



МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ-ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ
УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

**Совершенствование модели и методов обеспечения информационной
безопасности в образовательной организации на основе физической
защиты**

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения очная

Проверка на объем заимствований:
41,67% авторского текста

Работа рекомендована/ не рекомендована
к защите


«13» 05 2023 г.

Зав. кафедрой АТИТ и МОТД

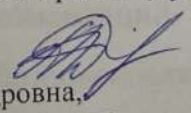
 Руднев В.В.

Выполнил:

Студент группы ОФ-209-210-2-1

Шуралева Елизавета Александровна 

Научный руководитель:

Диденко Галина Александровна, 

кан.пед.н., доцент кафедры АТ, ИТ и
МОТД

Челябинск
2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИССЛЕДОВАНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ НА ОСНОВЕ ФИЗИЧЕСКОЙ ЗАЩИТЫ	9
1.1. Сущность и содержание физической защиты информации в образовательной организации.....	9
1.2 Модели обеспечения информационной безопасности в образовательной организации.....	15
1.3 Виды угроз информационной безопасности в образовательной организации и их характеристика	24
Выводы по главе 1.....	30
ГЛАВА 2 РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО СОВЕРШЕНСТВОВАНИЮ МОДЕЛИ И МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ГБПОУ «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ КОЛЛЕДЖ»	32
2.1 Анализ системы обеспечения информационной безопасности ГБПОУ «Южно-Уральский государственный колледж».....	32
2.2 Мероприятия и средства по совершенствованию модели и методов информационной безопасности колледжа на основе физической защиты.....	41
2.3 Расчет экономической эффективности внедрения рекомендаций по совершенствованию модели и методов информационной безопасности в организации профессионального обучения.....	69
Выводы по главе 2.....	73
ЗАКЛЮЧЕНИЕ	76
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	79

ВВЕДЕНИЕ

Актуальность исследования. В современном мире развитие информационных технологий достигло довольно высокого уровня, однако при этом возросло и количество преступлений в сфере компьютерной информации. Также появилась необходимость обеспечения эффективной защиты пользователей от несанкционированного вторжения и хищения информации. В связи с этим внимание специалистов информационной безопасности было акцентировано на исследовании компонентов безопасности и формировании моделей информационной безопасности. В данном направлении ведутся научные исследования, совершенствуются и разрабатываются планы защиты информации, которые могут обеспечить защиту каждого компонента от возможного негативного воздействия, способного вывести его из строя. Учитываются общие критерии безопасности информационных технологий и такие нарушения состояния их защищенности, как аварийные ситуации вследствие стихийных бедствий и отключения питания, отказы и сбои в работе аппаратуры, ошибки в программном обеспечении и работе сотрудников, помехи в линиях связи и возможные преднамеренные действия нарушителей.

Следовательно, при формировании модели информационной безопасности, требуется предусмотреть все механизмы для создания необходимого и достаточного уровня информационной безопасности, обеспечить противостояние угрозам и предусмотреть проведение эффективных мероприятий по ликвидации неблагоприятных последствий инцидентов информационной безопасности. Для сохранения достаточного уровня информационной безопасности рекомендуется применять построенные модели информационной безопасности в течение длительного времени.

Различные аспекты обеспечения информационной безопасности рассматривались ранее в работах отечественных и иностранных ученых. К

наиболее разработанным в научном плане можно отнести области защиты информационных процессов и технологий, организации информационно-аналитической деятельности. Однако, несмотря на значительное количество исследований, которые уже проведены, проблематика совершенствования обеспечения информационной безопасности в субъектах Российской Федерации, на основе постоянного развития информационных технологий и возрастания масштабов информационных угроз остается недостаточно разработанным научным направлением.

В научной литературе проблемы обеспечения информационной безопасности рассматриваются с точки зрения различных подходов. Социально-психологический подход рассматривает информационную безопасность с точки зрения оказания информационного воздействия на человека. Изучением данной проблемы занимались Л.В. Астахова, Е.П. Белинская, Ю.Д. Бабаева, А.Е. Войскунский, Т.В. Владимирова, А.Е. Жичкина, О.М. Манжуева. Социокультурный подход к информационной безопасности, рассматриваемый в трудах Э.К. Наберушкиной, Е.А. Бердник, Л.В. Скворцова, предполагает необходимость выявления возможностей противостояния разрушению социальных ценностей. Особое место в изучении понятия информационной безопасности занимает анализ нормативно-правового характера такими авторами, как Е.К. Волчинская, Г.В. Загузов, П.У. Кузнецов, Н.В. Лопатин, А.А. Стрельцов. Представители технологического подхода рассматривают информационную безопасность как комплекс средств, методов и мероприятий, которые обеспечивают защиту информации от различного рода воздействий, ведущих к несанкционированному доступу к ней, разглашению и утечке. Изучению технологического подхода посвятили свои труды А.Н. Асаул, М.В. Арсеньев, В.А. Галатенко, В.Ю. Гайкович, Д.Е. Ершов, Е.А. Ерофеев, В.К. Левин, Д.А. Ловцов, Ю.С. Уфимцев, В.П. Шерстюк, В.Н. Ясенев.

Особый вклад в исследование информационной безопасности в различных сферах общества, культуры, науки и техники, внесли такие ученые

и исследователи, как А.Б. Агапов, А.С. Алексеев, И.Л. Бачило, А.В. Возженников, Ю.М. Горский, Г.Н. Горшенков, И.С. Даниленко, Н.В. Данилов, С.А. Дятлов, Г.Г. Феоктистов, А.М. Яновский и другие. В работах этих ученых сформулированы концептуальные положения о сущности и содержании категорий информационной безопасности, исследованы их взаимосвязи, обоснованы приемы и способы исследования информационной безопасности и различных составляющих системного подхода.

Технические аспекты обеспечения информационной безопасности рассматривали в своих трудах М.В. Буйневич, М.А. Вус, В.А. Васенин, М.П. Зегжда, О.В. Казарин, А.А. Малюк, А.В. Старовойтов, Н.В. Скабцов, А.Ю. Щеглов, Р.М. Юсупов.

Организационно-правовые аспекты обеспечения информационной безопасности рассматривали И.Л. Бачило, Н.А. Белобородова, А.Н. Велигура, М.В. Елин, Н.А. Комлева, И.М. Левкин, А.В. Манойло, Н.Г. Милославская, С.А. Нестеров, Л.Л. Попов, Е.А. Проценко, М.Ю. Сенаторов, А.А. Стрельцов.

В правовом аспекте работы данных авторов сосредоточены на развитии законодательной базы и совершенствовании правоприменительной практики в области информации, информационных технологий и защиты информации.

Таким образом, актуальность и степень разработанности выбранной научной проблемы подтверждают целесообразность проведения исследования.

В настоящее время, несмотря на большое количество работ по проблематике, следует отметить, что ее теоретическая изученность явно недостаточна, практические методики по формированию оптимального механизма информационной безопасности в образовательных организациях не соответствуют условиям реального времени. В работах отечественных и западных авторов превалирует односторонний подход в исследовании проблем информационной безопасности, рассматривается какая-то одна

сторона из всего механизма информационной безопасности в организациях вообще.

Исходя из выше сказанного, сформулируем проблему исследования: разработка рекомендаций по совершенствованию модели и методов обеспечения информационной безопасности на основе физической защиты в образовательных организациях СПО.

