

Принято
Советом общеобразовательного
учреждения ГБОУ «Санаторная
школа-интернат № 9 г. о. Самара»
Протокол № 1 от 30.08.2019г.

Утверждено
Директор ГБОУ «Санаторная
школа-интернат № 9 г. о. Самара»
Т.Ю. Сафиуллина
Приказ № 122-о/д от 2.09.2019г.



ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Государственного бюджетного оздоровительного общеобразовательного
учреждения Самарской области «Санаторная школа-интернат № 9 для
обучающихся, нуждающихся в длительном лечении,
городского округа Самара»**

г. Самара, 2019

1. Вводные положения

1.1. Введение

Политика информационной безопасности Государственного бюджетного оздоровительного общеобразовательного учреждения Самарской области «Санаторная школа-интернат № 9 для обучающихся, нуждающихся в длительном лечении, городского округа Самара» (далее по тексту – Учреждение) определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Учреждение в своей деятельности.

1.2. Цели

Основными целями политики информационной безопасности Учреждения являются защита информации и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в его Уставе.

Общее руководство обеспечением ИБ Учреждения осуществляет директор Учреждения. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет ответственный за информатизацию (далее системный администратор).

Должностные обязанности системного администратора закрепляются в соответствующей инструкции.

Сотрудники Учреждения обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

1.3. Задачи

Политика информационной безопасности Учреждения направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических

сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Для противодействия угрозам информационной безопасности в Учреждении составляются модели угроз.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

1.4. Область действия

Настоящая Политика обязательна для исполнения уполномоченными сотрудниками Учреждения.

2. Период действия и порядок внесения изменений

Настоящая политика вводится в действие приказом директора Учреждения.

Политика признается утратившей силу на основании приказа директора Учреждения.

Изменения в политику вносятся приказом директора Учреждения.

Инициатором внесения изменений в политику информационной безопасности является:

- системный администратор.

Плановая актуализация настоящей политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация политики информационной безопасности производится в обязательном порядке в следующих случаях:

- при изменении политики РФ в области информационной безопасности, указов и законов РФ в области защиты информации;

- при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности Учреждения;
- при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб Учреждения.

Ответственность за актуализацию политики информационной безопасности (плановую и внеплановую) несет системный администратор.

Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на системного администратора, директора Учреждения.

3. Термины и определения

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

Актив – что-либо, что имеет ценность для учреждения.

Анализ риска – систематическое использование информации для определения источников и оценки риска.

Аудит информационной безопасности – процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самим обществом (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит). Результаты проверки документально оформляются свидетельством аудита.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

Доступ к информации – возможность получения информации и ее использования.

Доступность – доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Доступность информации – состояние информации, характеризующееся способностью АС обеспечивать беспрепятственный доступ к информации субъектов имеющих на это полномочия.

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – это актив, который, подобно другим активам общества, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов общества.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения производственных задач Учреждения.

Информационно-телекоммуникационная система – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники, а также информационные системы, обеспечивающие автоматизацию процессов Учреждения и средства защиты информации.

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

Информационные активы – информационные системы, информационные средства, информационные ресурсы.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий, используемая в производственных - процессах Учреждения.

Инцидент информационной безопасности – действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов учреждения.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

Код аутентификации электронного сообщения – данные, используемые для установления подлинности и контроля целостности электронного сообщения.

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

Конфиденциальность – доступ к информации только авторизованных пользователей.

Корпоративная сеть – объединение информационных систем, компьютерного, телекоммуникационного и офисного оборудования всех подразделений ГБОУ «Санаторная школа-интернат № 9 г. о. Самара», посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.

Мониторинг информационной безопасности – постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности, сбор,

анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы учреждения, информационные услуги учреждения и пр.

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Обработка риска – процесс выбора и осуществления мер по модификации риска.

Ответственное лицо (администратор) информационных активов – сотрудник Учреждения, получивший на основании соответствующего распорядительного документа права обладателя информации, обрабатываемой в информационной системе.

Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

Периметральное средство защиты информации (СЗИ) – шлюз информационной безопасности, обеспечивающий межсетевое экранирование и защиту данных пересылаемых по открытым каналам связи (шифрование), а так же фильтрацию вредоносного ПО и блокирование внешних атак.

Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в Учреждении для обеспечения его информационной безопасности.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе

данных, приложениях и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Системный администратор – сотрудник Учреждения, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети учреждения и ПК.

Средства криптографической защиты информации – средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Угрозы информационным данным – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Управление информационной безопасностью – совокупность целенаправленных действий, осуществляемых в рамках политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности учреждения при реализации угроз в информационной сфере.

