УТВЕРЖДЕНО:
Директор ОГАУ ДО ОСШ по футболу
(наименование общеобразовательной организации)

_____ /А.Ю. Фомин/
подпись расшифровка подписи

Приказ № 37 от 09.01.2024 г.

Инструкция по организации защиты информации в информационных системах персональных данных.

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; то есть 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 со 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 АИС, 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 со 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

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 (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, то есть 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 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 ОГАУ ДО ОСШ по футболу (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.
2.2. 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;
- 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;
- 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;
- 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. 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 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;
- 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;
- 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, 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.

11.2. 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.

11.2.2. 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.