ПРИНЯТО
собранием трудового коллектива
МАОУ «ГМУК №2»
24.12.2021
Протокол № 7

УТВЕРЖДАЮ
Директор МАОУ «ГМУК №2»
_____ М.А. Золотова
30.12.2021
Приказ № 581/1-пр от 30.12.2021

Золотова Марина Анатольевна

Подписано цифровой подписью: Золотова Марина Анатольевна
Дата: 2022.04.21 11:19:14 +03'00'

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Муниципального автономного общеобразовательного учреждения г. Владимира «Городской межшкольный учебный комбинат № 2»

г. Владимир – 2021 г.

Содержание

Термины и определения

В настоящем документе используются следующие термины и их определения.

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

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения информации, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки информации или в помещениях, в которых установлены информационные системы.

Государственная информационная система – федеральная информационная система и региональная информационная система, созданная на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

Доступ в операционную среду компьютера – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и её использования.

Закладочное устройство – элемент средства съёма информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съёма информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

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

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Нарушитель безопасности информации – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при их обработке техническими средствами в информационных системах.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит своё отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации),программные средства (операционные системы, системы управления БД и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов.

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

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы – лицо, участвующее в функционировании информационной системы или использующее результаты её функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесённый в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие информации – умышленное или случайное нарушение конфиденциальности информации.

Распространение информации – действия, направленные на передачу информации определённому кругу лиц или на ознакомление с информацией неограниченного круга лиц, в том числе обнародование информации в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к информации каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности информации – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при их обработке в информационных системах.

Уничтожение информации – действия, в результате которых невозможно восстановить содержание информации в информационной системе или в результате которых уничтожаются материальные носители.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

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

Обозначения и сокращения

АИС	Автоматизированная информационная система
БД	База данных
ИБ	Информационная безопасность
ИС	Информационная система
КЗ	Контролируемая зона
НСД	Несанкционированный доступ
ПО	Программное обеспечение
СЗИ	Средства защиты информации
СЗПДн	Система защиты персональных данных
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю

1. Введение

Настоящая Концепция информационной безопасности (далее – Концепция) является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности (далее – ИБ) МАОУ «ГМУК № 2» (далее – Учебный комбинат).

Необходимость разработки Концепции обусловлена расширением сферы применения новейших информационных технологий и процессов при обработке информации.

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (далее – СЗПДн) в Учебном комбинате. Концепция определяет основные требования и базовые подходы к их реализации для достижения требуемого уровня защищенности для автоматизированных информационных систем (далее - ИС) в Учебном комбинате.

Концепция разработана в соответствии с системным подходом к обеспечению ИБ. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз ИБ и разработку СЗПДн с позиции комплексного применения технических и организационных мер и средств защиты.

Под ИБ Учебного комбината понимается защищённость информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, в том числе персональные данные (далее – информация) и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, её владельцам (субъектам) или инфраструктуре. Задачи ИБ сводятся минимизации ущерба от возможной реализации угроз безопасности информации, а также к прогнозированию и предотвращению таких воздействий.

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению ИБ в Учебном комбинате, а также нормативных и методических документов, обеспечивающих её реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности информации Учебного комбината;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности, и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности в ИС.

Область применения Концепции распространяется на все подразделения Учебного комбината, эксплуатирующие технические и программные средства ИС, в которых осуществляется автоматизированная обработка информации, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИС.

Правовой базой для разработки настоящей Концепции служат требования действующих в Российской Федерации законодательных и нормативных актов по вопросам информационной безопасности.

2. Общие положения

СЗПДн представляет собой совокупность организационных и технических мероприятий для защиты информации от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий с ними.

Безопасность информации достигается путём исключения несанкционированного, в том числе случайного, доступа к ней, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение, а также иных несанкционированных действий.

Структура, состав и основные функции СЗПДн определяются исходя из класса защищенности ИС и уровня значимости информации. СЗПДн включает в себя организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки информации), а также используемые в ИС информационные технологии.

Эти меры призваны обеспечить:

- конфиденциальность информации;
- целостность информации;
- доступность информации.

Стадии создания СЗПДн включают:

- предпроектная стадия, включающая предпроектное обследование ИС, разработку технического (частного технического) задания на создание СЗПДн;
- стадия проектирования и реализации СЗПДн, включающая разработку Технического проекта на построение системы защиты информации;
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приёмо-сдаточные испытания СЗПДн, а также оценку соответствия ИС требованиям ИБ.

Организационные меры предусматривают создание и поддержание правовой базы безопасности информации и разработку (введение в действие) предусмотренных Политикой информационной безопасности ИС.

