Приложение

к приказу колледжа

от 22.03.2022 № 179-П

|  |
| --- |
| Профессионально-педагогический колледж федерального государственного бюджетного образовательного учреждения высшего образования «Саратовский государственный технический университет имени Гагарина Ю.А.» |
| **Концепция** **информационной безопасности** **Профессионально-педагогического колледжа** **СГТУ имени Гагарина Ю.А.** |
|  |
| Саратов 2022 |

**Содержание**

Определения

Обозначения и сокращения

Введение

1. Общие положения
2. Задачи СЗИ
3. Объекты защиты
	* 1. Перечень ИС
		2. Перечень объектов защиты
4. Классификация пользователей ИС
5. Основные принципы построения СЗИ
	* 1. Законность
		2. Системность
		3. Комплексность
		4. Непрерывность
		5. Своевременность
		6. Преемственность и совершенствование
		7. Персональная ответственность
		8. Принцип минимизации полномочий
		9. Взаимодействие и сотрудничество
		10. Гибкость СЗИ
		11. Открытость алгоритмов и механизмов защиты
		12. Простота применения средств защиты
		13. Научная обоснованность и техническая реализуемость
		14. Специализация и профессионализм
		15. Обязательность контроля
6. Меры и средства обеспечения требуемого уровня защищенности
	* 1. Законодательные (правовые) меры
		2. Организационные (административные) меры
		3. Физические меры
		4. Аппаратно-программные средства
7. Контроль эффективности системы защиты
8. Сферы ответственности за ИБ
9. Нарушители безопасности
10. Угрозы безопасности
11. Механизм реализации концепции
12. Ожидаемый эффект от реализации концепции

**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 пользователя –** подтверждение того, что пользователь соответствует заявленному.

**Безопасность информации (данных) –** состояние защищенности информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при её обработке в информационных системах.

**Блокирование информации (данных) –** временное прекращение сбора, систематизации, накопления, использования, распространения информации, в том числе её передачи.

**Вредоносная программа –** программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационных систем.

**Доступ к информации (данным) –** возможность получения и использования информации.

**Защищаемая информация (защищаемые данные) –** информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требований, устанавливаемыми собственником информации.

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

**Информативный сигнал –** электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная (служебная, коммерческая) информация, обрабатываемая в информационных системах.

**Информационная система –** система, представляющая собой совокупность информации, а также информационных технологий и технических средств, позволяющих осуществлять обработку информации с использованием средств автоматизации или без использования таких средств.

**Информационная безопасность –** защищенность информационных систем (информации и обрабатывающей её инфраструктуры) от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, её владельцам или инфраструктуре.

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

**Использование информации (данных) –** действия (операции) с данными, совершаемыми в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта данных или других лиц либо иным образом затрагивающих права и свободы субъекта данных или других лиц.

**Источник угрозы безопасности –** 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 средств, технических и иных материальных средств.

**Конфиденциальность информации (данных) –** обязательное для соблюдения требование не допускать распространение информации без согласия владельца информации или наличия иного законного основания.

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

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

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

**Обработка информации (данных) –** действия (операции) с информацией, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение информации.

**Объект доступа –** единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

**Технические средства информационных систем –** средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема 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 базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

**Перехват информации (данных) –** неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информационных сигналов.

**Пользователь информационных систем –** лицо, участвующее в функционировании информационной системы либо использующее результаты её функционирования.

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

**Программное воздействие –** несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Распространение информации (данных) –** действия, направленные на передачу информации определенному 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 образом.

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

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

**Субъект доступа (субъект) –** лицо или процесс, действие которого регламентируется правилами разграничения доступа.

**Система защиты информации (данных) –** совокупность организационных и технических мероприятий для защиты информации от неправомерного илислучайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий с ней.

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

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

**Уничтожение информации (данных) –** действия, в результате которых невозможно восстановить содержание информации в информационных системах, или в результате которых уничтожаются материальные носители информации.

