служебные машинные носители информации;
* уничтожать, копировать или производить какие-либо действия над информацией, программным обеспечением, и базами данных других пользователей без разрешения руководителя своего структурного подразделения, если это не определено функциональными обязанностями;
* хранить парольную документацию и личные карточки с паролями в открытом виде, в местах, доступных для обозрения (на дисплеях ПЭВМ, на рабочих столах и т.д.) другими работниками и посторонними лицами.

# 9. Задачи и мероприятия защиты информации от несанкционированного доступа

9.1 Цели защиты информации от несанкционированного доступа (далее – НСД) достигаются решением следующих задач:

* разграничение прав доступа к информации;
* предотвращение неавторизованного (неполномочного) воздействия на информацию как в режиме реального времени (вторжение), так и посредством вредоносных программ (заражение, закладка);
* обеспечение возможности восстановления информации после непредусмотренной технологией обработки модификации, в том числе уничтожения;
* организация безопасного обращения носителей информации;
* недопущение несанкционированного проникновения в помещения и воздействия на технические средства обработки и хранения информации, нарушающего режимы их функционирования;
* минимизация возможности перехвата информации или ее съема посредством побочных излучений и полей.

9.2 Основными мероприятиями защиты информации от НСД и вредоносных программ в Учреждении являются:

* учет защищаемых ресурсов;
* минимизация перечня лиц, допущенных к защищаемой информации, и разграничение их прав доступа;
* авторизация пользователей информационных ресурсов и вычислительных средств;
* управление правами и привилегиями пользователей, разграничение доступа пользователей информационной системы на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил;
* контроль конфигурации вычислительных средств и их программного обеспечения;
* организация учета и безопасного хранения носителей информации;
* сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе и их анализ;
* организация защиты от вредоносных программ;
* обнаружение (предотвращение) вторжений в ИСПДн;
* создание и организация безопасного хранения резервных копий (дубликатов) информационных ресурсов ИСПДн;
* пропускная система допуска работников и посетителей в здания;
* ограничение доступа работников в помещения, в которых размещаются хранилища информации и средства ее обработки;
* создание контролируемых зон, оборудование зданий и помещений элементами и системами безопасности и контроля.

# 10. Средства защиты информации от несанкционированного доступа

10.1 Для обеспечения защиты информации от несанкционированного доступа и вредоносных программ применяются встроенные и специализированные технические (аппаратные и программные) средства защиты.

10.2 К встроенным средствам защиты относятся такие средства защиты, механизмы которых являются неотъемлемой частью функциональных программ (системных и прикладных) и реализуют их дополнительную функцию – обеспечение защиты обрабатываемой информации.

10.3 К специализированным средствам защиты относятся такие средства защиты, основным функциональным назначением которых является обеспечение безопасности информации.

10.4 Встроенные и специализированные средства защиты могут использоваться совместно.

10.5 При организации защиты ИСПДн от несанкционированного доступа к информации и вредоносных программ учитывается фактор наличия в корпоративной сети вычислительной техники низкой производительности (морально устаревшей).

10.6 Основными специализированными средствами защиты, применяемыми для защиты от несанкционированного доступа к информации и вредоносных программ, являются:

* антивирусные комплексы;
* межсетевые защитные (фильтрующие) экраны;
* средства мониторинга состояния объектов защиты;
* средства авторизации пользователей;
* средства криптографической защиты информации;
* средства блокирования устройств и портов вычислительных систем;
* средства гарантированного уничтожения информации на носителях;
* средства охранной, пожарной сигнализации, видеоконтроля и контроля доступа.

# 11. Мероприятия защиты информации от несанкционированного доступа

## 11.1 Работа с персоналом

11.1.1 В целях придания мероприятиям защиты информации характера обязательных элементов производственного процесса Учреждения требования по обеспечению защиты информации от несанкционированного доступа и вредоносных программ вменяются в обязанность всем пользователям вычислительной техники.

