ПРИНЯТО
Решением Управляющего совета
ГБОУ школа №34
Невского района Санкт-Петербурга
Протокол от 30.08.2024 № 6

УТВЕРЖДЕНО
Приказом от 30.08.2024 № 255
Директор ГБОУ школа №34
Невского района Санкт-Петербурга
_____ Сергеева Т.А.

ПОЛОЖЕНИЕ
О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

ограниченного доступа, не содержащей сведений, составляющих государственную тайну

в Государственном бюджетном общеобразовательном учреждении школа № 34 Невского района Санкт – Петербурга

Санкт-Петербург, 2025 г.

Содержание

Используемые сокращения

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БД	Базы данных
ЗИ	Защита информации
ИСПДн	Информационная система персональных данных
КС	Корпоративная сеть
КЗ	Класс защищенности
КИ	Конфиденциальная информация
ЛВС	Локальная вычислительная сеть
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
ПЭМИН	Побочные электромагнитные излучения и наводки
РД	Руководящий документ
СВТ	Средства вычислительной техники
СЗИ	Система защиты информации
СКЗИ	Средства криптографической защиты информации
СКУД	Система контроля управления доступом
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЧС	Чрезвычайная ситуация
ЭВМ	Электронная вычислительная машина
ЭК	Экспертная комиссия

Термины и определения

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

Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации определенного вида деятельности.

Аттестация автоматизированной системы – процесс комплексной проверки выполнения заданных функций автоматизированной системы по обработке защищаемой информации на соответствие требованиям стандартов и/или нормативных документов в области защиты информации и оформления документов о ее соответствии требованиям безопасности информации.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение его подлинности.

Безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних и внешних угроз.

Государственная информационная система – федеральная информационная система и региональная информационная система, созданная на основании соответственно федерального закона, закона субъекта Российской Федерации, на основании правовых актов государственных органов.

Доступность информации – состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями нормативных и правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Класс защищенности автоматизированной системы – определенная совокупность требований по защите автоматизированной системы от несанкционированного доступа к информации.

Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации или обладателем информации.

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

Несанкционированный доступ – получение защищаемой информации заинтересованным субъектом с нарушением установленных нормативными правовыми документами или обладателем информации прав или правил доступа к защищаемой информации.

Обработка информации – совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Оператор информационной системы персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация.

Система защиты информации в автоматизированной – системе совокупность технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации

Система обеспечения безопасности информации – совокупность органов и (или) исполнителей, используемых ими средств защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Средство защиты информации – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Техническая защита конфиденциальной информации – комплекс мероприятий и (или) услуг по ее защите от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Целостность информации – состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

1. Общие положения

Настоящий документ «Положение о порядке организации и проведения работ по защите информации ограниченного доступа, не содержащей сведения, составляющих государственную тайну в Государственном бюджетном общеобразовательном учреждении школа № 34 Невского района Санкт – Петербурга (далее — Положение) определяет цели, задачи и основные мероприятия по обеспечению безопасности информации ограниченного доступа, не содержащей сведения, составляющих государственную тайну в Государственном бюджетном общеобразовательном учреждении школа № 34 Невского района Санкт – Петербурга (далее — Учреждение).

В соответствии с Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», в Положении под сведениями конфиденциального характера понимается следующая информация (далее — КИ):

– Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

– Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

– Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

Положение разработано в соответствии с действующим законодательством РФ в области безопасности информации, а также ГОСТ и руководящими документами (РД) ФСТЭК (Гостехкомиссии) России, перечень которых приведен в Разделе 9.

Положение является основой для разработки локальных нормативных актов Учреждения по обеспечению безопасности информации.

Положение распространяется на всех сотрудников Учреждения, включая сотрудников, работающих по договору подряда, а также на сотрудников сторонних организаций, взаимодействующих с Учреждением на основании соответствующих нормативных, правовых и организационно-распорядительных документов.

Положение применимо ко всем средствам вычислительной техники, активному сетевому оборудованию, персональным компьютерам в пределах среды ИСПДн.

2. Цели и задачи обеспечения безопасности информации

Под безопасностью информации понимается состояние защищенности информационной среды Учреждения, обеспечивающее полноту, достоверность и своевременность информации, и обеспечение безопасности такой информации.