Таким образом, потребность в создании оптимальной системы информационной безопасности, а также проработка вопроса использования более совершенных методов и моделей обеспечения информационной безопасности образовательных организаций определили выбор темы диссертационного исследования: «Совершенствование модели и методов обеспечения информационной безопасности в образовательной организации на основе физической защиты».

Исходя из поставленной проблемы, можно определить объект, предмет и цель исследования.

Цель исследования заключается в анализе существующей системы обеспечения информационной безопасности образовательной организации и совершенствовании модели и методов обеспечения информационной безопасности образовательной организации.

Объектом исследования является система обеспечения информационной безопасности образовательной организации на основе физической защиты.

Предмет исследования: совершенствование системы обеспечения информационной безопасности в образовательной организации (на примере ГБПОУ «Южно-Уральский государственный колледж»).

Гипотеза исследования состоит в разработке методического аппарата, позволяющего осуществлять рациональный выбор защитных мер для образовательной организации за счет совершенствования модели и методов обеспечения информационной безопасности на основе физической защиты.

Выдвинутая гипотеза и цель приводят к постановке ряда задач:

1. Раскрыть сущность и содержание физической защиты информации.
2. Изучить модели обеспечения информационной безопасности и виды угроз в образовательной организации.
3. Изучить объект защиты – ГБПОУ «Южно-Уральский государственный колледж», его структуру, информационные ресурсы и информационные потоки колледжа; проанализировать систему обеспечения информационной безопасности в ГБПОУ «ЮУГК»; выявить уязвимости в системе защиты информации.
4. Разработать рекомендации по совершенствованию модели и методов обеспечения информационной безопасности колледжа ГБПОУ «Южно-Уральский государственный колледж».
5. Привести экономическое обоснование эффективности предложенных мер совершенствования системы обеспечения информационной безопасности колледжа ГБПОУ «Южно-Уральский государственный колледж».

Методологическую основу исследования составили законодательные и нормативно-правовые документы РФ, разработки в области обеспечения информационной безопасности, методы и способы построения процессов управления информационной безопасностью в целях повышения информационной безопасности в организациях, системный анализ.

Теоретическую и информационную базу исследования составляют: основные положения по информационной безопасности, системный подход к исследуемому объекту и предмету, в качестве информационных источников использованы аналитические и статистические материалы по информационной безопасности, материалы научных конференций, средств массовой информации, отражающие аспекты информационной безопасности.

Научная новизна исследования состоит в комплексном решении актуальной задачи, состоящей в совершенствовании системы обеспечения информационной безопасности образовательной организации, позволяющей повысить уровень информационной безопасности колледжа за счет внедрения

рекомендаций по совершенствованию модели и методов обеспечения информационной безопасности колледжа на основе физической защиты.

Теоретическая значимость работы обусловлена возможностью использовать представленные в данном исследовании положения и полученные по его итогам выводы в целях дальнейшей оптимизации деятельности образовательных организаций в сфере обеспечения информационной безопасности и при разработке соответствующих систем обеспечения информационной безопасности.

Практическая значимость работы заключается в разработке рекомендаций по совершенствованию модели и методов обеспечения информационной безопасности колледжа, за счет модернизации противопожарной защиты серверных помещений, системы контроля и управления доступом в ГБПОУ «Южно-Уральский государственный колледж». Проведенное исследование и полученные результаты могут быть использованы для создания, внедрения и управления системой защиты информации в других образовательных организациях.

Апробация исследования: результаты исследования были опубликованы на:

- 1) Международной научно-практической конференции «Актуальные проблемы современной когнитивной науки», 09 февраля 2022 год, г. Пенза.
- 2) Международной научно-практической конференции «Проблемы и перспективы осуществления междисциплинарных исследований»: 30 декабря 2022 год, г. Стерлитамак.

Экспериментальная база исследования: Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный колледж».

Структура диссертационного исследования. Магистерская диссертация состоит из введения, двух глав, заключения, списка использованных источников, состоящего из 45 наименований. Работа содержит 19 рисунков, 5 таблиц. Общий объем работы составляет 84 страниц.

ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИССЛЕДОВАНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ НА ОСНОВЕ ФИЗИЧЕСКОЙ ЗАЩИТЫ

1.1. Сущность и содержание физической защиты информации в образовательной организации

Система безопасности потенциальных и реальных угроз непостоянна, поскольку те могут появляться, исчезать, уменьшаться или нарастать. Все участники отношений в процессе обеспечения безопасности информации, будь то человек, государство, предприятие или регион, представляют собой многоцелевые сложные системы, для которых трудно определить уровень необходимой безопасности.

В понятие информационной безопасности образовательной организации входит система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы. Вторым аспектом понятия станет защита образовательного процесса от любых сведений, носящих характер запрещенной законом пропаганды, или любых видов рекламы.

В составе массивов охраняемой законом информации, находящейся в распоряжении образовательной организации, можно выделить три группы:

- персональные сведения, касающиеся обучающихся и преподавателей, оцифрованные архивы;
- ноу-хау образовательного процесса, носящие характер интеллектуальной собственности и защищенные законом;
- структурированная учебная информация, обеспечивающая образовательный процесс (библиотеки, базы данных, обучающие программы).

Все эти сведения не только могут стать объектом хищения. Намеренное проникновение в них может нарушить сохранность оцифрованных книг,

уничтожить хранилища знаний, внести изменения в код программ, используемых для обучения.

Обязанностями лиц, ответственных за защиту информации, должно стать сохранение данных в целостности и неприкосновенности и обеспечение их:

- доступности в любое время для любого авторизованного пользователя;
- защиты от любой утраты или внесения несанкционированных изменений;
- конфиденциальности, недоступности для третьих лиц.

На основании этого система обеспечения информационной безопасности организации рассматривается как целый комплекс принятых управленческих решений, направленных на выявление и предотвращение внешних и внутренних угроз. Эффективность принятых мер основывается на определении таких факторов, как степень и характер угрозы, аналитическая оценка кризисной ситуации и рассмотрение других неблагоприятных моментов, представляющих опасность для развития организации и достижения поставленных целей. Обеспечение информационной безопасности организации базируется на принятии таких мер, как:

1. Анализ потенциальных и реальных ситуаций, представляющих угрозу безопасности информации образовательной организации.
2. Оценка характера угроз безопасности информации.
3. Принятие и комплексное распределение мер для определения угрозы.
4. Реализация принятых мер по предотвращению угрозы.

Основная цель обеспечения комплексной системы безопасности информации для защиты образовательной организации, это:

- создать благоприятные условия для нормального функционирования в условиях нестабильной среды;
- обеспечить защиту собственной безопасности;

- возможность на законную защиту собственных интересов от противоправных действий конкурентов;
- обеспечить сотруднику и студенту сохранностью жизни и здоровья;
- предотвращать возможность материального и финансового хищения, искажения, разглашения и утечки конфиденциальной информации, растраты, производственные нарушения, уничтожение имущества и обеспечить нормальную производственную деятельность.

Организация обеспечения безопасности образовательной организации основывается на тех же принципах защиты и предполагает постоянную модернизацию защитных функций, поскольку эта сфера постоянно развивается и совершенствуется. Казалось бы, еще недавно созданные новые защитные системы со временем становятся уязвимыми и недейственными, вероятность их взлома с каждым годом возрастает.