Технические меры защиты реализуются при помощи соответствующих программно-технических средств защиты информации.

Перечень необходимых мер защиты информации определяется по результатам обследования ИС.

3. Задачи СЗПДн

Основной целью создания СЗПДн является минимизация ущерба от возможной реализации угроз безопасности информации.

Для достижения основной цели система безопасности информации ИС должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИС посторонних лиц (возможность использования ИС и доступ к её ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИС (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИС для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:
  - к информации, циркулирующей в ИС;
  - средствам вычислительной техники ИС;
  - аппаратным, программным и криптографическим средствам защиты, используемым в ИС;
- регистрацию действий пользователей при использовании защищаемых ресурсов ИС в системных журналах и периодический контроль корректности действий пользователей системы путём анализа содержимого этих журналов;
- контроль целостности (обеспечение неизменности) среды исполнения программ и её восстановление в случае нарушения;
- защиту от несанкционированной модификации и контроль целостности используемых в ИС программных средств, а также защиту системы от внедрения несанкционированных программ;
- защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- защиту информации, хранимую, обрабатываемую и передаваемую по каналам связи, от несанкционированного разглашения или искажения;
- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;
- своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба субъектам, создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

4. Объекты защиты

4.1 Перечень информационных систем

В Учебном комбинате производится обработка информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

Перечень ИС, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, определяется на основании «Отчёта по результатам обследования».

4.2 Перечень объектов защиты

Объектами защиты являются информация, обрабатываемая в ИС, и технические средства ее обработки и защиты. Информации, подлежащая защите, определяется на основании «Отчёта по результатам обследования».

К объекты защиты относятся:

- обрабатываемая информация;
- технологическая информация;
- программно-технические средства обработки;
- средства защиты информации;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИС.

5. Классификация пользователей ИС

Пользователем ИС является лицо, участвующее в функционировании информационной системы или использующее результаты её функционирования. Также пользователем ИС является любой сотрудник Учебного комбината, имеющий доступ к ИС и её ресурсам в соответствии с установленным порядком и в соответствии с его функциональными обязанностями.

Пользователи ИС делятся на три основные категории (роли):

1. Администратор ИС - сотрудники Учебного комбината, которые занимаются настройкой, внедрением и сопровождением системы. Администратор ИС обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном ПО ИС;
- обладает полной информацией о технических средствах и конфигурации ИС;
- имеет доступ ко всем техническим средствам обработки информации и данным ИС;
- обладает правами конфигурирования и административной настройки технических средств ИС.

2. Разработчик ИС - сотрудники Учебного комбината или сторонних организаций, которые занимаются разработкой ПО ИС. Программист-разработчик ИС обладает следующим уровнем доступа:

- обладает информацией об алгоритмах и программах обработки информации ИС;

 обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИС на стадиях её разработки, внедрения и сопровождения;

 может располагать любыми фрагментами информации о топологии ИС и технических средствах обработки и защиты информации, обрабатываемой в ИС;

3. Оператор ИС- сотрудники ИС, участвующих в процессе эксплуатации ИС. Оператор ИС обладает следующим уровнем доступа:

 обладает всеми необходимыми атрибутами (например, идентификатором и паролем), обеспечивающими доступ к некоторому подмножеству информации;

 располагает конфиденциальными данными, к которым имеет доступ.

Категории пользователей должны быть определены для каждой ИС. При построении СЗПДн требуется уточнение разделения сотрудников Учебного комбината внутри категорий, в соответствии с типами пользователей, определёнными в Политике информационной безопасности ИС.

Все выявленные группы (роли) пользователей отражаются в «Отчёте по результатам обследования». На основании Отчёта выявляются права доступа к элементам ИС для всех групп (ролей) пользователей и отражаются в Матрице доступа в Положении о разграничении прав доступа к обрабатываемой информации.

6. Основные принципы построения системы защиты информации

Построение системы обеспечения безопасности информации ИС в Учебном комбинате и её функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

6.1 Законность

Предполагает осуществление защитных мероприятий и разработку СЗПДн в Учебном комбинате в соответствии с действующим законодательством в области защиты информации и другими нормативными актами по ИБ, утверждёнными органами государственной власти в пределах их компетенции.

Пользователи и обслуживающий персонал ИС должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за нарушение безопасности информации.

6.2 Системность

Системный подход к построению СЗПДн в Учебном комбинате предполагает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения ИБ.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места ИС, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределённые системы и НСД к информации. СЗПДн должна строиться с учётом не только всех известных каналов проникновения и НСД к информации, но и с учётом возможности появления принципиально новых путей реализации угроз безопасности.