Обеспечение безопасности информации Учреждения осуществляется путем реализации деятельности по защите информации, т.е. деятельности по предотвращению утечки и утраты информации. При этом в понятие утрата входит хищение, потеря информации, а также блокирование (временная утрата) и искажение (частичная утрата), а в понятие утечка информации — неправомерный выход информации за пределы защищаемой зоны ее функционирования или установленного круга лиц, результатом которого является получение информации лицами, не имеющими к ней санкционированного доступа. Утечка и утрата информации могут происходить в результате несанкционированного доступа (НСД) к информации, несанкционированных и непреднамеренных воздействий на нее или средства ее обработки и передачи.

Таким образом, целью реализации различных мер и мероприятий по защите информации является, в конечном итоге, обеспечение безопасности информации Учреждения.

Задачами, которые необходимо решить для достижения поставленной цели являются:

– своевременное выявление потенциальных угроз защищаемой информации и средствам ее обработки и передачи;
– выявление причин, обстоятельств и условий, способствующих реализации выявленных угроз и выработка мероприятий по их нейтрализации;
– предотвращение НСД к информации и средствам ее обработки и передачи;
– предотвращение непреднамеренных воздействий на информацию и средства ее обработки и передачи;
– предотвращение утечки информации по техническим каналам;
– контроль эффективности защитных мер и мероприятий.

3. Защищаемые информационные ресурсы

К защищаемым информационным ресурсам Учреждения относятся:

– информация, зафиксированная на различных носителях;

– средства обработки, хранения, передачи информации и средства связи, в том числе программное обеспечение указанных средств (при его наличии).

3.1. Информация, подлежащая защите

Защите подлежит информация, касающаяся различных направлений деятельности, неправомерное обращение с которой может нанести ущерб интересам Учреждения или иному физическому или юридическому лицу, доверившему свою информацию Учреждения.

В рамках деятельности Учреждения ведется обработка конфиденциальной информации. Конкретный состав информации определяется в установленном действующим законодательством порядке и закрепляется в соответствующих документах: в «Перечне сведений конфиденциального характера в Государственном бюджетном общеобразовательном учреждении школа № 34 Невского района Санкт – Петербурга, утверждаемом директором Государственного бюджетного общеобразовательного учреждения школа № 34 Невского района Санкт – Петербурга. Указанный перечень разрабатывается в соответствии с действующим законодательством, в том числе, в части определения сведений, которые не могут быть отнесены к категории конфиденциальной информации. Защищаемые информационные ресурсы могут быть представлены в виде отдельных документов (массивов документов) на бумажных носителях, а также в виде документов (файлов) и массивов документов в ЛВС и/или на машинных носителях информации.

3.2. Средства обработки информации

Состав средств обработки, хранения и передачи информации, а также средств связи, используемых для обработки конфиденциальной информации, закрепляется в «Техническом паспорте» объекта информатизации.

Средства вычислительной техники, используемые для обработки информации в Учреждении, объединены в ЛВС.

Программное обеспечение представлено клиентскими ОС для рабочих станций. Стандартный пакет ПО, устанавливаемый на рабочих станциях, приведен в «Техническом паспорте». Иное программное обеспечение, необходимое сотрудникам для выполнения своих функциональных обязанностей, устанавливается на АРМ после согласования с администратором безопасности Учреждения.

В качестве средств защиты и взаимодействия с участниками информационного обмена используется сертифицированные средства шифрования и межсетевого экранирования.

4. Угрозы защищаемым информационным ресурсам

Дестабилизирующее воздействие на информацию и/или средства ее обработки, хранения и передачи может привести к реализации следующих угроз:

- хищение персональных данных сотрудниками учреждения для использования в корыстных целях;
- передача финансовой, адресной, юридической и прочей информации о субъекте ПДн третьим лицам;
- несанкционированное публичное разглашение персональных данных, ставших известными сотрудникам учреждения;
- несанкционированное получение персональных данных третьими лицами;
- уничтожение финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- модификация финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- блокирование финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- ввод некорректной финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- передача некорректной финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- искажение архивной информации по субъекту ПДн.