Информационные технологии являются одним из ключевых векторов развития практически всех сфер жизнедеятельности современного человека. Именно посредством эффективной работы алгоритмов защиты информационных потоков и стабильной работы физических средств защиты информации достигается эффективная и бесперебойная деятельность образовательной организации. На сегодняшний день активно разрабатываются и модернизируются исключительно программные и системные методы защиты информации в то время, как внедрением и совершенствованием физических средств защиты информации современные предприятия практически не занимаются.

Физические средства защиты информации играют немаловажную роль при работе с информационными ресурсами образовательной организации. Именно поэтому образовательные организации обязаны оснащаться не только инновационным программным обеспечением, но и разрабатывать оптимальные и эффективные физические методы со средствами защиты информации. Исходя из этого формируется проблема, связанная с недооценкой физических методов защиты информации [1].

Актуальность проблемы защиты информации и информационных технологий в современном мире определяется основными факторами, указанными на рисунке 1.

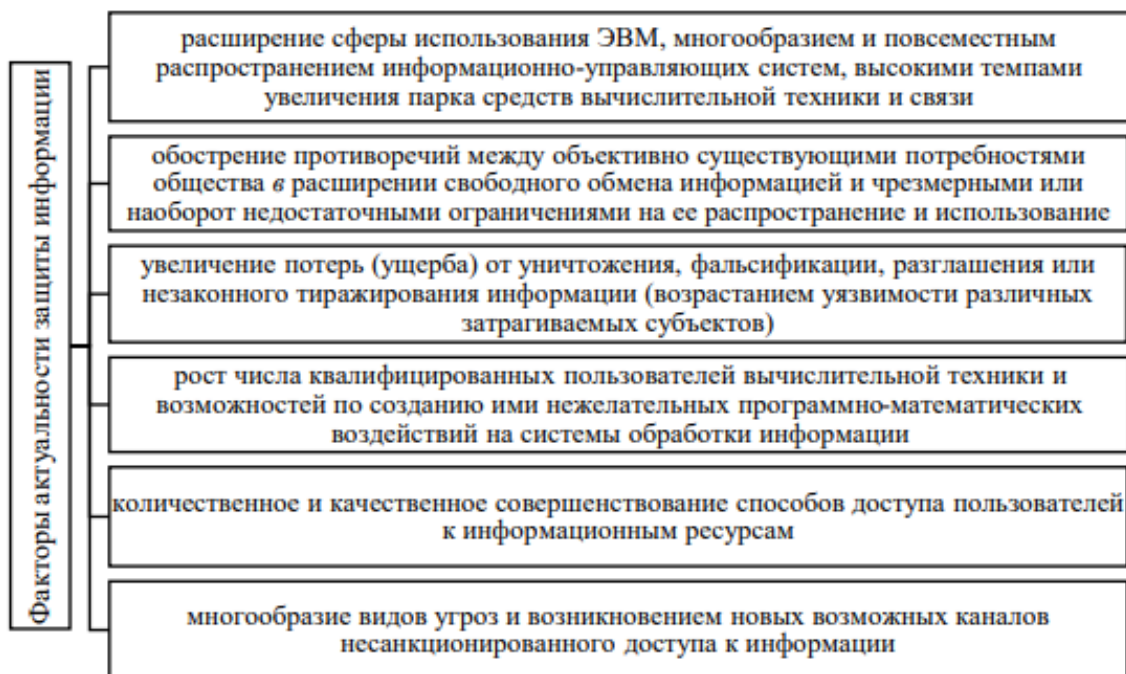


Рисунок 1 – Основные факторы, определяющие актуальность защиты информации

Именно информационные ресурсы имеют высокую степень потенциальной угрозы перед нападением и утечкой конфиденциальной информации. В связи с этим существует необходимость в ее защите и охране, будь то информация, хранящаяся в электронном виде или физическом. Методы защиты информации делятся на 4 группы: физические, аппаратные, программные, организационные (рис. 2).



Рисунок 2 – Методы защиты информации

Физическая защита информации является таким методом защиты информационных ресурсов, при котором применяются организационные мероприятия и совокупности средств, способные препятствовать несанкционированному проникновению или доступу неуполномоченных физических лиц к защищаемому объекту [4].

Основные организационные мероприятия, направленные на поддержание физической защиты информации, предусматривают установление режимных, пространственных, временных, территориальных и иных ограничений относительно условий использования и распорядка работы объекта защиты.

К таким объектам обычно относятся: здания (сооружения), охраняемая территория, отдельно-выделенные помещения, сама информация или информационные ресурсы информатизированного объекта.

Параллельное взаимодействие программных и физических методов защиты информации является одной из актуальных задач в вопросе информационной безопасности на сегодняшний день. Интеграция многоуровневой системы защиты информации, включающей в себя данные методы, позволит более эффективно справляться с потенциальными угрозами, а также вычислять и производить операции, связанные с защитой

информационных ресурсов, более быстро относительно существующих на сегодняшний день программных комплексов.

Физическая защита является первым рубежом для злоумышленника, поэтому она необходима для комплексного обеспечения безопасности информационных систем [5].

На рисунке 3 указаны основные виды и предназначения физических методов защиты информационных ресурсов.



Рисунок 3 – Физические средства защиты информации

Задачи, возлагаемые на физические средства защиты: обеспечение безопасности строений, внутренних помещений и территорий; защита оборудования и документов от несанкционированного доступа к ним; обеспечение защиты от перехвата информационного потока методами наблюдения и подслушивания; защита от пожаров и иных угроз, способствующих уничтожению информации.

Подводя итоги, необходимо отметить, что современная информационная безопасность образовательной организации базируется на концепции комплексной защиты информации, а также физических методах, подразумевающие одновременное использование многих взаимосвязанных программно-аппаратных решений и мер социального характера, которые поддерживают и дополняют друг друга.

1.2 Модели обеспечения информационной безопасности в образовательной организации

Словосочетание «информационная безопасность» рассматривают в разных контекстах, при этом оно может иметь различное толкование, а также использоваться в широком смысле. В Доктрине информационной безопасности РФ, утвержденной Указом Президента РФ от 5 декабря 2016 года №646 под информационной безопасностью Российской Федерации понимают «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [7].

Рассматривая это понятие в более узком смысле, мы предполагаем, что «информационная безопасность в современности основывается на концепции совокупной защиты данных, которая подразумевает применение определенного количества объединённых программно-аппаратных решений и мероприятий социального характера, поддерживающих и взаимодополняющих» [1, 302 с.].

В направлении обеспечения безопасности информации особое внимание уделяют:

- соблюдению конфиденциальности, обеспечивая полный контроль доступа к информации, которую необходимо защитить, и одновременно сделать ее доступной для авторизированных пользователей, с учетом регулярного обновления паролей доступа;

- сохранению целостности информации, исключив несанкционированное изменение части информации третьими лицами, не имеющими к ней доступа;

– обеспечению доступности информации, то есть рассматриваются лица, которые имеют полный доступ к информации без каких-либо ограничений. В этом случае ответственность за сохранность возложена на допущенных к работе с данными.