6.3 Комплексность

Комплексное использование методов и средств защиты в Учебном комбинате предполагает согласованное применение разнородных средств при построении целостной СЗПДн, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных её компонентов.

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учётом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укреплённых рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

6.4 Непрерывность защиты информации

Защита информации – не разовое мероприятие и не простая совокупность проведённых мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС.

ИС должна находиться в защищённом состоянии на протяжении всего времени функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИС в незащищённое состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имён, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления её функционирования.

6.5 Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите ИС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки ИС в целом и СЗПДн в частности. Разработка СЗПДн должна вестись параллельно с разработкой и развитием самой ИС. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счёте, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищённые системы.

6.6 Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИС и СЗПДн с учётом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

6.7 Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности информации и системы их обработки на каждого сотрудника Учебного комбината в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников Учебного комбината строится таким образом, чтобы в случае любого противоправного действия круг нарушителей был чётко известен или сведен к минимуму.

6.8 Принцип минимизации полномочий

Означает предоставление пользователям ИС минимальных прав доступа в соответствии с производственной необходимостью на основе принципа «всё, что не разрешено, запрещено».

Доступ к информации должен предоставляться только в том случае и объёме, в которых необходимо сотруднику Учебного комбината для выполнения его должностных обязанностей.

6.9 Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе Учебного комбината, обеспечивающего деятельность ИС, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

В такой обстановке сотрудники Учебного комбината должны осознанно соблюдать установленные правила и оказывать содействие деятельности подразделений технической защиты информации.

6.10 Гибкость системы защиты информации

Принятые меры и установленные СЗИ, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности СЗИ должны обладать определённой гибкостью. Особенно важным это свойство является в тех случаях, когда установку СЗИ необходимо осуществлять на работающую систему, не нарушая процесса её нормального функционирования.

6.11 Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов СЗПДн состоит в том, что защита не должна обеспечиваться только за счёт секретности структурной организации и алгоритмов функционирования её подсистем. Знание алгоритмов работы СЗПДн не должно давать возможности её преодоления (даже авторам). Однако это не означает, что информация о СЗПДн должна быть общедоступна.

6.12 Простота применения средств защиты

Механизмы работы СЗПДн должны быть интуитивно понятны и просты в использовании. Применение СЗИ не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных и малопонятных ему операций (ввод нескольких паролей и имён и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИС.

6.13 Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации в СЗПДн должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации.

СЗПДН должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

6.14 Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информации, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация СЗИ должна осуществляться профессионально подготовленными специалистами.

6.15 Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и СЗИ при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль над деятельностью любого пользователя, каждого СЗИ и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

7. Меры, методы и средства обеспечения требуемого уровня защищённости

Обеспечение требуемого уровня защищённости ИС должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИС подразделяются на:

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

7.1 Законодательные (правовые) меры защиты

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

7.2 Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утверждённые нормативные акты, однако, их несоблюдение ведёт обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе Учебного комбината. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

7.3 Организационные (административные) меры защиты

Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования ИС, использование ресурсов ИС, деятельность сотрудников Учебного комбината и сторонних организаций, а также порядок взаимодействия пользователей с ИС таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз ИБ или снизить размер потерь в случае их реализации.

Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать Политику информационной безопасности ИС, отражающую подходы к защите информации, и обеспечить её выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности в ИС состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность ИС в целом. Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

 принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности информации, определение ответственных за её реализацию;

 формулирование целей, постановка задач, определение направлений деятельности Учебного комбината в области безопасности информации;

 принятие решений по вопросам реализации программы безопасности;

 обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна чётко очертить сферу влияния и ограничения при определении целей безопасности информации, определить, какими ресурсами (материальные, персонал) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИС.

На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности информации в Учебном комбинате. Эти правила определяют:

 какова область применения политики безопасности информации;

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

 кто имеет права доступа к информации;

 какими мерами и средствами обеспечивается защита информации;

 какими мерами и средствами обеспечивается контроль соблюдения введённого 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 информации;

 определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов СЗПДн;

 организовать меры противодействия НСД к информации пользователями на этапах идентификации, аутентификации и авторизации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

Организационные меры должны состоять из:

 регламента доступа в помещения Учебного комбината;

 порядок допуска сотрудников к ИС;

 регламента процессов ведения БД и осуществления модификации информационных ресурсов;

 регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИС;

 инструкций пользователей ИС (администратора ИС, администратора безопасности ИС, операторов ИС);

 инструкции пользователя при возникновении нештатных ситуаций.

7.4 Физические меры защиты

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 путём 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.