5. Меры по обеспечению безопасности информации

Всю совокупность мер по обеспечению безопасности информации, наличие которых необходимо для построения системы защиты информации (СЗИ) Учреждения, условно можно разделить на:

- законодательные (правовые);
- организационные (административные);
- технические (программные и аппаратные);
- физические.

5.1. Законодательные (правовые) меры

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с конфиденциальной информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию конфиденциальной информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

5.2. Организационные (административные) меры

Организационные (административные) меры защиты — это меры организационного характера, регламентирующие процессы функционирования ИС, использование ресурсов ИС, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИС таким образом, чтобы в наибольшей степени затруднить или исключить

возможность реализации угроз безопасности конфиденциальной информации или снизить размер потерь в случае их реализации.

Главная цель организационных мер, предпринимаемых на высшем управленческом уровне — сформировать политику информационной безопасности Учреждения (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация политики информационной безопасности КИ в ИС состоит из мер административного уровня и организационных мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность ИС в целом. Примером таких решений могут быть:

– принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности КИ, определение ответственных за ее реализацию;

– формулирование целей, постановка задач, определение направлений деятельности в области безопасности КИ;

– принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне Учреждения в целом;

– обеспечение нормативной (правовой) базы по безопасности и т.п.

Политика административного уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности КИ, определить какими ресурсами (материальные, персонал) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и стоимостью проводимых мероприятий по защите КИ в ИС.

На уровне процедурных мер защиты определяются процедуры и правила достижения целей и решения задач политики информационной безопасности КИ. Эти правила определяют:

– какова область применения политики безопасности КИ;

– каковы роли и обязанности должностных лиц, отвечающих за проведение политики безопасности КИ, а также их ответственность;

– кто имеет права доступа к КИ;

– какими мерами и средствами обеспечивается защита КИ;

– какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

– предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

– определять коалиционные и иерархические принципы и методы разграничения доступа к КИ;

– определять порядок работы с программно-математическими и техническими (аппаратными) средствами защиты и криптозащиты.

5.2.1. Регламентация состава и содержания защищаемой информации

Состав информации, относимой к конфиденциальной, а также порядок такого отнесения определяется «Перечнем сведений конфиденциального характера» (далее - Перечень).

Любая иная информация, не указанная в данном Перечне, не должна относиться к категории конфиденциальной.

Если выявляется необходимость отнесения сведений к конфиденциальным, не подходящих ни под одну категорию из названного Перечня, то вносятся предложения по

его пересмотру. Пересмотр перечня осуществляется в порядке, установленном для его утверждения

5.2.2. Определение полномочий доступа сотрудников к защищаемым информационным ресурсам и их реализация

Порядок доступа сотрудников к защищаемым информационным ресурсам Учреждения определяется в соответствии с документом «Порядок управления доступом к информационным ресурсам в_____.

Защищаемые информационные ресурсы (с персональными данными), доступ пользователей к которым ограничен, определяется в документе «Перечень защищаемых информационных ресурсов».

Каждый сотрудник Учреждения должен иметь права доступа только к той части конфиденциальной информации, которая действительно необходима ему для выполнения своих трудовых обязанностей.

Необоснованное служебной необходимостью ознакомление сотрудников с конфиденциальной информацией Учреждения не допускается.

5.2.3. Технология обработки конфиденциальных документов

Технология обработки конфиденциальных документов включает в себя определение правил учета, хранения и выдачи носителей конфиденциальной информации (в том числе съемных машинных носителей) и правил работы сотрудников с защищаемой информацией.

При разработке конфиденциальных документов гриф должен определять сам разработчик. Гриф проставляется в правом верхнем углу с указанием количества экземпляров документа.

Полученные извне документы грифуются на основе «Перечня сведений конфиденциального характера». Все грифованные документы должны учитываться в книге учета и выдачи конфиденциальных документов.

Грифованные документы должны храниться в сейфах или надежно закрываемых шкафах. Учет, хранение и выдача документов осуществляется специально назначаемым сотрудником.

Для уничтожения таких документов приказом по Учреждению ежегодно назначается комиссия по их уничтожению, которая составляет и подписывает Акт уничтожения конфиденциальных документов, утверждаемый главным врачом.

Запрещается работа с конфиденциальными документами вне помещений Учреждения (кроме случаев служебных командировок). Вынос носителей с конфиденциальной информации с территории Учреждения и их транспортировка осуществляется в порядке, определенном соответствующим документом.