Исторически сформировался подход к классификации информации с учетом уровня требований к сведениям с ограниченным доступом, обеспечения конфиденциальности информации. Этот факт можно объяснить тем, что ущерб, причиненный в результате разглашения открытой информации, не будет настолько существенным. Поэтому важно также учитывать целостность, подлинность и доступность информации, которая не является конфиденциальной.

Также «для гарантирования информационной безопасности необходимо применение ряда мероприятий: выработать политику обеспечения защиты и составить соответствующую техдокументацию; внедрить технические средства обеспечения информационной безопасности» [3, С. 139-140].

В сфере ИБ для прогнозирования, как правило, используются модели угроз и нарушителей ИБ. При разработке моделей используются имеющийся у организации опыт и знания, поэтому чем выше знания, тем точнее прогноз.

Рассмотрим подробнее процесс моделирования информационной безопасности.

Вначале эксперт знакомится с объектом защиты, тем самым создавая (не всегда формально) модель объекта защиты. Далее он рассматривает возможные угрозы, применимые к данному объекту защиты, опираясь на специфику объекта защиты (в том числе уязвимости объекта защиты), выраженную в модели объекта защиты. В итоге эксперт получает модель угроз ИБ. Угрозы можно брать из каталогов угроз ИБ, но в то же время могут существовать угрозы, характерные только для определенного объекта защиты. Далее на основе модели угроз эксперт формирует модель нарушителя. На основе перечисленных трех моделей создается модель противодействия, некая стратегия противодействия угрозам ИБ (согласно модели угроз ИБ),

реализуемым нарушителями ИБ (согласно модели нарушителя ИБ) в условиях данного объекта (согласно модели объекта защиты). Данная последовательность процедур моделирования изображена на рис. 4.



Рисунок 4 – Последовательность создания моделей ИБ

Модели могут быть как формализованными, так и неформализованными. Как правило, при создании СОИБ организации происходит высокоуровневое моделирование, создаются неформализованные модели, которые образуют следующий возможный комплекс документов:

1. Концепция обеспечения ИБ организации.
2. Политика ИБ организации.
3. Модель угроз.
4. Модель нарушителей.

Для обеспечения информационной безопасности создают модели безопасности, которые являются формальным (математическим, алгоритмическим, схематическим и т.п) выражением политики безопасности.

Учитывая непрерывность процесса данные модели должны постоянно совершенствоваться и обеспечивать на достаточном уровне устранение возможных слабостей, некорректностей и неисправностей.

Построение системы информационной безопасности предполагает в обязательном порядке рассмотрение следующих объективных факторов:

- угроз информационной безопасности, вероятность их возникновения и реализации;
- уязвимостей системы информационной безопасности;
- риск и возможный ущерб в случае успешной реализации угрозы информационной безопасности, который найдет отражение в вероятных финансовых потерях – прямых или косвенных.

При создании модели информационной безопасности рассматривают такие защищаемые объекты, как объекты информатизации, ресурсы информационной системы, информационные системы, информационные технологии, программные средства, сети связи, автоматизированные системы. «Под объектом защиты понимается информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации» [6].

К объектам защиты также можно отнести охраняемую территорию, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

Модели безопасности посредством системотехнического подхода, дают возможность рассмотреть решение следующих задач:

- выбор, обоснование базовых принципов архитектуры автоматизированных систем;
- подтверждение свойства защищенности системы;
- составления формальной спецификации политики безопасности разрабатываемых систем.

Последним важным вопросом при построении моделей или систем является их жизненный цикл, который включает следующие этапы:

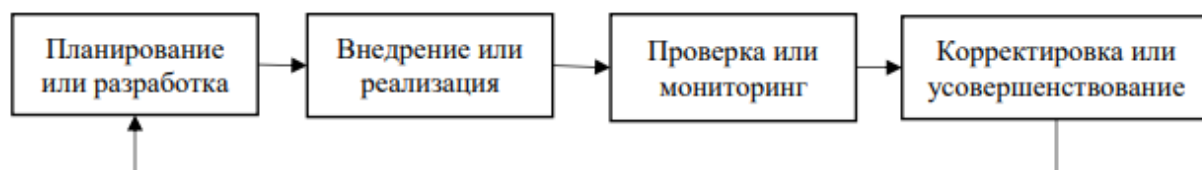


Рисунок 5 – Жизненный цикл системы информационной безопасности

К основным моделям информационной безопасности относятся концептуальная, математическая и функциональная модели.

Концептуальная модель информационной безопасности.

Концептуальная модель представляет собой множество понятий и связей между ними, которые определяют смысловую структуру исследуемой предметной области. Данная модель должна включать перечень взаимосвязанных понятий, включая их свойства, характеристики, классификацию, учитывая также типы, ситуации, признаки в данной области и условия протекания процесса. В этом случае правомерно рассмотреть возможные угрозы безопасности, источники возникновения рассматриваемых угроз, способы реализации, цели и другие условия, которые способны нарушить безопасность. Перечисленные компоненты определяют концептуальную модель информационной безопасности, которая также включает объекты угроз, способы доступа, направления защиты, средства защиты, а также источники информации.

Для того, чтобы грамотно выстроить концептуальную модель, необходимо изначально определить объект защиты, киберугрозы, способы защиты информации. Также необходимо предварительно установить:

- источники данных;
- направления, методики, средства защиты;
- технологии получения доступа к системе, защита которой обеспечивается;
- источники и цели угроз;
- приоритетные источники данных.

Таким образом, создание концептуальной модели информационной безопасности направлено на предоставление ответов на общие вопросы, схематически отражая при этом общую структуру модели, на основе которой будут строиться другие модели и концепции информационной безопасности. При этом, реализация концептуальной модели информационной безопасности рассматривает создание нескольких уровней. В основном – это сервисный и

организационно-управленческий уровень. Полная концептуальная модель информационной безопасности, которая является общей для всех информационных систем, представлена на рисунке 6.

