РАССМОТРЕНО»
На Управляющем Совете
Протокол №2 от 16.02.2020

«УТВЕРЖДЕНО»
Директор МБОУ «СОШ №106»
Матвеева Л.Г. _____
Приказ № 01-04/12 от 20.02.2020

Матвеева Лариса Геннадьевна
Подписано цифровой подписью: Матвеева Лариса Геннадьевна
Дата: 2021.03.20 11:58:57 +07'00'

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа №106»

Содержание

Вводные положения

1.1.Введение

Политика информационной безопасности МБОУ «СОШ №106» определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется МБОУ «СОШ №106» в своей деятельности.

1.2.Цели

Основными целями политики информационной безопасности МБОУ «СОШ №106» являются защита информации учреждения и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в его Уставе.

Общее руководство обеспечением ИБ МБОУ «СОШ №106» осуществляет заместитель директора по УВР (ответственный за организацию работы по информационной безопасности). Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет заместитель директора по УВР (далее администратор информационной безопасности).

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 МБОУ «СОШ №106» 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.

Наибольшими возможностями для нанесения ущерба МБОУ «СОШ №106» обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне общества), либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

Задачами настоящей политики являются:

- описание организации системы управления информационной безопасностью в МБОУ «СОШ №106»;
- определение Политик информационной безопасности МБОУ «СОШ №106», а именно:
  - Политика реализации антивирусной защиты;
  - Политика использования паролей;
  - Политика конфиденциального делопроизводства;
- определение порядка сопровождения ИС МБОУ «СОШ №106».

1.4.Область действия

Настоящая Политика обязательна для исполнения всеми сотрудниками и должностными лицами МБОУ «СОШ №106». Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах МБОУ «СОШ №106», а также в договорах.

1.5.Период действия и порядок внесения изменений

Настоящая политика вводится в действие приказом руководителя образовательной организации.

Политика признается утратившей силу на основании приказа руководителя образовательной организации.

Изменения в политику вносятся приказом руководителя образовательной организации.

Инициаторами внесения изменений в политику информационной безопасности являются:

- Заместитель директора по УВР, который выполняет функции администратора информационной безопасности
- Учитель информатики, который является ответственным за функционирование автоматизированной системы учреждения.

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 МБОУ «СОШ №106»;
- при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб МБОУ «СОШ №106».

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

Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на заместителя директора по УВР, который выполняет функции администратора информационной безопасности.

2. Термины и определения

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

Администратор информационной безопасности – специалист, осуществляющий контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Администратор сети – сотрудник, который выполняет функции администратора информационной безопасности, осуществляющие непосредственную организацию и выполнение работ по созданию (модернизации), техническому обслуживанию и управлению (администрированию) информационной управляющей ЛВС, включая технические аспекты информационной безопасности.

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.

Внутренняя сеть – внутренний участок корпоративной сети, отделенный от внешней сети (сети Интернет) и DMZ межсетевым экраном. Внутренняя сеть объединяет производственные, тестовые, административные сети и сети разработчиков.

Демилитаризованная зона (DMZ) – участок корпоративной сети, расположенный между внешним МЭ и внешним маршрутизатором, используемым для подключения корпоративной сети к сети телекоммуникационных провайдеров (сети Интернет). В DMZ размещаются серверы, используемые для взаимодействия и предоставления сетевых сервисов внешним пользователям корпоративной сети, а также серверы, которые по соображениям информационной безопасности не целесообразно размещать во внутренней сети МБОУ «СОШ №106»

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, характеризуемое способностью АС обеспечивать беспрепятственный доступ к информации субъектов имеющих на это полномочия.

Защищенный канал передачи данных – логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных (средствами VPN), либо путем их физической изоляции и размещения на охраняемой территории.

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 среда – совокупность информационно-телекоммуникационной системы МБОУ «СОШ №106», процессов, источников и потребителей информации, обслуживающего персонала и пользователей информационных систем, обеспечивающего автоматизацию производственных процессов МБОУ «СОШ №106».

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения производственных задач подразделений МБОУ «СОШ №106». В МБОУ «СОШ №106» используются различные типы информационных систем для решения производственных, управленческих, учетных и других задач.

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 МБОУ «СОШ №106», 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 средства – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая

эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий, используемая в производственных - процессах МБОУ «СОШ №106».

Инфраструктура открытых ключей (ИОК, PKI) – технологическая инфраструктура и сервисы, обеспечивающие безопасность информационных и коммуникационных систем на основе использования криптографических алгоритмов и сертификатов ключей подписей.

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 МБОУ «СОШ №106», посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений МБОУ «СОШ №106», привести к причинению МБОУ «СОШ №106» материального или иного вида ущерба.

Криптопровайдер – программный или программно-аппаратный модуль, реализующий алгоритмы шифрования.