5.2.4. Организационное сопровождение функционирования технических и программно-аппаратных средств обработки и защиты информации

Порядок работы с техническими и программно-аппаратными средствами защиты информации определяется соответствующими руководителями для всех категорий пользователей, которые должны быть ознакомлены с содержанием данных документов и строго выполнять содержащиеся в них требования.

АРМ сотрудников Учреждения должны быть оборудованы необходимыми программными или программно-аппаратными средствами защиты информации — система парольной защиты, средства защиты информации от НСД, антивирусы, криптографические средства (при необходимости), и т.п.

Сотрудники обязаны использовать технические и программно-аппаратные средства защиты информации, установленные на их рабочих местах и/или использующиеся совместно со средствами обработки, передачи информации и средствами связи.

Не допускается обработка КИ на ЭВМ, включая портативные персональные компьютеры, без установленных программных или программно-аппаратных средств защиты информации.

Не допускается передача КИ по открытым каналам связи без использования специальных технических средств защиты информации.

Не допускается использование незащищенных личных средств мобильной связи для обсуждения вопросов, содержащих сведения конфиденциального характера.

В Учреждении должно проводиться обучение сотрудников правилам работы с используемыми техническими и программно-аппаратными средствами защиты информации.

Все используемые в Учреждении технические и программно-аппаратные средства защиты информации должны быть сертифицированы в установленном порядке.

5.2.5. Организация технического обслуживания оборудования, используемого для обработки защищаемой информации

Оборудование, предназначенное для обработки защищаемой информации Учреждения, должно эксплуатироваться в условиях (температура, влажность, электромагнитный режим) в соответствии с инструкциями производителя и/или соответствующих нормативных документов. Техническое обслуживание оборудования должно обеспечивать его постоянную работоспособность.

Проводить ремонт и техническое обслуживание оборудования могут только организации, обладающие в соответствии с действующим законодательством правом на осуществление указанного вида деятельности, привлекаемые Учреждением для оказания данных услуг на основании договора.

5.2.6. Организация пропускного и внутриобъектового режима в Учреждении

Для помещения, где обрабатывается КИ, должен быть составлен список сотрудников, имеющих право доступа в данное помещение. Список должен своевременно корректироваться по мере увольнения сотрудников Учреждения, приема на работу новых сотрудников или перевода сотрудника на другую работу. Сотрудники, не указанные в данном списке, не имеют права находиться в помещении без сопровождения сотрудника, имеющего право такого доступа, кроме случаев экстренной необходимости при чрезвычайных обстоятельствах.

Доступ посетителей на территорию Учреждения осуществляется по предварительной договоренности с конкретным сотрудником Учреждения, который должен сопровождать посетителя на протяжении всего времени нахождения на территории Учреждения. Доступ посетителей во внутреннее помещение Учреждения, где обрабатывается КИ, запрещен.

Доступ приглашенного технического и обслуживающего персонала в помещение, где обрабатывается КИ, осуществляется в соответствии с необходимыми письменными распоряжениями администрации Учреждения и фиксируется в журнале учета посещений. Доступ технического и обслуживающего персонала в защищаемые помещения без сопровождения сотрудника Учреждения не допускается.

5.2.7. Разработка организационно-распорядительной и нормативной документации

В Учреждении должны быть разработаны и введены в действие все организационно-распорядительные и иные нормативные документы, на которые имеются

ссылки в данном Положении. Одним из основных документов является «Перечень сведений конфиденциального характера».

В ходе подготовки Перечня должностные лица Учреждения должны провести анализ всех сторон его деятельности с целью определения конкретных сведений, разглашение которых может нанести ущерб.

Для работы по составлению Перечня должен привлекаться широкий круг экспертов и должностных лиц отделов, служб Учреждения с тем, чтобы ни одно из возможных направлений деятельности не было упущено при его разработке.

Перечень вводится в действие приказом директора.

5.2.8. Контроль соблюдения требований по обеспечению информационной безопасности информации

Контроль соблюдения требований по обеспечению безопасности информации в Учреждении возлагается на администрацию Учреждения и специально назначенные проверочные комиссии.