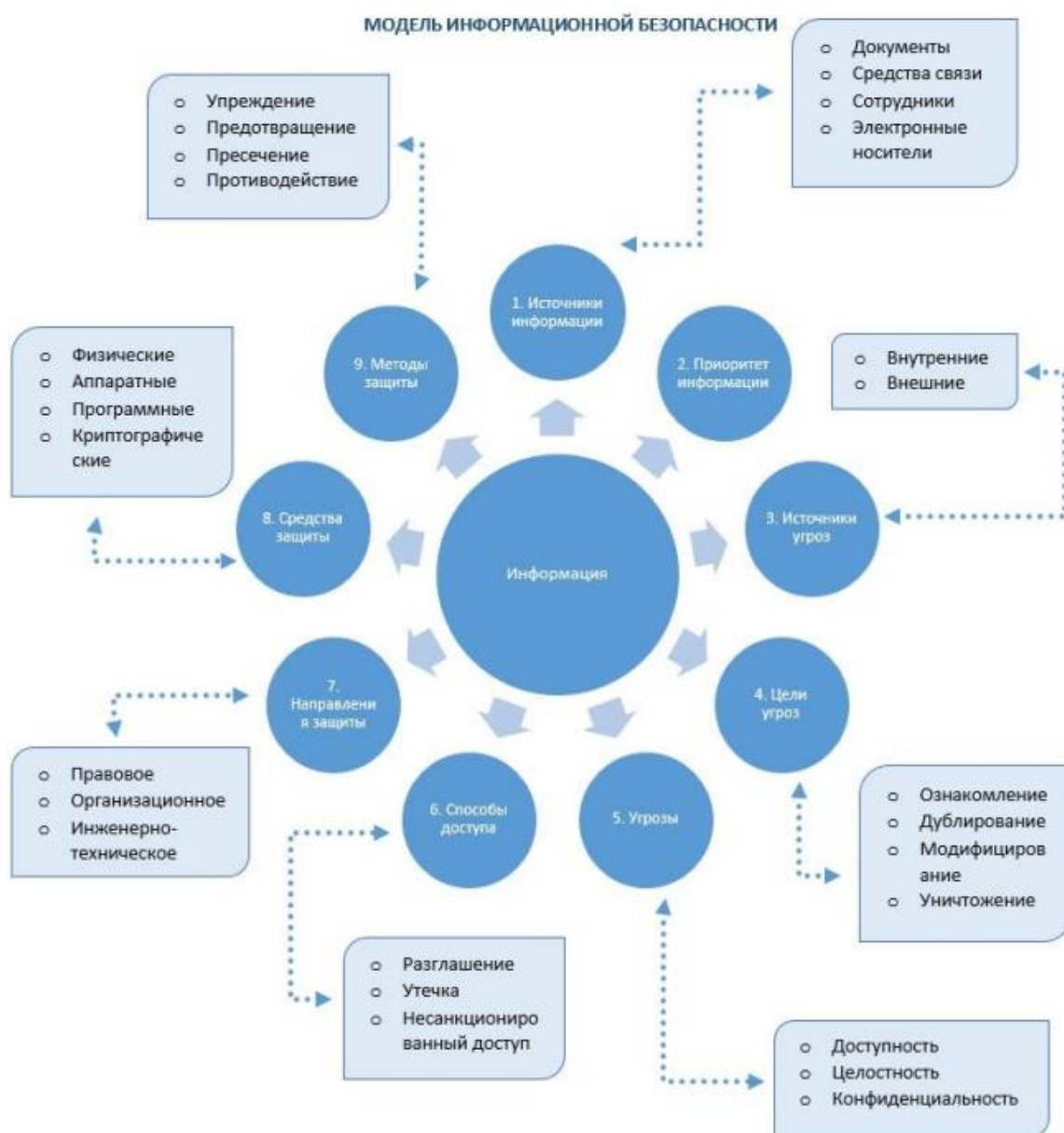


Рисунок 6 – Концептуальная модель ИБ

В процессе реализации концептуальной модели информационной безопасности должно быть создано несколько уровней. Для большинства организаций хватает двух уровней – сервисного и организационно-управленческого. В рамках реализации организационно-управленческого уровня выполняются следующие работы:

- стратегическое планирование;

- создание и реализация политики в сфере кибербезопасности организации;
- оценка и управление рисками;
- координирование работы и функций сотрудников компании в сфере кибербезопасности;
- контроль выполнения этих функций.

В рамках сервисного уровня предполагается обеспечение эффективности и экономически целесообразной защиты информационных сервисов. Специалисты заранее должны определить по результатам проверенного исследования, анализа и оценки, какие средства и защитные методики должны применяться в конкретном случае, как будет выполняться повседневное администрирование и мониторинг, как будет выполняться первичное обучение сотрудников и т. д. Для этого уровня надо получить ответы на следующие вопросы:

- типы данных, обрабатываемые сервисом;
- вероятные последствия компрометации внутренней сети, доступности и целостности информации;
- максимально уязвимые сегменты используемой и защищаемой информационной системы;
- уровень квалификации, благонадежности, дисциплинированности сотрудников компании на каждом участке, находящихся под защитой;
- корпоративные регламенты, юридические положения, которым должен соответствовать сервис.

Концептуальная модель безопасности информации определяет процесс разработки методических рекомендаций по ее внедрению, которые должны использоваться с учетом рассмотренных принципов и являться основой защиты информации.

После разработки концептуальной модели переходят к выстраиванию математической и функциональной модели информационной безопасности. Данные модели имеют неразрывные связи.

«Математическая модель в информационной безопасности — это описание сценариев в виде последовательности действий нарушителей и соответствующих ответных мер. Такие модели описывают процессы взаимодействия нарушителя с системой защиты и возможные результаты действий» [5, 93 с.].

В процессе создания математической модели информационной безопасности проводится экспертная оценка вероятности киберугроз с учетом их значимости и степени финансовых трат на восстановление нормального функционирования системы и сохранения данных после кибератак и утечек информации. Также производят расчет общего риска отказа системы.

Таким образом, математическая модель информационной безопасности позволяет [2, 9]:

- оценить возможность реализации различных угроз на информационные системы и проведения атак на них;
- дать количественную оценку качества функционирования системы защиты;
- оценить экономическую эффективность применения средств защиты информации;
- определить структуру построения системы защиты информационной системы.

Если в итоге общие денежные траты на устранение рисков меньше или равны максимальному уровню затрат, которые выделяются на снижение или устранение суммарных рисков, систему информационной безопасности считают финансово оправданной.

В дальнейшем на базе сформированной математической модели создается функциональная модель, которая в свою очередь требует особого внимания, учитывая рассмотрение конкретных мер по защите. Функциональная модель определяет функции служб защиты информации, которые должны быть реализованы. При этом, требуется предоставить

упорядоченный набор функций, с учетом входных данных (материальных объектов), ограничений, исполнителей, ожидаемого результата.

Отдельно хотелось бы уделить внимание преступлениям в сфере информационной безопасности, которые могут осуществляться через человека. К ним относятся хищение носителей информации, ознакомление с информацией без разрешения владельца. С помощью программ можно осуществлять преступления путем перехвата паролей, копирования информации с носителей, дешифровки. Хищение информации возможно с помощью подключения специальных аппаратных средств доступа к информации, а также посредством перехвата побочных электромагнитных излучений от аппаратуры. Кроме того, информационная безопасность персональных данных может подвергаться атаке со стороны компьютерных сетей и распространения известных видов троянских программ. Также нельзя забывать, что средства нападения, способные обмануть защиту информации, постоянно развиваются и совершенствуются.

Следовательно, модели информационной безопасности обеспечивают формализацию политик безопасности и определяют единый подход с учетом ключевых особенностей объектов и ожидаемых результатов в процессе применения той или иной модели. Предоставленный набор правил дает возможность проецирования абстрактных положений в политику безопасности, которая будет применяться при проектировании программного и аппаратного обеспечения. При этом, в основе системы защиты информации должна быть концептуальная модель информационной безопасности.

Прогресс в области развития средств вычислительной техники, программного обеспечения и сетевых технологий стал решающим условием создания современных средств обеспечения безопасности, что требует во многом предусмотреть научную парадигму информационной безопасности. На сегодняшний день теория информационной безопасности – одна из самых развивающихся естественных наук.

Заинтересованность российских компаний, учреждений и предприятий в использовании моделей информационной безопасности, несомненно, есть. В дальнейшем популярность таких моделей будет неуклонно расти, учитывая экономическую целесообразность.

1.3 Виды угроз информационной безопасности в образовательной организации и их характеристика

Под угрозами безопасности информационной системы понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации или несанкционированными, непреднамеренными воздействиями на нее [10].

Угроза – это потенциальные или реальные действия, приводящие к моральному или материальному ущербу.