Локальная вычислительная сеть (ЛВС) – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран (МЭ) – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав корпоративной сети, а также между корпоративной сетью и внешними сетями (сетью Интернет).

Менеджмент риска – скоординированные действия по руководству и управлению учреждением в отношении риска.

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.

Операционная система – системная программа, осуществляющая взаимодействие пользователя и прикладных программ с аппаратной частью ЭВМ.

Остаточный риск – риск, остающийся после обработки риска.

Ответственное лицо (администратор) информационных активов – сотрудник МБОУ «СОШ №106», получивший на основании соответствующего распорядительного документа права обладателя информации, обрабатываемой в информационной системе Примечание: Понятия «Ответственное лицо (администратор) информационных активов» и «владелец информационных средств (ресурсов)» идентичны.

Оценивание риска – процесс сравнения оцененного риска с данными критериями риска для определения значимости риска.

Оценка риска – общий процесс анализа риска и оценивания риска.

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 взаиМБОУвязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в учреждении для обеспечения его информационной безопасности.

Пользователь ЛВС – сотрудник МБОУ «СОШ №106» (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в корпоративной сети в установленном порядке и получивший права на доступ к ресурсам корпоративной сети в соответствии со своими функциональными обязанностями.

Принятие риска – решение принять риск.

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, приложении 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., название подразделения, телефоны, E-mail и т.п.

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

Сервер – выделенный компьютер, имеющий разделяемые ресурсы, выполняющий определенный перечень задач и предоставляющий пользователям ЛВС ряд сервисов.

Сетевые (информационные) сервисы – сетевые приложения, предоставляющие различные виды сервисов для внутренних и внешних пользователей корпоративной сети, включая DNS, FTP, HTTP, Telnet, и другие.

Система менеджмента информационной безопасности (СМИБ) – та часть общей системы менеджмента, которая основана на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и совершенствовании информационной безопасности.

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

Список контроля доступа (ACL) – правила фильтрации сетевых пакетов, настраиваемые на маршрутизаторах и МЭ, определяющие критерии фильтрации и действия, производимые над пакетами.

Собственник – лицо или организация, которые имеют утвержденные обязательства по менеджменту для контроля производства, разработки, поддержки, использования и безопасности активов. Термин «собственник» не означает, что лицо действительно имеет какие-либо права собственности на актив.

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).

Структурное подразделение – структурное подразделение учреждения с самостоятельными функциями, задачами и ответственностью.

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.

Удостоверяющий центр – автоматизированная система, включающая в себя аппаратно-программные средства, нормативно-методическую документацию и пользователей.

Узел – совокупность ЛВС МБОУ «СОШ №106», расположенных в пределах одной контролируемой зоны.

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, характеризуемое 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.

VPN (VIRTUAL PRIVATE NETWORK) – «Виртуальная частная сеть»: технология и организация систематической удаленной связи между выбранными группами узлов в крупных распределенных сетях.

3. Обозначения и сокращения

АРМ – Автоматизированное рабочее место.
АС – Автоматизированная система.
БД – База данных.
ЗИ – Защита информации.
ИБ – Информационная безопасность.
ИОК – Инфраструктура открытых ключей.
ИС – Информационная система.
ИТС – Информационно-телекоммуникационная система.
КЗ – Контролируемая зона.
МЭ – Межсетевой экран.
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.

4. Политики информационной безопасности МБОУ «СОШ №106».

4.1. Назначение политик информационной безопасности

Политики информационной безопасности МБОУ «СОШ №106» – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в МБОУ «СОШ №106».

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

Политики информационной безопасности относятся к административным мерам обеспечения информационной безопасности и определяют стратегию МБОУ «СОШ №106» в области ИБ.

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

Все документально оформленные решения, формирующие Политики, должны быть утверждены руководителем учреждения.

4.2. Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются следующие:

- Постоянный и всесторонний анализ информационного пространства общества с целью выявления уязвимостей информационных активов.
- 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.
- Персонификация и адекватное разделение ролей и ответственности между сотрудниками учреждения, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

4.3. Соответствие ПБ действующему законодательству

Правовую основу политик составляют Конституция Российской Федерации, законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, МБОУ «СОШ №106» и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

4.4. Ответственность за реализацию политик информационной безопасности

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

Ответственность за реализацию политик возлагается:

- в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на администратора информационной безопасности;
- в части, касающейся доведения правил политик до сотрудников МБОУ «СОШ №106», а также иных лиц (см. область действия настоящей политики) – на администратора информационной безопасности;
- в части, касающейся исполнения правил политики, – на каждого сотрудника МБОУ «СОШ №106», согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

4.5.Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация просвещения сотрудников МБОУ «СОШ №106» в области информационной безопасности возлагается на администратора информационной безопасности. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности». Обучение сотрудников МБОУ «СОШ №106» правилам обращения с конфиденциальной информацией, проводится путем:

- проведения администратором информационной безопасности инструктивных занятий с сотрудниками, принимаемыми на работу в МБОУ «СОШ №106»;
- самостоятельного изучения сотрудниками внутренних нормативных документов МБОУ «СОШ №106».