В Учреждении должна быть введена должность администратора информационной безопасности, который осуществляет организацию деятельности по защите конфиденциальной информации Учреждения, установку, настройку и администрирование программных и программно-аппаратных средств защиты информации в КС, контроль за выполнением требований по обеспечению безопасности информации.

Допускается совмещение выполнения указанных функций с другими обязанностями. При этом совмещение в одном лице функций системного администратора и администратора информационной безопасности **не допускается**.

Каждый сотрудник несет персональную ответственность за соблюдение правил настоящего Положения и иных нормативных документов по вопросам обеспечения безопасности информации.

5.3. Технические (программные и аппаратные) меры

Данные меры предполагают обеспечение защиты конфиденциальной информации от утечки по техническим каналам, а также от НСД.

5.3.1. Общие меры по защите КИ от НСД

Установка и настройка программно-аппаратных средств защиты информации в ЛВС осуществляется только администратором информационной безопасности.

Установка и настройка программных и программно-аппаратных средств обработки информации в ЛВС осуществляется лицами, выполняющими функции системного администратора (далее - системный администратор).

Все действия администратора информационной безопасности по настройке программных и программно-аппаратных средств защиты информации Учреждения, действия системного администратора по настройке программных и программно-аппаратных средств обработки информации в ЛВС, а также их результаты заносятся в протокол настройки.

Все действия системного администратора по настройке программных и программно-аппаратных средств обработки информации в ЛВС не должны нарушать состояние защищенности обрабатываемой информации. Контроль соблюдения требований безопасности при работах в ЛВС должен осуществляться администратором информационной безопасности.

Доступ к конфигурации программно-аппаратных средств защиты информации для иных пользователей, кроме администратора информационной безопасности, должен быть блокирован.

На АРМ пользователей должно быть установлено прикладное программное обеспечение (ПО), только действительно необходимое пользователю для выполнения им своих трудовых обязанностей. Неиспользуемое пользователем ПО должно быть отключено или удалено.

Должно проводиться своевременное обновление ПО АРМ.

Установку нового ПО на АРМ и обновление ПО должен осуществлять только системный администратор или сотрудники службы, осуществляющие обслуживание и техническое сопровождение СВТ Учреждения.

АРМ должно эксплуатироваться тем сотрудником, за которым оно закреплено. Этот сотрудник несет персональную ответственность за работу своего АРМ и выполнение требований данного Положения по безопасности для своего АРМ.

Из операционной системы удаляются (отключаются) все неиспользуемые сервисы и протоколы, регулярно устанавливаются пакеты обновлений для создания более безопасной конфигурации операционной системы (ОС).

Рекомендуется использование источников бесперебойного питания для АРМ, где ведется обработка КИ.

Съемные машинные носители конфиденциальной информации должны быть учтены в подразделении, выполняющем функции службы конфиденциального делопроизводства, в установленном порядке.

5.3.2. Контроль доступа пользователей к АРМ

При доступе к АРМ Учреждения должны обеспечиваться: идентификация, аутентификация, авторизация; управление доступом; контроль целостности; регистрация, включая:

– функционирование системы парольной защиты АРМ;

– контроль доступа пользователей к ресурсам АРМ. Оперативный контроль доступа пользователей осуществляется администратором информационной безопасности;

– непротиворечивая и прозрачная административно-техническая поддержка задач управления доступом к ресурсам АРМ.

Системный администратор не должен иметь служебных полномочий (а при возможности и технических средств) по настройке параметров системы, влияющих на полномочия пользователей по доступу к информации. Администратор безопасности должен иметь служебные полномочия и технические возможности по контролю действий соответствующих системных администраторов (без вмешательства в их действия) и пользователей, а также полномочия (а при возможности и технические средства) по настройке для каждого пользователя параметров системы, которые определяют права доступа к информации.

Права доступа пользователей к ресурсам АРМ назначаются администратором информационной безопасности.

Для каждого пользователя заводится отдельная учетная запись.

Учетные записи пользователей делятся на 2 категории: администраторы и пользователи.

Администраторы:

– учетная запись используется сотрудниками службы, осуществляющей поддержку функционирования АРМ и средств его защиты;

– администраторы имеют доступ ко всем штатным средствам настройки АРМ.