Угроза безопасности информации – потенциальная возможность нарушения основных качественных характеристик (свойств) информации при её обработке техническими средствами: конфиденциальности, целостности, доступности [12].

Под угрозами конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями.

Таковыми действиями являются:

- ознакомление с конфиденциальной информацией различными путями и способами без нарушения её целостности;
- модификация информации в криминальных целях как частичное или значительное изменение состава и содержания сведений;
- разрушение (уничтожение) информации как акт вандализма в целях прямого нанесения материального ущерба.

В конечном итоге противоправные действия с информацией приводят к нарушению её конфиденциальности, полноты, достоверности и доступности,

что в свою очередь приводит к нарушению как режима управления, так и его качества в условиях ложной или неполной информации.

Каждая угроза влечёт за собой определённый ущерб – моральный или материальный, а защита и противодействие угрозе призвано снизить его величину, в идеале – полностью, реально – значительно или хотя бы частично. Но и это удаётся далеко не всегда [12].

С учётом этого угрозы могут быть классифицированы по следующим кластерам:

1) по величине принесённого ущерба:

- предельный, после которого образовательная организация может стать банкротом;

- значительный, но не приводящий к банкротству;

- незначительный, который образовательная организация может компенсировать и др.;

2) по вероятности возникновения:

- весьма вероятная угроза;

- вероятная угроза;

- маловероятная угроза;

3) по причинам появления:

- стихийные бедствия;

- преднамеренные действия;

4) по характеру нанесённого ущерба:

- материальный;

- моральный;

5) по характеру воздействия:

- активные;

- пассивные;

6) по отношению к объекту:

- внутренние;

- внешние.

Источниками внешних угроз являются:

- недобросовестные конкуренты;
- преступные группировки и формирования;
- отдельные лица и организации административно-управленческого аппарата.

Источниками внутренних угроз могут быть:

- администрация организации;
- персонал;
- технические средства обеспечения производственной и трудовой деятельности [12].

Соотношение внешних и внутренних угроз на усреднённом уровне можно охарактеризовать так:

82% угроз совершается собственными сотрудниками образовательной организации либо при их прямом или опосредованном участии;

17% угроз совершается извне – внешние угрозы;

1% угроз совершается случайными лицами [12].

Особенностью угроз становится не только возможность хищения сведений или повреждение массивов какими-либо сознательно действующими хакерскими группировками, но и сама деятельность студентов, намеренно, по злему умыслу или ошибочно способных повредить компьютерное оборудование или внести вирус. Выделяются четыре группы объектов, которые могут подвергнуться намеренному или ненамеренному воздействию:

– компьютерная техника и другие аппаратные средства, которые могут быть повреждены в результате механического воздействия, вирусов, по иным причинам;

– программы, используемые для обеспечения работоспособности системы или в образовательном процессе, которые могут пострадать от вирусов или хакерских атак;

- данные, хранимые как на жестких дисках, так и на отдельных носителях;

- сам персонал, отвечающий за работоспособность IT-систем;

- обучающиеся, подверженные внешнему агрессивному информационному влиянию и способные создать в колледже криминальную ситуацию. В последнее время перечень таких ситуаций существенно расширился, что говорит о возможной целенаправленной психологической атаке на сознание детей и подростков.

Угрозы, направленные на повреждение любого из компонентов системы, могут носить как случайный, так и осознанный преднамеренный характер. Среди угроз, не зависящих от намерения персонала, обучающихся или третьих лиц, можно назвать:

- любые аварийные ситуации, например, отключение электроэнергии или затопление;

- ошибки персонала;

- сбои в работе программного обеспечения;

- выход техники из строя;

- проблемы в работе систем связи [21].

Все эти угрозы информационной безопасности носят временный характер, предсказуемы и легко устраняются действиями сотрудников и специальных служб.

Намеренные угрозы информационной безопасности носят более опасный характер и в большинстве случаев не могут быть предвидены. Их виновниками могут оказаться обучающиеся, служащие, конкуренты, третьи лица с намерением на совершение кибер-преступления. Для подрыва информационной безопасности такое лицо должно иметь высокую квалификацию в отношении принципов работы компьютерных систем и программ. Наибольшей опасности подвергаются компьютерные сети, компоненты которых расположены отдельно друг от друга в пространстве. Нарушение связи между компонентами системы может привести к полному

подрыву ее работоспособности. Важной проблемой может стать нарушение авторских прав, намеренное хищение чужих разработок. Компьютерные сети редко подвергаются внешним атакам с целью воздействия на сознание обучающихся, но и это не исключено. И самой серьезной опасностью станет использование оборудования в колледже для вовлечения студента в криминал и терроризм.

С точки зрения проникновения в периметр информационной безопасности и для совершения хищения информации или создания нарушения в работе систем необходим несанкционированный доступ.

Способы несанкционированного доступа.

Можно выделить несколько видов несанкционированного доступа:

1. Человеческий. Информация может быть похищена путем копирования на временные носители, переправлена по электронной почте. Кроме того, при наличии доступа к серверу изменения в базы данных могут быть внесены вручную.

2. Программный. Для хищений сведений используются специальные программы, которые обеспечивают копирование паролей, копирование и перехват информации, перенаправление трафика, дешифровку, внесение изменений в работу иных программ.

3. Аппаратный. Он связан или с использованием специальных технических средств, или с перехватом электромагнитного излучения по различным каналам, включая телефонные.

Существует 5 принципов системы обеспечения информационной безопасности организации.

Принцип комплексности. При создании защитных систем необходимо предполагать вероятность возникновения всех возможных угроз для каждой организации, включая каналы закрытого доступа и используемые для них средства защиты. Применение средств защиты должно совпадать с вероятными видами угроз и функционировать как комплексная система защиты, технически дополняя друг друга. Комплексные методы и средства

обеспечения информационной безопасности организации являются сложной системой взаимосвязанных между собой процессов.

Принцип эшелонирования представляет собой порядок обеспечения информационной безопасности организации, при котором все рубежи защитной системы будут состоять из последовательно расположенных зон безопасности, самая важная из которых будет находиться внутри всей системы.

Принцип надежности (равнопрочности). Стандарт организации обеспечения информационной безопасности должен касаться всех зон безопасности. Все они должны быть равнопрочными, то есть иметь одинаковую степень надежной защиты с вероятностью реальной угрозы.

Принцип разумной достаточности предполагает разумное применение защитных средств с приемлемым уровнем безопасности без фанатизма создания абсолютной защиты. Обеспечение организации высокоэффективной защитной системой предполагает большие материальные затраты, поэтому к выбору систем безопасности нужно подходить рационально. Стоимость защитной системы не должна превышать размер возможного ущерба и затраты на ее функционирование и обслуживание.

Принцип непрерывности. Работа всех систем безопасности должна быть круглосуточной и непрерывной [22].

Как правило, защита от угроз, в основном регламентируется инструкциями, разработанными и утвержденными в образовательной организации с учетом особенностей эксплуатации информационных систем организации и действующей нормативной базой образовательной организации.

Выводы по главе 1

В первой главе магистерской диссертации раскрыты теоретические аспекты исследования обеспечения информационной безопасности в образовательной организации на основе физической защиты.