11.1.2 Придание требованиям по исполнению мероприятий по защите информации в ИСПДн от несанкционированного доступа и вредоносных программ характера элементов производственной дисциплины обеспечивается включением их в должностные обязанности всех работников, а также взятием с каждого принимаемого на работу в Учреждение работника письменного обязательства о соблюдении конфиденциальности информации.

11.1.3 Понимание и знание работниками Учреждения требований политики безопасности информации обеспечивается:

* своевременным изучением работниками под подпись требований нормативных документов и корректировкой их функциональных и должностных инструкций;
* регулярным проведением с работниками занятий по вопросам защиты информации;
* приобщением обязательств о соблюдении конфиденциальности информации, к личным делам работников.

11.1.4 Ответственность за своевременное доведение требований нормативных (руководящих) документов до работников, проведения занятий по вопросам защиты информации возлагается на непосредственных руководителей.

11.1.5 Ответственность за организацию занятий с работниками возлагается на руководителя Учреждения.

## 11.2 Оборудование помещений для размещения средств обработки информации

11.2.1 Средства обработки конфиденциальной информации размещаются в помещениях, оборудование которых обеспечивает предотвращение бесконтрольного использования размещенных средств, возможность хищения носителей информации, визуальную досягаемость для посторонних лиц отображаемой информации. Помещения оборудуются прочными дверями с замками и устройствами для опечатывания или устройствами, гарантирующими надежное их закрытие и контроль вскрытия.

11.2.2 Помещения, в которых размещаются средства обработки информации, оборудуются аппаратурой обеспечения требуемого температурно-влажностного режима.

11.2.3 При использовании автоматизированной системы контроля и управления доступом в технологические помещения применяются электромеханические нормально закрытые замки или электромагнитные замки с резервируемым питанием.

11.2.4 Помещения цокольного, первого, последнего этажей, помещения других этажей, примыкающие к карнизам, балконам, пожарным лестницам и т.п. должны иметь три рубежа технической охраны или прочные распашные металлические решетки и два рубежа охраны. В случае сдачи здания Учреждения на пульт централизованного наблюдения (ПЦН), необходимо руководствоваться требованиями вневедомственной охраны по оборудованию техническими средствами.

11.2.5 По окончании рабочего времени закрытые помещения сдаются под охрану установленным в Учреждении порядком.

11.2.6 Допуск работников, в помещения, в которых размещены средства обработки информации ограниченного доступа, не связанных непосредственно с их обслуживанием и обработкой информации, производится в сопровождении ответственных за обработку информации работников.

## 11.3 Учет ресурсов и авторизация пользователей

11.3.1 Защищаемые ресурсы Учреждения определяются «Перечнем защищаемых информационных ресурсов», который утверждается руководителем Учреждения.

11.3.2 Доступ к защищаемому ресурсу ИСПДн обеспечивается минимально необходимому для выполнения производственных задач числу сотрудников, определяемому «Матрицей доступа к информационной системе персональных данных».

11.3.3 «Матрицей доступа к информационной системе персональных данных» определяются разрешенные режимы работы пользователей и уровни доступа.

11.3.4 Авторизация пользователей и информационных ресурсов производится на основании положительных результатов аутентификации. Не допускается авторизация неаутентифицированных пользователей.

11.3.5 По возможности используется двухфакторная аутентификация пользователей. Двухфакторная аутентификация организуется в первую очередь при организации доступа к конфиденциальной информации.

## 11.4 Межсетевые экраны

11.4.1 Межсетевые экраны в Учреждении применяются как для ограничения или запрещения доступа узлов (хостов) внешней сети к устройствам внутренней сети, так и для ограничения доступа узлов внутренней сети к сервисам внешней сети, а также для защиты и изоляции приложений, сервисов и устройств во внутренней сети от нежелательного трафика.