Пользователи:

– учетная запись используется для всех сотрудников, АРМ которых используются для обработки КИ;

– пользователи имеют право на использование ПО, установленного на АРМ;

– пользователи не имеют права установки дополнительного ПО без согласования с администратором информационной безопасности и системным администратором.

Учетные записи сотрудников, которые прекратили работу в Учреждении, должны блокироваться. Удаление таких учетных записей должно осуществляться не ранее, чем через 6 месяцев.

Доступ пользователей к АРМ осуществляется с использованием средств парольной защиты.

Пароль пользователя назначается администратором информационной безопасности при создании учетной записи пользователя и в дальнейшем может изменяться только им с соблюдением следующих условий:

– должен состоять не менее, чем из 6 символов;

– должен содержать хотя бы по одной строчной, прописной букве и цифре;

– должен быть известен только владельцу и администратору информационной безопасности;

– не должен использоваться для доступа к другим информационным системам и сервисам вне Учреждения;

– не должен содержать устойчивых выражений, словосочетаний, аббревиатур и т.п.;

– не должен содержать любых персональных данных;

– не должен содержать повторений или простых последовательностей букв и цифр.

В целях обеспечения доступа к системе в случае, когда пользователь забыл пароль, список паролей хранится у администратора информационной безопасности в зашифрованном виде.

Смена пароля должна проводиться периодически, как установлено в Учреждении, или при его компрометации.

Должна быть обеспечена автоматическая блокировка сеанса работы через 10 минут с момента последнего взаимодействия пользователя с компьютером.

Должна быть предусмотрена возможность ручной блокировки экрана на случай оставления пользователем рабочего места.

Снятие блокировки осуществляется вводом пароля пользователя.

Контроль доступа (как локального, так и удаленного) к АРМ администратора информационной безопасности и системного администратора должен дополнительно обеспечиваться с помощью средств аутентификации.

5.3.3. Мониторинг системы защиты информации

Мониторинг СЗИ должен проводиться администратором информационной безопасности с целью обнаружения и регистрации отклонений защитных мер от требований обеспечения безопасности информации и оценки полноты реализации требований данного Положения.

Основной целью мониторинга СЗИ является оперативное и постоянное наблюдение, сбор, анализ и обработка данных, необходимых для решения следующих задач:

– контроль за реализацией положений нормативных актов по обеспечению безопасности информации на Учреждения;

– выявление нештатных (или злоумышленных) действий в АРМ Учреждения;
– выявление потенциальных нарушений безопасности информации.

Для целей оперативного и постоянного наблюдения объектов мониторинга могут использоваться как специализированные (например, программные) средства, так и штатные (входящие в коммерческие продукты и системы) средства регистрации действий пользователей, процессов и т.п.

В СЗИ должен вестись журнал регистрации действий пользователей. Журнал ведется в электронной форме, при необходимости, с использованием штатных средств ОС.

Журнал регистрации должен быть защищен от несанкционированного доступа и изменений.

Должно осуществляться резервное копирование данных журнала регистрации.

Должно быть настроено оперативное оповещение администратора информационной безопасности при регистрации критических событий нарушения безопасности.

Администратор безопасности должен регулярно просматривать и анализировать данные журнала регистрации.

5.3.4. Антивирусная защита

На каждом АРМ должны использоваться официально приобретенные (лицензионные) средства антивирусной защиты.

Обязателен автоматический запуск антивирусного средства при загрузке ОС и обязательное автоматическое обновление антивирусных баз не реже, чем раз в сутки.

Любые файлы, полученные из сети Интернет, должны автоматически проверяться на наличие вирусов и открываться только в случае подтверждения отсутствия вирусной опасности.

Устанавливаемое или изменяемое программное обеспечение и АРМ должно быть предварительно проверено на отсутствие вирусов. После установки или изменения программного обеспечения должна быть выполнена полная антивирусная проверка.

При обнаружении компьютерного вируса необходимо принять меры по устранению последствий вирусной атаки, проинформировать администратора информационной безопасности и, при необходимости, приостановить работу (на период устранения последствий вирусной атаки). В случае обнаружения вирусной атаки должно проводиться «лечение» зараженных файлов (без запроса действия у пользователя). В случае невозможности лечения — должно выдаваться сообщение администратору для дальнейшего принятия им требуемых мер.

Не должно допускаться самостоятельное удаление пользователями зараженных файлов.