1. Физические средства защиты информации играют немаловажную роль при работе с информационными ресурсами образовательной организации. Именно поэтому образовательные организации обязаны оснащаться не только инновационным программным обеспечением, но и разрабатывать оптимальные и эффективные физические методы со средствами защиты информации.

Физическая защита информации является таким методом защиты информационных ресурсов, при котором применяются организационные мероприятия и совокупности средств, способные препятствовать несанкционированному проникновению или доступу неуполномоченных физических лиц к защищаемому объекту. Основные организационные мероприятия, направленные на поддержание физической защиты информации, предусматривают установление режимных, пространственных, временных, территориальных и иных ограничений относительно условий использования и распорядка работы объекта защиты.

2. Во втором параграфе первой главы описаны модели обеспечения информационной безопасности, а также процесс моделирования информационной безопасности.

В сфере ИБ для прогнозирования, как правило, используются модели угроз и нарушителей ИБ. При разработке моделей используются имеющийся у организации опыт и знания, поэтому чем выше знания, тем точнее прогноз.

Таким образом, модели информационной безопасности обеспечивают формализацию политик безопасности и определяют единый подход с учетом ключевых особенностей объектов и ожидаемых результатов в процессе применения той или иной модели. Предоставленный набор правил дает

возможность проецирования абстрактных положений в политику безопасности, которая будет применяться при проектировании программного и аппаратного обеспечения. При этом, в основе системы защиты информации должна быть концептуальная модель информационной безопасности.

3. Рассмотрены виды угроз информационной безопасности в образовательной организации.

Под угрозами безопасности информационной системы понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации или несанкционированными, непреднамеренными воздействиями на нее. Как правило, защита от угроз, в основном регламентируется инструкциями, разработанными и утвержденными в образовательной организации с учетом особенностей эксплуатации информационных систем организации и действующей нормативной базой образовательной организации.

Подводя итоги, необходимо отметить, что современная информационная безопасность образовательной организации базируется на концепции комплексной защиты информации, а также физических методах, подразумевающие одновременное использование многих взаимосвязанных программно-аппаратных решений и мер социального характера, которые поддерживают и дополняют друг друга.

ГЛАВА 2 РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО СОВЕРШЕНСТВОВАНИЮ МОДЕЛИ И МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ГБПОУ «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ КОЛЛЕДЖ»

2.1 Анализ системы обеспечения информационной безопасности ГБПОУ «Южно-Уральский государственный колледж»

Базой исследования является ГБПОУ «Южно-Уральский государственный колледж». Адрес базы исследования: Челябинская область, г. Челябинск, ул. Курчатова, дом 7. Руководителем образовательной организации является – Лапин Владимир Геннадьевич.

ГБПОУ «Южно-Уральский государственный колледж» является старейшим в Уральском регионе государственным средним профессиональным образовательным учреждением повышенного типа, которое готовит специалистов экономического и технического профиля. История колледжа начинается с экономического техникума, который был создан в 1967 году. За это время для предприятий и учреждений Южного Урала колледж подготовил тысячи бухгалтеров и товароведов. Многие из них стали ведущими специалистами в своих отраслях. Колледж сегодня специализируется на подготовке бухгалтеров, финансистов, коммерсантов, менеджеров, маркетологов, юристов, техников автоматизированных систем обработки информации и управления, дизайнеров.

На протяжении ряда лет Южно-Уральский государственный колледж (бывший Челябинский колледж информационно-промышленных технологий и художественных промыслов, бывший Челябинский экономический колледж) занимается разработкой и внедрением в учебном процессе интенсивных информационных образовательных технологий, основанных на широком использовании компьютерной и коммуникационной техники, электронных обучающих программ, проектной культуры. Это позволяет

колледжу активно решать проблемы доступности, эффективности и качества профессиональной подготовки современных специалистов для отраслей предприятий России. Педагоги колледжа имеют опыт практической работы по соответствующей специальности и глубокую теоретическую подготовку, необходимую для успешной реализации профессиональных образовательных программ. Среди них — кандидаты наук, заслуженные работники образования РФ, преподаватели высшей категории.

Выпускники колледжа имеют возможность продолжать обучение в вузе на базе полученной в колледже профессиональной подготовки, получить полноценное высшее образование в ускоренные сроки.

Образовательный комплекс информационных технологий и экономики находится по адресу г. Челябинск, ул. Курчатова, 7. Учредителем колледжа является Министерство образования и науки Челябинской области.

Организационная структура колледжа представлена на рисунке 7.

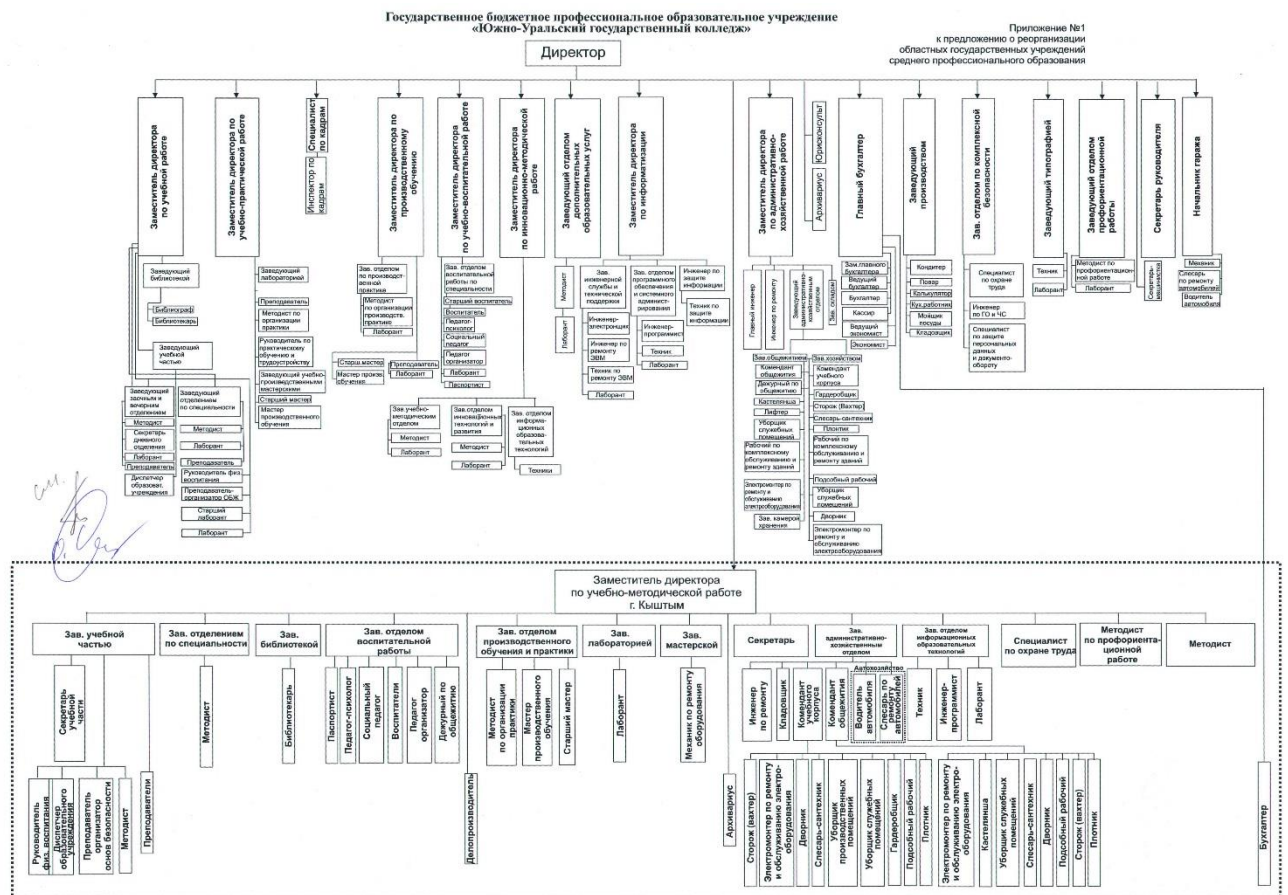


Рисунок 7 – Структура ГБПОУ «Южно-Уральский государственный колледж» [31]

Одной из основополагающих составных частей успешной деятельности образовательной организации является развитие системы обеспечения информационной безопасности и защиты информации [20]. Необходимость проведения мероприятий в этой области объясняется большим объёмом информации, находящимся в различных представлениях на территории колледжа.