Допуск персонала к работе с информационными ресурсами МБОУ «СОШ №106» осуществляется только после его ознакомления с настоящими политиками, а также после ознакомления пользователей с «Инструкцией по работе пользователей в АС МБОУ «СОШ №106», а так же иными инструкциями пользователей отдельных информационных систем. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Допуск персонала к работе с конфиденциальной информацией МБОУ «СОШ №106» осуществляется после ознакомления с «Инструкцией по обращению с носителями конфиденциальной информации». Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками МБОУ «СОШ №106», определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

4.6.Защищаемые информационные ресурсы МБОУ «СОШ №106»

Различаются следующие категории информационных ресурсов, подлежащих защите в МБОУ «СОШ №106»:

Конфиденциальная – информация, определенная в соответствии с Федеральным Законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне», ФЗ от 27.07.2006 г. №152-ФЗ «О персональных данных», указом президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера», постановлением правительства РФ от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», предусмотренная Перечнем сведений конфиденциального характера.

Публичная – информация, получаемая из публичных источников (публикации в СМИ, теле и радиовещание и т.д.). Информация, предназначенная для размещения на внешних публичных ресурсах;

Открытая – информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят. Информация, сформированная в результате деятельности МБОУ «СОШ №106», которую запрещено относить конфиденциальной на основании законодательства России. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности МБОУ «СОШ №106» или имеющая принципиальное значение для имиджа МБОУ «СОШ №106»;

Ограниченного доступа – информация, не попадающая под остальные категории, доступ к которой должен быть ограничен определенной категории лиц.

Конфиденциальная информация представляет собой сведения ограниченного доступа, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

Правила отнесения информации к конфиденциальной и порядок работы с конфиденциальными документами, определяются «Перечнем сведений конфиденциального характера» и «Инструкцией по организации работы с материальными носителями конфиденциальной информации».

Подходы к решению проблемы защиты информации в МБОУ «СОШ №106», в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования производственных процессов МБОУ «СОШ №106». Для этого в МБОУ «СОШ №106» выполняются следующие мероприятия:

- определяется порядок работы с документами, образцами изделиями и др., содержащими конфиденциальные сведения;
- устанавливается круг лиц и порядок доступа к подобной информации;
- вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения;
- включаются в трудовые договоры с сотрудниками обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

Форма подписки о неразглашении конфиденциальной информации подписывается при заключении трудового договора, который подписывается всеми сотрудниками учреждения при приеме на работу в МБОУ «СОШ №106». Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых МБОУ «СОШ №106» с другими организациями. Персональные данные сотрудника учреждения – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника.

Согласно Ст.86 п.7 Трудового кодекса РФ защита персональных данных сотрудника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

Согласно Ст.88 Трудового кодекса РФ при передаче персональных данных сотрудника работодатель должен соблюдать следующие требования:

- осуществлять передачу персональных данных сотрудника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым сотрудник должен быть ознакомлен под расписку;
- разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретных функций.

Согласно Ст.90 Трудового кодекса РФ лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

4.7.Политики информационной безопасности

4.7.1. Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к информационным ресурсам МБОУ «СОШ №106».

4.7.2. Политика использования паролей

4.7.2.1. Назначение

Настоящая политика определяет основные правила обращения с паролями, используемыми для доступа к информационным активам МБОУ «СОШ №106».

4.7.2.2. Положения политики

Положения политики закрепляются в «Инструкции по парольной защите в АС».

4.7.3. Политика реализации антивирусной защиты

4.7.3.1. Назначение

Настоящая Политика определяет основные правила для реализации антивирусной защиты в МБОУ «СОШ №106».

4.7.3.2. Положения политики

Положения политики закрепляются в «Инструкции по проведению антивирусного контроля в АС».

4.7.4. Политика защиты АРМ

4.7.4.1. Назначение

Настоящая Политика определяет основные правила и требования по защите конфиденциальной информации МБОУ «СОШ №106» от неавторизованного доступа, утраты или модификации.

4.7.4.2. Положения политики

Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратор информационной безопасности. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к корпоративной информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры. Конфигурация программ на компьютерах должна проверяться на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к лаборанту информатики.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции

пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками МБОУ «СОШ №106». Запрещается использование указанных АРМ другими пользователями без согласования заместителем директора по ИКТ. При передаче указанного АРМ другому пользователю, должна производится гарантированная очистка диска (форматирование).