**Утечка информации (данных) по техническим каналам связи –** 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 (данных) –** способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях её случайного и (или) преднамеренного искажения (разрушения).

**Обозначения и сокращения**

**АС –** автоматизированная система

**БД –** база данных

**ИБ** – информационная безопасность

**ИС** – информационная система

**ЛВС** – локально-вычислительная сеть

**НСД** – несанкционированный доступ

**СЗИ** – система (подсистема) защиты информации

**Введение**

Настоящая Концепция информационной безопасности Профессионально-педагогического колледжа СГТУ имени Гагарина Ю.А. (далее – Колледж, Концепция) является официальным документом, в котором в самом общем виде сформулированы цели и приоритеты Колледжа в области информационной безопасности, намечены общие пути достижения этих целей.

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

Задачи ИБ сводятся к минимизации ущерба от возможной реализации угроз безопасности информации, а также к прогнозированию и предотвращению таких воздействий.

Концепция является методологической основой для:

- формирования и проведения единой Политики ИБ Колледжа;

- принятия управленческих решений и разработки практических мер по воплощению Политики ИБ Колледжа;

- выработки комплекса согласованных мер нормативного, организационного и технического характера, направленных на предупреждение, выявление, отражение и ликвидацию последствий реализации различных видов угроз;

- координации деятельности структурных подразделений Колледжа при проведении работ по развитию и эксплуатации ИС с соблюдением требований обеспечения ИБ;

- разработки предложений по совершенствованию нормативного, организационного, методического и технического обеспечения ИБ ИС Колледжа.

Концепция распространяется на все подразделения Колледжа, в которых осуществляется автоматизированная обработка информации, не составляющей государственную тайну, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение функционирования ИС Колледжа, в которых обрабатывается информация, не составляющая государственную тайну. Настоящая Концепция разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

**1. Общие положения**

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения СЗИ в ИС Колледжа. Концепция определяет основные требования и базовые подходы к их реализации для достижения требуемого уровня безопасности информации.

Структура, состав и основные функции СЗИ определяются, исходя из типа ИС.

СЗИ включает организационные и технические меры и средства защиты информации, а также используемые в ИС информационные технологии.

Эти меры призваны обеспечить:

- **конфиденциальность** информации (защиту от несанкционированного ознакомления);

- **целостность** информации (актуальность и непротиворечивость информации, её защищенность от разрушения и несанкционированного изменения);

- **доступность** информации (возможность за приемлемое время получить требуемую информационную услугу).

**Организационные меры** предусматривают создание и поддержание правовой базы ИБ и разработку (введение в действие) необходимых организационно-распорядительных документов:

- политику информационной безопасности Колледжа;

- правила, инструкции, положения, необходимые для обеспечения определенного уровня защищенности информации.

**Технические меры** реализуются при помощи соответствующих программно-технических средств и методов защиты.

**Предполагается:**

- провести внутренний аудит (инвентаризацию) всех ИС Колледжа;

- составить отчет по результатам внутреннего аудита;

- на основании отчета определить перечень необходимых мер защиты информации.

**2. Задачи системы защиты информации**

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

СЗИ должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в функционирование ИС посторонних лиц (возможность использования ИС и доступа к её ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

- разграничение доступа пользователей к аппаратным, программным и информационным ресурсам ИС (доступ 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 НСД:

- к информации, хранящейся и обрабатываемой в ИС;

- к средствам вычислительной техники ИС;

- к 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 путем 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 от внедрения несанкционированных программ;

- защиту информации от утечки по техническим каналам при её обработке, хранении и передачи по каналам связи;

- защиту информации, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

- своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба информации;

- оперативное реагирование на угрозы безопасности информации;

- локализация и минимизация ущерба, наносимого неправомерными действиями физических и юридических лиц;

- ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

**3. Объекты защиты**

**3.1 Перечень информационных систем**

В Колледже производится обработка информации в информационных системах.