Отключение или отказ от обновления антивирусных средств не допускается. Установка и обновление антивирусных средств в Учреждении должны контролироваться администратором информационной безопасности и системным администратором.

Ответственность за выполнение требований по антивирусной защите должна быть возложена на администратора безопасности Учреждения, а обязанности по выполнению мер антивирусной защиты должны быть возложены на каждого сотрудника Учреждения, имеющего доступ к АРМ.

Должны проводиться периодические антивирусные проверки АРМ в соответствии с «Инструкцией по организации антивирусной защиты»

5.3.5. Резервное копирование данных

Резервные копии наиболее важной информации рекомендуется периодически сохранять на съемных носителях и хранить их в закрытых сейфах, запираемых шкафах, местах, исключающих посторонний доступ. Порядок работы со съемными носителями информации выполняется в соответствии с «Инструкцией по порядку учета, хранения и уничтожения носителей, содержащих КИ».

5.3.6. Организация взаимодействия между удаленными сегментами сети

Взаимодействие между удаленными сегментами сети должно осуществляться с использованием VPN-соединения, построенного на основе используемой в качестве транспортной среды телекоммуникационной сети провайдера.

Организация VPN-сети обеспечивает защиту информации, передаваемой при взаимодействии между сегментами корпоративной сети с помощью следующих механизмов:

– организация шифрованного логического соединения на основе криптоалгоритмов, сертифицированных ФСБ РФ;

– использование надежных с точки зрения безопасности информации методов аутентификации и средств организации VPN-сетей.

Должен быть организован мониторинг за установленными VPN-соединениями.

В каждом сегменте должен быть регламентирован перечень объектов доступа, доступных для пользователей внешних сегментов корпоративной сети.

Применение несертифицированных средств криптографической защиты запрещается.

5.4. Физические меры

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

5.4.1. Установка и использование средств охранно-пожарной сигнализации

В помещениях Учреждения должны быть установлены необходимые элементы системы охранно-пожарной сигнализации: дымовые и/или тепловые пожарные датчики, датчики охранной сигнализации, извещатели, а также средства пожаротушения.

Должен проводиться периодический профилактический осмотр указанных средств на предмет своевременного выявления неисправностей.

5.4.2. Установка и использование средств физической защиты

Помещения Учреждения должны быть оборудованы запирающими конструкциями (электромеханическими замками).

Помещения, в которых ведется обработка конфиденциальной информации, по возможности должны быть оборудованы дополнительными средствами ограничения

доступа (опечатывающие устройства и т.п.) и оборудованы сейфами для хранения носителей конфиденциальной информации и материальных ценностей.

6. Контроль эффективности защиты

Эффективность защиты информации — это степень соответствия реального функционирования и состояния СЗИ поставленным целям.

Основным принципом оценки эффективности является постоянный контроль выполнения требований действующих законодательных, нормативно-методических и организационно-распорядительных документов по данной проблеме.

Для оценки эффективности используются показатели, определяемые действующими нормами, установленными нормативными документами ФСТЭК, ФСБ и документами Учреждения.

Контроль эффективности проводимых мероприятий по защите информации и выполнения требований Положения осуществляется лицами, ответственными за безопасность информации в Учреждении, с докладом руководству Учреждения. Состав сотрудников, ответственных за проведение контрольных мероприятий, определяется в соответствии с Положением.

Непосредственный контроль за выполнением требований Положения при обработке КИ осуществляется администратором информационной безопасности. Контроль может проводиться в ходе различных проверок на рабочих местах.

Необходимо отслеживать состояние работы всех элементов СЗИ, входящих в состав защитных механизмов и соответствующих мер и мероприятий, корректность выполнения ими своих функций и соответствия результатов их выполнения заданным показателям. В целях оценки эффективности действующей СЗИ проводится ее аудит.

Аудит СЗИ Учреждения может быть внутренним или внешним. Порядок и периодичность проведения внутреннего аудита определяется руководством Учреждения на основе потребностей в такой деятельности. Внешний аудит СЗИ проводится независимыми аудиторами.

Цель аудита СЗИ состоит в проверке и оценке ее соответствия требованиям настоящего Положения и других принятых в организации нормативных актов по защите информации. Аудит СЗИ должен проводиться периодически.