11.4.2 Межсетевой экран устанавливается в «разрыв» канала связи между внутренней сетью Учреждения и внешней информационно-телекоммуникационной сетью или между сегментами внутренней сети и контролирует (фильтрует) весь проходящий через него трафик.

11.4.3 Фильтрация трафика организуется, как правило, в соответствии с разрешительным принципом, то есть путем явного указания разрешенного для пропускания трафика и блокирования всего остального.

11.4.4 Устройства с выходом в Интернет располагаются в сегменте сети, отделенном от устройств, выход которых в Интернет запрещен, межсетевым экраном.

11.4.5 Допускается в целях ограждения узлов (сегментов) ЛВС от нежелательного внутреннего сетевого трафика использование фильтрации в соответствии с запретительным принципом, при котором межсетевым экраном не пропускается только соответствующий правилу трафик.

11.4.6 Для сокрытия схемы внутренней сети от внешнего наблюдателя используется прокси-сервер или предоставляемый межсетевым экраном режим трансляции сетевых адресов, позволяющий подменять IP-адреса пакетов, проходящих через него.

# 12. Защита активного сетевого оборудования и рабочих станций

12.1 В целях контроля конфигурации средств вычислительной техники для каждого хоста (узла) сети фиксируется состав устройств и программного обеспечения на момент ввода его в эксплуатацию и все изменения, вносимые в процессе эксплуатации.

12.2 Учет состояния средств вычислительной техники ведется вручную или с использованием специальных программных продуктов.

12.3 Защищаемые компьютеры настраиваются на обеспечение:

* защиты входа в настройку базовой системы ввода-вывода (BIOS) паролем;
* использования в качестве первого загрузочного устройства накопителя на жестком магнитном диске;
* исключения входа в систему без пароля;
* отсутствия привилегий администратора системы у остальных пользователей вычислительного средства;
* отсутствия консоли восстановления системы.

12.4 В целях исключения бесконтрольного вскрытия корпус компьютера опечатывается путем соединения разъемных деталей специальными легко разрываемыми наклейками или пломбируется.

12.5 Диски горячей замены серверов или закрывающие доступ к ним панели также опечатываются.

12.6 Использование функций вывода информации всех, не требующихся для непосредственного выполнения функций автоматизированного рабочего места, устройств рабочей станции блокируется с помощью специального программного обеспечения. При отсутствии программных средств защиты блокировка портов производится контрольными наклейками.

12.7 Для защиты рабочих станций применяются программно-аппаратные средства, обеспечивающие защиту устройств и информационных ресурсов от несанкционированного доступа посредством выполнения контрольных процедур: аутентификации пользователя, проверки целостности программных средств компьютера.

12.8 Доступ в помещения с активным сетевым оборудованием ограничивается.

# 13. Системы безопасности зданий (помещений)

13.1 В целях защиты от несанкционированного доступа к информации в Учреждении определена контролируемая зона.

13.2 Охрана контролируемой зоны организуется в целях предотвращения доступа в нее посторонних лиц, а также создания надежных препятствий для несанкционированного проникновения в помещения Учреждения и хранилища носителей информации.

13.3 В целях повышения эффективности охраны здания, при необходимости, помещения Учреждения оборудуются системами безопасности:

* системой пожарной сигнализации;
* системой охранной сигнализации;

## 13.4 Охранная сигнализация

13.4.1 Охранная сигнализация предназначается для обеспечения своевременного выявления попыток несанкционированного проникновения в помещения и выдачи сигнала тревоги в случае несанкционированного проникновения в помещение, находящееся под охраной.

13.4.2 Охранная сигнализация должна обеспечить надежное и быстрое срабатывание извещателей с достаточной для принятия немедленных мер локализацией места проникновения, самодиагностику и возможность работы от автономного источника электроэнергии.