Общая ИС Колледжа является распределенной системой, объединяющей автоматизированные ИС (подсистемы) подразделений Колледжа в единую корпоративную вычислительную (информационно-телекоммуникационную) сеть.

В ИС Колледжа циркулирует информация разных категорий. Информация может быть совместно использована различными пользователями из различных подсетей единой вычислительной сети.

В ряде подсистем ИС Колледжа предусмотрено взаимодействие с внешними организациями по различным каналам связи.

Комплекс технических средств ИС Колледжа включает средства обработки данных (компьютеры, серверы, почтовые серверы и т.п.), средства обмена данными в ЛВС с возможностью выхода в глобальные сети (кабельная система, коммутаторы, маршрутизаторы и т.д.), а также средства хранения (в т.ч. архивирования) данных.

Особенности функционирования ИС Колледжа:

- большая территориальная распределённость системы;

- объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;

- большое разнообразие решаемых задач и типов обрабатываемых данных;

- сложные режимы автоматизированной обработки информации, совмещенные с выполнением информационных запросов множества различных категорий пользователей;

- объединение в единых БД информации различного назначения, принадлежности и уровней конфиденциальности;

- большое число каналов взаимодействия с внешними источниками и потребителями информации;

- непрерывность функционирования ИС Колледжа;

- высокая интенсивность информационных потоков;

- наличие в ИС функциональных подсистем с различными требованиями по уровням защищенности (физически объединенных в единую сеть).

Общая структурная и функциональная организация ИС Колледжа определяется организационно-штатной структурой Колледжа и задачами, решаемыми его структурными подразделениями. В самом общем виде, единая телекоммуникационная ИС Колледжа представляет собой совокупность ЛВС отделений Колледжа, объединенных средствами телекоммуникации. Каждая ЛВС в ИС Колледжа объединяет ряд взаимосвязанных и взаимодействующих подсистем, обеспечивающих решение задач отдельными структурными подразделениями Колледжа.

**Предполагается:**

На основании отчета по результатам внутреннего аудита составить перечень ИС Колледжа.

**3.2. Перечень объектов защиты**

Объектами защиты являются: информация, обрабатываемая ИС, и технические средства её обработки и защиты.

Объекты защиты ИС Колледжа включают:

- технологическое оборудование (средства вычислительной техники, сетевое и кабельное оборудование);

- информационные ресурсы, содержащие сведения различной категории доступа и представленные в виде документов или записей в носителях на магнитной, оптической и другой основе, информационных физических полях, массивах и базах данных;

- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение);

- каналы и средства информационного обмена и телекоммуникации;

- технические средства, используемые для создания, тиражирования и обработки информации;

- средства защиты информации;

- объекты и помещения, в которых размещены компоненты ИС.

**Предполагается:**

На основании отчета по результатам внутреннего аудита составить перечень объектов, подлежащих защите в ИС Колледжа.

**4. Классификация пользователей информационных систем**

Пользователем ИС является лицо, участвующее в функционировании ИС или использующее результаты её функционирования. Пользователем ИС является любой обучающийся и работник Колледжа, имеющий доступ к ИС и её ресурсам в соответствии с установленным порядком и его функциональными обязанностями.

Пользователи ИС делятся на три основные категории:

1. **Администраторы ИС.** Работники Колледжа, которые занимаются настройкой, внедрением и сопровождением информационных систем. Администратор ИС обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном программном обеспечении ИС;

- обладает полной информацией о технических средствах и конфигурации ИС;

- имеет доступ ко всем техническим средствам обработки информации и к данным ИС;

- обладает правами конфигурирования и административной настройки технических средств ИС.