При проведении аудита СЗИ должны использоваться стандартные процедуры документальной проверки, опрос и интервью с руководством и персоналом Учреждения. При необходимости уточнения результатов документальной проверки, опросов и интервью в рамках внутреннего аудита СЗИ в качестве дополнительного способа может применяться «проверка на месте», которая проводится для обеспечения уверенности в том, что конкретные защитные меры реализуются, правильно используются и проверяются с помощью тестирования. Обстоятельства, при которых требуется дополнительный способ в рамках внутреннего аудита СЗИ, должны быть определены и согласованы в плане проведения аудита.

При проведении внутреннего аудита СЗИ могут использоваться журналы регистрации событий, ведущиеся администраторами информационной безопасности Учреждения и формируемые на основе данных мониторинга СЗИ.

При проведении внешнего аудита СЗИ руководство Учреждения должно обеспечить документальное и, если это необходимо, техническое подтверждение того, что:

- положение отражает требования и цели Учреждения;
- организационная структура управления СЗИ создана;
- процессы выполнения требований по защите информации реализуются и удовлетворяют поставленным целям;

– защитные меры (например, межсетевые экраны, средства управления физическим доступом) настроены и используются правильно;

– остаточные риски оценены и остаются приемлемыми для организации;

– рекомендации предшествующих аудитов СЗИ реализованы.

Аудиторский отчет должен храниться в Учреждении в течение установленного времени. Доступ к аудиторскому отчету должен быть разрешен только руководству организации и ответственному за безопасность информации в Учреждении.

Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам.

Несоответствие принимаемых мер установленным требованиям или нормам является нарушением.

7. Ответственность

Все сотрудники Учреждения, допущенные в установленном порядке к работе с защищаемой информацией, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности такой информации и соблюдение правил работы с ней, установленных данным Положением и иными организационно-распорядительными документами Учреждения, разработанными на его основе.

Ответственность за доведение требований настоящего Положения до сотрудников Учреждения и обеспечение мероприятий по их реализации несет руководство Учреждения.

Все сотрудники Учреждения обязаны неукоснительно соблюдать относящиеся к ним требования настоящего Положения.

Отказ соблюдать настоящее Положение может подвергнуть защищаемую информацию Учреждения недопустимому риску потери целостности, доступности, актуальности или конфиденциальности при ее хранении, обработке или передаче.

Нарушения сотрудниками Учреждения положений, инструкций, руководств и иных организационно-распорядительных документов, поддерживающих данное Положение, будут рассматриваться руководством Учреждения в административном порядке и лица-нарушители будут привлекаться к ответственности в установленном действующим законодательством порядке.

8. Мероприятия по реализации требований Положения

Состав, порядок, сроки исполнения указанных мероприятий, а также лица, ответственные за их проведение, указываются в разрабатываемых на основании данного Положения документах.

В состав данных мероприятий должны быть включены следующие меры:

Организационные:

– разработка соответствующего комплекса организационно-распорядительной документации, включающей различные инструкции, руководства, положения и прочие документы;

– ознакомление с Положением и соответствующими инструкциями и руководствами сотрудников Учреждения под роспись;

– обучение сотрудников Учреждения основам обеспечения безопасности информации, в случае необходимости;

– контроль за выполнением требований организационно-распорядительной документации.

Технические:

– мониторинг угроз безопасности информации;

– внедрение технических и программно-аппаратных средств защиты;

– поддержание указанных средств в работоспособном состоянии, их техническая поддержка и обслуживание;

– технический контроль за соблюдением требований Положения и поддерживающих его документов;

– осуществление соответствующих мероприятий по ЗИ.

9. Законодательная и нормативная база

– Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации от 05.12.2016 № 646.

– Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».

– Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

– Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

– Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

– Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

– Приказ ФСТЭК России от 18 февраля 2013г. №21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

– Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в информационных системах».

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России от 15.02.2008.

– приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

– приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

– руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением председателя Гостехкомиссии России от 30.03.1992)

– Нормативно-методический документ Государственной технической комиссии при Президенте Российской Федерации «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденный приказом Гостехкомиссии России от 30.08.2002 года № 282.

– информационное сообщение ФСТЭК России от 15.02.2021 № 240/22/690 «Об утверждении Методики оценки угроз безопасности информации».