Лаборант информатики вправе отказать в устранении проблемы, вызванной наличием на рабочем месте программного обеспечения или оборудования, установленного или настроенного пользователем в обход действующей процедуры.

4.8.Порядок сопровождения ИС МБОУ «СОШ №106».

Обеспечение информационной безопасности информационных систем на стадиях жизненного цикла ИБ ИС должна обеспечиваться на всех стадиях жизненного цикла (ЖЦ) ИС, автоматизирующих технологические процессы, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации). Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводится при участии заместителя директора по ИКТ и лаборанта информатики. Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться.

При разработке ИС необходимо придерживаться требований и методических указаний, определенных стандартами, входящими в группу ГОСТ 34.ххх «Стандарты информационной технологии».

Ввод в действие, эксплуатация, снятие с эксплуатации ИС в части вопросов ИБ должны осуществляться при заместителе директора по ИКТ.

На стадиях, связанных с разработкой ИС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

- неверной формулировки требований к ИС;
- выбора неадекватной модели ЖЦ ИС, в том числе неадекватного выбора процессов ЖЦ и вовлеченных в них участников;
- принятия неверных проектных решений;
- внесения разработчиком дефектов на уровне архитектурных решений;
- внесения разработчиком недокументированных возможностей в ИС;
- неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к ИС;
- разработки некачественной документации;
- сборки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований;
- неверного конфигурирования ИС;
- приемки ИС, не отвечающей требованиям заказчика;
- внесения недокументированных возможностей в ИС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

Привлекаемые для разработки и (или) производства средств и систем защиты ИС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ.

При приобретении готовых ИС и их компонентов разработчиком должна быть предоставлена документация, содержащая, в том числе, описание защитных мер, предпринятых разработчиком в отношении угроз информационной безопасности.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком ИС и их компонентов относительно безопасности разработки, безопасности поставки, эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, оценки уязвимости. Данная документация может быть представлена в рамках декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки.

В договор (контракт) о поставке ИС и их компонентов рекомендуется включать положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность приобретения полного комплекта рабочей конструкторской документации на изделие, обеспечивающее возможность сопровождения ИС и их компонентов без участия разработчика.

На стадии эксплуатации должна быть обеспечена защита от следующих угроз:

- умышленное несанкционированное раскрытие, модификация или уничтожение информации;
- неумышленная модификация или уничтожение информации;
- недоставка или ошибочная доставка информации;
- отказ в обслуживании или ухудшение обслуживания.

Кроме этого, актуальной является угроза отказа от авторства сообщения. На стадии сопровождения должна быть обеспечена защита от угроз:

- внесения изменений в ИС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей;
- невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС.

На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб МБОУ «СОШ №106», и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС или с внешних носителей.

Требования ИБ должны включаться во все договора и контракты на проведение работ или оказание услуг на всех стадиях ЖЦ ИС.

4.8.1. Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений политик информационной безопасности понимается предупреждение возможных нарушений информационной безопасности в МБОУ «СОШ №106» и проведение разъяснительной работы по информационной безопасности среди пользователей МБОУ «СОШ №106».

Задача предупреждения в ИС МБОУ «СОШ №106» возможных нарушений информационной безопасности решается по мере наступления следующих событий:

- включение в состав ИС МБОУ «СОШ №106» новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС МБОУ «СОШ №106»;
- изменение конфигурации программных и технических средств ИС МБОУ «СОШ №106» (изменение конфигурации программного обеспечения рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС МБОУ «СОШ №106»;
- при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения технических средств, используемых в ИС МБОУ «СОШ №106».

Заместитель директора по ИКТ (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 МБОУ «СОШ №106». Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний,

общественных объединений и других организаций, специализирующихся в области защиты информации.

Заместитель директора по ИКТ (при помощи сторонней организации, специализирующейся в области информационной безопасности) организовывает периодическую проверку СЗИ ИС МБОУ «СОШ №106» путем моделирования возможных попыток осуществления НСД к защищаемым информационным ресурсам.

Плановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников МБОУ «СОШ №106» по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в МБОУ «СОШ №106», проводится заместителем директора по ИКТ при пересмотре настоящих политик, при возникновении инцидента нарушения правил настоящих политик и при приеме на работу новых сотрудников МБОУ «СОШ №106».

4.8.2. Ответственность нарушителей ПБ

Ответственность за выполнение правил Политик безопасности несет каждый сотрудник МБОУ «СОШ №106» в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политики безопасности МБОУ «СОШ №106», 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 МБОУ «СОШ №106» в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса РФ).

За умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, сотрудники МБОУ «СОШ №106» несут материальную ответственность в полном размере причиненного ущерба (Ст. 243 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 МБОУ «СОШ №106» несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.