2. **Программисты (разработчики) ИС.** Работники Колледжа или сторонних организаций, которые занимаются разработкой программного обеспечения. Разработчик ИС обладает следующим уровнем доступа:

- обладает информацией об алгоритмах и программах обработки данных на ИС;

- может располагать любыми фрагментами сведений о топологии ИС и технических средствах обработки и защиты данных, обрабатываемых в ИС;

3. **Операторы ИС.** Обучающиеся и работники Колледжа, участвующие в процессе эксплуатации ИС. Оператор ИС обладает следующим уровнем доступа:

- обладает всеми необходимыми атрибутами (например, логином и паролем), обеспечивающими доступ к некоторому подмножеству данных;

 - имеет требуемый служебными обязанностями доступ к служебной и конфиденциальной информации.

**5. Основные принципы построения системы защиты информации**

Построение СЗИ ИС Колледжа 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.

**5.1. Законность**

Предполагает осуществление защитных мероприятий и разработку СЗИ Колледжа в соответствии с действующим законодательством в области защиты информации и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

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

**5.2. Системность**

Системный подход к построению СЗИ Колледжа предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения ИБ ИС Колледжа.

При создании системы защиты необходимо учитывать все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации.

Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

**5.3. Комплексность**

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее 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 учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из внешних рубежей могут быть средства криптографической защиты, реализованные с использованием технологии VPN.

Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

**5.4. Непрерывность**

Защита информации (данных) – непрерывный, целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС.

ИС должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИС в незащищенное 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 имен, 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 ее функционирования.

**5.5. Своевременность**

Предполагает упреждающий характер мер обеспечения информационной безопасности, то есть постановку задач по комплексной защите ИС и реализацию мер обеспечения ИБ на ранних стадиях разработки ИС в целом, и ее системы защиты, в частности.

Разработка СЗИ должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

**5.6. Преемственность и совершенствование**

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

**5.7. Персональная ответственность**

Предполагает возложение ответственности за обеспечение безопасности информации и системы её обработки на каждого сотрудника в пределах его полномочий.

В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

**5.8. Принцип минимизации полномочий**

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью, на основе принципа «все, что явно не разрешено — запрещено».

Доступ к информации должен предоставляться только в том времени и объеме, которые необходимы сотруднику для выполнения его должностных обязанностей.

**5.9. Взаимодействие и сотрудничество**

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИС Колледжа, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности по защите информации.

**5.10. Гибкость системы защиты информации**

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важно это в тех случаях, когда применение мер и (или) установка средств защиты осуществляется на работающую систему, без нарушения процессов её нормального функционирования.

**5.11. Открытость алгоритмов и механизмов защиты**

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структуры ИС Колледжа и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления. Однако это не означает, что информация о конкретной системе защиты должна быть общедоступна.

**5.12. Простота применения средств защиты**

Механизмы защиты должны быть понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков программирования или с выполнением действий, требующих значительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных, малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Необходимо стремиться к автоматизации максимального числа действий пользователей и администраторов ИС.

**5.13. Научная обоснованность и техническая реализуемость**

Информационные технологии, технические и программные средства, средства и меры защиты информации 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.

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

**5.14. Специализация и профессионализм**

Предполагает, при необходимости, привлечение к разработке средств и реализации мер защиты информации специализированных организаций, 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 средств защиты должна осуществляться профессионально подготовленными специалистами Колледжа.

**5.15. Обязательность и контроль**

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения правил обеспечения ИБ на основе используемых систем и средств защиты информации. При этом необходимо совершенствовать критерии и методы оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты 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.

1. **Меры и средства обеспечения требуемого уровня защищённости**

Требуемый уровень защищенности информации достигается с использованием необходимых мер, методов и средств защиты. Все меры защиты информации подразделяются на:

- законодательные (правовые);

- организационные (административные);

- физические;

- технические (аппаратные и программные).

**6.1. Законодательные (правовые) меры**

К правовым мерам защиты относятся действующие законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе её 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 ИС.