7.5 Аппаратно-программные средства защиты информации

Технические (аппаратно-программные) меры защиты информации основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, обеспечение целостности и т.д.).

С учётом всех требований и принципов обеспечения безопасности информации в ИС по всем направлениям защиты в состав СЗПДн могут быть включены следующие средства:

 средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей;

 средства разграничения доступа зарегистрированных пользователей к ресурсам;

 средства обеспечения и контроля целостности программных и информационных ресурсов;

 средства оперативного контроля и регистрации событий безопасности;

 средства обнаружения и предотвращения вторжений;

 средства анализ защищённости;

 средства межсетевого экранирования;

 антивирусные средства; СКЗИ.

Успешное применение технических средств защиты на основании принципов предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

 обеспечена физическая целостность всех компонент ИС;

 каждый сотрудник (пользователь ИС) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

 в ИС разработка и отладка программ осуществляется за пределами ИС, на испытательных стендах;

 все изменения конфигурации технических и программных средств ИС производятся строго в установленном порядке (регистрируются и контролируются) только на основании распоряжений вышестоящих организаций;

 сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, не доступных для посторонних (специальных помещениях, шкафах, и т.п.).

 специалистами по ИБ осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

8. Контроль эффективности системы защиты ИС

Контроль эффективности СЗПДн должен осуществляться на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы системы защиты (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности информации.

Контроль СЗПДн может проводиться как администратором безопасности ИС (оперативный контроль в процессе информационного взаимодействия в ИС), а также ФСТЭК России и ФСБ России в пределах их компетенции.

Контроль может осуществляться администратором безопасности ИС как с помощью штатных средств СЗПДн, так и с помощью специальных программных средств контроля.

Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

9. Сферы ответственности за безопасность информации

Ответственным за разработку мер и контроль над обеспечением безопасности информации является директор Учебного комбината (далее – Руководитель). Руководитель может делегировать часть полномочий по обеспечению безопасности информации.

Сфера ответственности Руководителя включает следующие направления обеспечения безопасности информации:

 планирование и реализация мер по обеспечению безопасности информации;

 анализ угроз безопасности информации;

 разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности информации в Учебном комбинате;

 контроль защищённости информационной инфраструктуры от угроз ИБ;

 обучение и информирование пользователей ИС о порядке работы с техническими средствами;

 предотвращение, выявление, реагирование и расследование нарушений безопасности информации.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты, с этими организациями должно быть заключено «Соглашение о конфиденциальности» либо «Соглашение о соблюдении режима безопасности информации при выполнении работ».

10. Модель нарушителя безопасности

Под нарушителем понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты .

Нарушители подразделяются по признаку принадлежности к ИС. Все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории КЗ, в пределах которой размещается оборудование ИС;
- внутренние нарушители – физические лица, имеющие право пребывания на территории КЗ, в пределах которой размещается оборудование ИС.

11. Модель угроз безопасности

Для ИС выделяются следующие основные категории угроз безопасности информации:

- угрозы от утечки по техническим канала;
- угрозы несанкционированного доступа к информации:
- угрозы уничтожения, хищения аппаратных средств ИС, носителей информации путем физического доступа к элементам ИС;
- угрозы хищения, несанкционированной модификации или блокирования информации за счёт НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);
- угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИС;
- в результате сбоев ПО, а также угрозы неантропогенного (сбоев аппаратуры из-за ненадёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;
- угрозы преднамеренных действий внутренних нарушителей; о угрозы НСД по каналам связи.

12. Механизм реализации Концепции

Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения ИБ и защиты информации;
- постановлений Правительства Российской Федерации;
- руководящих, организационно-распорядительных и методических документов ФСТЭК России и ФСБ России;
- потребностей ИС в средствах обеспечения безопасности информации.

13. Ожидаемый эффект от реализации Концепции

Реализация Концепции информационной безопасности в ИС позволит:

- оценить состояние безопасности информации в ИС, выявить источники внутренних и внешних угроз ИБ, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;
- разработать распорядительные и нормативно-методические документы, применительно к ИС;
- провести организационно-режимные и технические мероприятия по обеспечению безопасности информации в ИС;
- обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной СЗПДн и создаст условия для её дальнейшего совершенствования.

Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящая Концепция, являются:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
3. Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
4. Постановление Правительства РФ от 24 октября 2011 г. № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)»;
5. Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
6. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
7. Приказ ФАПСИ от 13 июня 2001 г. № 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»;
8. Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения оразработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

9. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
10. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
11. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённая Заместителем директора ФСТЭК России 15 февраля 2008 г.;
12. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённая Заместителем директора ФСТЭК России 15 февраля 2008 г.