Целостность – достоверность и полноту информации и методов ее обработки.

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

ЭВМ – электронная - вычислительная машина, персональный компьютер.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца ключа подписи, а также установить отсутствие искажения информации в электронном документе.

4.Обозначения и сокращения

АРМ – Автоматизированное рабочее место.

АС – Автоматизированная система.

БД – База данных.

ЗИ – Защита информации.

ИБ – Информационная безопасность.

ИС – Информационная система.

НСД – Несанкционированный доступ.

ОС – Операционная система.

ПБ – Политики безопасности.

ПО – Программное обеспечение.

СВТ – Средства вычислительной техники.

СЗИ – Средство защиты информации.

СКЗИ – Средство криптографической защиты информации.

СПД – Система передачи данных.

СУБД – Система управления базами данных.

СУИБ – Система управления информационной безопасностью.

СЭД – Система электронного документооборота.

ЭВМ – электронная - вычислительная машина, персональный компьютер.

ЭЦП – Электронная цифровая подпись.

5. Политика информационной безопасности Учреждения

5.1. Назначение политики информационной безопасности

Политика информационной безопасности Учреждения – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в Учреждении.

Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика информационной безопасности относится к административным мерам обеспечения информационной безопасности, и определяет стратегию Учреждения в области ИБ.

Политика информационной безопасности (далее, ПБ) регламентируют эффективную работу средств защиты информации. Она охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политика информационной безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

5.2. Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются следующие:

- Своевременное обнаружение проблем, потенциально способных повлиять на ИБ общества, корректировка моделей угроз и нарушителя.

- Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей общества, а также повышать трудоемкость технологических процессов обработки информации.
- Контроль эффективности принимаемых защитных мер.
- Адекватное разделение ролей и ответственности между сотрудниками Учреждения, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

5.3.Соответствие ПБ действующему законодательству

Правовую основу политики составляет Конституция Российской Федерации, законы Российской Федерации и другие законодательные акты, определяющие права и ответственность сотрудников Учреждения в сфере безопасности информации.

5.4.Ответственность за реализацию политики информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт системный администратор.

5.5.Организация системы управления информационной безопасностью Учреждения

5.5.1.Организация системы управления ИБ

Система управления информационной безопасностью Учреждения (СУИБ) – предназначенная для создания, реализации, эксплуатации, анализа, поддержки и повышения информационной безопасности Учреждения.

Для успешного функционирования СУИБ Учреждения должны быть реализованы следующие процессы:

- определение и уточнение области действия СУИБ и выбор подхода к оценке рисков ИБ.

- определение и уточнение области действия СУИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью Учреждения.
- выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ.

5.5.2. Методы оценивания информационных рисков

Оценка информационных рисков Учреждения выполняется по следующим основным этапам:

- оценивание возможных угроз;
- оценивание существующих уязвимостей;
- оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые для производственного процесса уязвимые информационные ресурсы Учреждения подвергаются риску, если по отношению к ним существуют какие-либо угрозы.

Цель оценивания рисков состоит в определении характеристик рисков. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности Учреждения.

При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты.

5.5.3. Политика предоставления доступа к информационному ресурсу. Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к информационным ресурсам Учреждения.

К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей политикой.

6.Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений политик информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений информационной безопасности в Учреждении и проведение разъяснительной работы по информационной безопасности среди пользователей Учреждения.

Проведение в ИС Учреждения регламентных работ по защите информации предполагает ежегодное утверждение и выполнение плана мероприятий по обеспечению защиты персональных данных при их обработке в ИС персональных данных.

Системный администратор (возможно, при помощи сторонней организации специализирующейся в области информационной безопасности) собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения относительно ИС Учреждения. Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, общественных объединений и других организаций, специализирующихся в области защиты информации.

Системный администратор при помощи сторонней организации, специализирующейся в области информационной безопасности организывает периодическую проверку СЗИ ИС Учреждения.

7. Ликвидация последствий нарушения политик информационной безопасности

В случае обнаружения подсистемой защиты информации факта нарушения информационной безопасности или осуществления НСД к защищаемым информационным ресурсам ИС Учреждения рекомендуется уведомить системного администратора и отдел автоматизированных систем финансовых расчетов, и далее следовать их указаниям.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС Учреждения.

8. Ответственность нарушителей ПБ

Ответственность за выполнение правил Политики безопасности несет каждый сотрудник Учреждения в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования политики безопасности Учреждения, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Учреждению в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса РФ).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники Учреждения несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.