**6.2. Организационные (административные) меры**

Организационные (административные) меры защиты — это меры, регламентирующие процессы функционирования ИС, использование ресурсов ИС, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИС таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер, предпринимаемых на высшем управленческом уровне — сформировать Политику информационной безопасности и обеспечить ее 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 информационной безопасности, определение ответственных за ее реализацию;

- формулирование целей, постановка задач, определение направлений деятельности в области информационной безопасности;

- принятие решений по вопросам реализации Политики информационной безопасности, которые рассматриваются на уровне Колледжа в целом;

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

Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей информационной безопасности; определить, какими ресурсами (материальными, персональными) 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. Эти правила определяют:

- область применения политики информационной безопасности;

- роли, обязанности и ответственность должностных лиц, отвечающих за реализацию политики информационной безопасности;

- кто имеет права доступа к информации;

- какими мерами и средствами обеспечивается защита информации;

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

Организационные меры должны:

- реализовать правила информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

- определять правила и методы разграничения доступа к информации;

- определять порядок работы с программно-математическими и техническими средствами защиты, других защитных механизмов;

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

Организационные меры могут состоять из:

- правил доступа в помещения ИС;

- правил допуска сотрудников к использованию ресурсов ИС Колледжа;

- описания процессов ведения баз данных и модификации информационных ресурсов;

- описания процессов обслуживания и модификации аппаратных и программных ресурсов ИС;

- инструкций пользователей ИС (администратора безопасности, администратора ИС, оператора ИС);

- инструкций пользователей при возникновении внештатных ситуаций.

**6.3. Физические меры**

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

Физическая защита зданий, помещений, объектов и средств информатизации может осуществляться с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здания, помещения посторонних лиц; хищение информационных носителей, средств обработки и хранения информации, исключающими нахождение внутри контролируемой (охраняемой) зоны несанкционированных технических средств.

**6.4. Аппаратно-программные средства**

Технические (аппаратно-программные) меры защиты информации основаны на использовании электронных устройств и (или) 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, криптографическое закрытие информации и т.д.).

С учетом требований и принципов обеспечения ИБ по всем направлениям защиты, в состав систем защиты могут быть включены следующие средства:

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

- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИС Колледжа;

- средства обеспечения и контроля целостности программных и информационных ресурсов;

- средства оперативного контроля и регистрации событий безопасности;

- криптографические средства защиты информации (при необходимости).

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

- обеспечена физическая целостность всех компонентов 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;

- количество точек доступа к каждой ИС из внешних, по отношению к этой ИС, сетей (интернет, другие подсети Колледжа) сведено к необходимому минимуму;

- коммутационное (узловое) сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.д.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах и т. п.);

- специалистами Колледжа осуществляется непрерывное управление и административная поддержка функционирования средств защиты информации.

1. **Контроль и эффективность системы защиты информации**

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

Контроль может проводиться как администраторами безопасности ИС (оперативный контроль в процессе информационного взаимодействия в ИС), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности.

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

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

1. **Сферы ответственности за информационную безопасность**

Ответственным за разработку мер и контроль над обеспечением ИБ является директор Колледжа.

Директор Колледжа может делегировать свои полномочия в области информационной безопасности.

Сфера ответственности лиц, ответственных за разработку мер и контроль над обеспечением информационной безопасности, включает следующие направления:

- планирование и реализация мер по обеспечению информационной безопасности;

- анализ угроз информационной безопасности;

- разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии Концепций, политик, руководств, процедур, регламентов, инструкций и других организационных документов по обеспечению информационной безопасности;

- контроль защищенности информационно-телекоммуникационной сети Колледжа, в целом, и каждой ИС Колледжа, в частности, от угроз ИБ;

- обучение и информирование пользователей ИС о порядке работы с информацией и средствами защиты информации;

- предотвращение, выявление, реагирование и расследование нарушений информационной безопасности.

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 неразглашении сведений», либо в договор на выполнение работ (оказание услуг) должен быть внесен соответствующий раздел.