13.4.3 Системой охранной сигнализации обязательно оборудуются:

* все входы в здание, в том числе запасные, чердачные люки и вентиляционно-технологические проемы;
* помещения, в которых размещаются средства обработки и хранения информации ограниченного доступа (конфиденциальной информации);
* помещения, в которых размещаются хранилища носителей информации ограниченного доступа;
* помещение администратора по защите информации.

## 13.5 Пожарная сигнализация

13.5.1 Здания Учреждения оборудуются системами пожарной сигнализации в целях своевременного обнаружения очага возгорания и своевременного принятия мер по тушению пожара.

13.5.2 Пожарная сигнализация должна обеспечить надежное и быстрое срабатывание извещателей с достаточной для принятия немедленных мер по локализации места возникновения пожара, самодиагностику и возможность работы от автономного источника электроэнергии.

13.5.3 При повседневном режиме электроснабжения система пожарной сигнализации должна функционировать круглосуточно (непрерывно).

13.5.4 Устанавливаемое оборудование и сети систем должны быть безопасны при эксплуатации для лиц, соблюдающих правила обращения с ними.

# 14. Авторизация пользователей

14.1 К работе с защищаемым ресурсом допускается только определенный круг пользователей, в соответствии с должностными инструкциями.

14.2 Идентификация пользователя производится присвоением ему имени пользователя (код пользователя) – уникальной символьной последовательности.

14.3 Аутентификация пользователя производится посредством сравнения предъявляемого ими аутентификатора с аутентификатором, поставленным в однозначное соответствие предъявленному идентификатору (имени пользователя).

14.4 В качестве аутентификатора пользователя ИСПДн используется пароль (случайная уникальная символьная последовательность) или сертификат, которые вводятся в ПК с клавиатуры или считываются из индивидуального аутентификатора.

14.5 Аутентификация пользователя выполняется при:

* входе в систему;
* обращении к ресурсам.

14.6 Авторизация пользователей производится при положительном результате аутентификации.

14.7 Смена аутентификаторов, вводимых с клавиатуры, выполняется один раз в три месяца. Смена аутентификаторов, которые хранятся и предъявляются системе аутентификации посредством устройств аутентификации индивидуального пользования, производится не реже, чем один раз в год.

14.8 Технические мероприятия авторизации пользователей обеспечиваются выполнением следующих организационных мероприятий:

* актуализация перечня защищаемых информационных ресурсов;
* актуализация документов по допуску и обеспечению соответствующего доступа пользователей к защищаемым ресурсам;
* распределение ответственности за выполнение мероприятий по защите информации между должностными лицами, организующими и реализующими технические мероприятия;
* назначение администраторов защиты (безопасности) информации.

14.9 Пользователям предоставляются минимально необходимые для выполнения производственных задач права доступа к информации. Ответственность за обоснованность предоставляемых пользователям прав возлагается на руководителей структурных подразделений.

# 15. Действия при компрометации аутентификатора или парольной информации

15.1 Под компрометацией аутентификатора понимается: утрата электронного аутентификатора, разглашение PIN-кода электронного аутентификатора или иная ситуация, которая дает основание для предположения о нарушении конфиденциальности пароля или PIN-кода устройства аутентификации (неявная компрометация).

15.2 При выявлении факта компрометации аутентификатора пользователь незамедлительно обязан: при разглашении PIN-кода электронного аутентификатора сменить PIN-код; в остальных случаях – сообщить о факте выявления непосредственному руководителю и администратору по защите информации.

15.3 В случае выявления факта компрометации аутентификатора пользователя администратор по защите информации обязан немедленно заблокировать учетную запись пользователя, аутентификатор которого скомпрометирован.

15.4 Расследование факта компрометации проводится комиссией, назначаемой руководителем Учреждения. В состав комиссии обязательно включается администратор по защите информации.

15.5 Результаты работы комиссии оформляются актом. Акт утверждается руководителем Учреждения.

15.6 Выдача пользователю нового аутентификатора производится по указанию руководителя Учреждения.