1. **Нарушители безопасности**

Под нарушителем понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб информационным системам либо защищаемой информации.

По признаку принадлежности к ИС все нарушители делятся на две группы:

- внутренние нарушители — физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС;

- внешние нарушители — физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС.

**Внутренними нарушителями** могут быть следующие категории лиц:

- зарегистрированные, конечные пользователи ИС Колледжа (работники Колледжа);

- работники Колледжа, не допущенные к работе с ИС Колледжа;

- студенты, командированные, временные работники;

- персонал, обслуживающий технические средства ИС Колледжа (инженеры, техники);

- специалисты по разработке и сопровождению ПО (прикладные и системные программисты);

- технический персонал, обслуживающий здания (уборщицы, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты ИС Колледжа).

**Внешними нарушителями** могут быть следующие категории лиц:

- уволенные сотрудники Колледжа;

- представители организаций, взаимодействующих с Колледжем по вопросам обеспечения жизнедеятельности Колледжа (энерго-, водо-, теплоснабжения и т. п.);

- посетители (приглашённые представители организаций, граждане), представители фирм, поставляющих технику, программное обеспечение, услуги и т. п.;

- лица, случайно или умышленно проникшие в сети Колледжа из внешних (по отношению к Колледжу) сетей телекоммуникации (хакеры).

Пользователи и обслуживающий персонал из числа сотрудников Колледжа имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций.

Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные в Колледже знания и опыт выделяют их среди других источников внешних угроз.

Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в ИС Колледжа.

Организации, занимающиеся разработкой, поставкой и ремонтом оборудования, информационных систем, могут представлять внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

- несанкционированные действия могут быть следствием случайных ошибок пользователей и администраторов, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;

- нарушители скрывают свои несанкционированные действия;

- нарушители могут использовать любые доступные средства для перехвата информации, для воздействия на информацию и информационные системы, а также адекватные средства для влияния на персонал и другие средства и методы для достижения стоящих перед ними целей.

1. **Угрозы безопасности**

Для ИС Колледжа выделяются следующие основные категории угроз безопасности информации:

- угрозы от утечки по техническим каналам (например, по акустическим, акустоэлектрическим, оптическим, индукционным и прочим каналам распространения информации);

- угрозы несанкционированного доступа к информации;

- угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС;

- угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств;

- угрозы несанкционированного удаленного доступа по каналам связи;

- угрозы непреднамеренных действий пользователей;

- угрозы преднамеренных действий внутренних нарушителей;

- угрозы программного характера;

- нарушения безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении;

- нарушения работы операционных систем и прикладного ПО из-за вредоносных программ;

- угрозы технического характера (сбои аппаратуры из-за ненадежности элементов, сбои электропитания);

- угрозы стихийного характера (удары молний, пожары, наводнения и т.п.).

1. **Механизм реализации Концепции**

Реализация Концепции должна осуществляться на основе Политики ИБ, а также положений, правил, инструкций и других требуемых документов, которые составляются на основании и во исполнение:

- законов Российской Федерации в области обеспечения информационной безопасности и защиты информации;

- постановлений Правительства Российской Федерации;

- руководящих, организационно-распорядительных и методических документов ФСБ, ФСТЭК и Роскомнадзора РФ;

- потребностей ИС Колледжа в средствах обеспечения информационной безопасности.

1. **Ожидаемый эффект от реализации Концепции**

Реализация Концепции в ИС Колледжа позволит:

- оценить состояние и уровень информационной безопасности в ИС Колледжа;

- выявить источники внутренних и внешних угроз информационной безопасности;

- определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

- разработать распорядительные и нормативные документы применительно к различным ИС;

- провести классификацию ИС (там, где это необходимо);

- провести организационные и технические мероприятия по обеспечению информационной безопасности в ИС;

- обеспечить необходимый уровень безопасности объектов защиты информации.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИС Колледжа и создаст условия для её дальнейшего совершенствования.