Главной целью системы обеспечения ИБ является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационно-телекоммуникационной системы ГБПОУ «Южно-Уральский государственный колледж».

Для обеспечения учебного процесса цикловые комиссии и отделы ГБПОУ «Южно-Уральский государственный колледж» оснащены персональными компьютерами и необходимой техникой. Для решения производственных и учебных задач в колледже организована локальная сеть на одновременную работу 678 компьютеров. Все персональные компьютеры оснащены лицензионным программным обеспечением, подключены к локальной сети и имеют доступ в сеть Интернет, через защищенное соединение. Узлы оптических линий оборудованы управляемыми коммутаторами. В каждом комплексе имеется своя локальная сеть (100/1000 Мбит/с), охватывающая учебные корпуса и общежития. Создана единая локальная сеть колледжа (оптоволокно). В комплексах все компьютеры подключены к сети Интернет со скоростью доступа до 100 Мбит/с. На программном уровне защиты используются различные для студентов и сотрудников домены.

В колледже организована система электронного обучения – Moodle, она доступна для сотрудников и студентов колледжа, каждый имеет свой индивидуальный пароль и логин, доступ к системе возможен с любых

устройств. Портал построен на основе системы управления образованием (LMS). LMS позволяет управлять и распространять учебный материал и обеспечивать совместный доступ.

Открыт доступ к электронным образовательным ресурсам для студентов колледжа по сети Интернет, что позволяет использовать данные ресурсы в полном объеме.

Информационная система колледжа содержит огромное количество информационных ресурсов, зафиксированных на материальных носителях (информационное обеспечение хозяйственной деятельности, информация научно-технического характера, персональные данные сотрудников и обучающихся, базы данных организации, информация бытового характера о доступе к материальным товарам и услугам, обучающие ресурсы и т.д.), которые, в свою очередь, являются основным объектом защиты.

Информацией ограниченного доступа является:

- служебная тайна – информация, содержащая сведения о финансах, производстве, управлении и других видах деятельности субъекта, разглашение которой может нанести экономический ущерб;

- профессиональная тайна – сведения, содержащие организацию учебной деятельности и процессов;

- персональные данные – любая информация, содержащая сведения о конкретном лице (сведения о студентах, преподавателях и др.).

Информация общего доступа:

- постановления, указы, распоряжения;

- информация, содержащая статистические сведения об образовательной деятельности;

- информация, доступ к которой не ограничен законом и уставом.

На территории колледжа ведется круглосуточное наблюдение через пост охраны. Мониторинг объекта осуществляется через систему видеонаблюдения, которая установлена по периметру, а также в переходах образовательного комплекса и на главном, и со стороны запасных выходов.

Вход на территорию осуществляется по персональным пропускам и студенческим билетам. Посетители имеют право прибывать на территории только в сопровождении сотрудника организации. В колледже осуществлена пожарно-охранная сигнализация и установлены соответствующие датчики. Аппаратные средства хранения информации (сервера) располагаются в отдельном помещении.

Политика безопасности, реализована на избирательном способе управления доступом. Применение избирательной политики, соответствует требованиям по информационной безопасности, разграничению доступа, подотчетности. Реализацией этой политики безопасности занимается системный администратор. Такое управление характеризуется заданным администратором множеством разрешенных отношений доступа.

В качестве программного средства защиты от вредоносного программного обеспечения используется антивирусное решение «Kaspersky Endpoint Security для Windows», которая отвечает требованиям надежности, качества и системы защиты, предъявляемым для защиты корпоративных сетей.

Технически информационная безопасность и защита информации осуществляется при помощи системы паролей для доступа к ресурсам информационной системы разного уровня. Прежде всего, это пароль входа пользователя в операционную систему его рабочего места. Ввод этого пароля открывает пользователю доступ к ресурсам данного компьютера и к документам, хранящимся на нем. Политика безопасности настроена таким образом, чтобы пользователь не обладал полным правом на своем рабочем месте и не мог, например, установить вредоносное программное обеспечение или программы по копированию информации. Ограничение прав дает гарантию защищенности данных.

Для обучающихся не предусмотрены различные пароли для входа в операционную систему, есть единый пароль и логин для всех колледжа, для сотрудников и педагогов предусмотрена замена пароля 1 раз в месяц.

Когда пользователь вводит свой пароль для входа в операционную систему, он получает доступ не только к ресурсам данного компьютера, но и к ресурсам локальной компьютерной сети. Это возможно в том случае, если пользователь входит на компьютер как доменный или сетевой пользователь. В этом случае отнестись к разграничению прав пользователей в сети нужно еще более внимательно. Права сетевого пользователя настроены таким образом, чтобы дать ему возможность беспрепятственно работать со своими документами, но при этом ограничить доступ к документам, прав на работу с которыми у него нет, либо это только права на просмотр. В этом случае решается одновременно задача защиты данных от несанкционированного доступа и от случайной их порчи. Прерогативой распределения прав пользователей обладает системный администратор. Он разграничивает права пользователей по доступу к документам и приложениям как в сети, так и на локальных компьютерах.

Парольная защита доступа осуществляется в информационной системе «1С: Предприятие 8.3». Данная ИС имеет в своем составе механизм ведения списка пользователей и разграничения их прав доступа к данным. В результате можно гибко настроить доступ пользователей скрыв от несанкционированного доступа и от возможности случайной порчи данных, доступа к которым у пользователя нет. Обязанность распределения прав доступа пользователей лежит на системном администраторе колледжа.

Для того чтобы понять, насколько хорошо организована система обеспечения информационной безопасности колледжа, была проведена комплексная проверка состояния безопасности информационных систем ГБПОУ «ЮУГК» и выявлены следующие уязвимости системы и несоответствия.

Уязвимость информации есть событие, возникающее как результат такого стечения обстоятельств, когда в силу каких-то причин используемые в автоматизированных системах обработки данных средства защиты не в состоянии оказать достаточного противодействия проявлению

дестабилизирующих факторам и нежелательного их воздействия на защищаемую информацию [15]. Источники угроз используют уязвимости для нарушения безопасности информации. Кроме того, возможны действия источников угроз по активизации тех или иных уязвимостей, не связанных со злым умыслом [13].

Нормативное регулирование системы информационной безопасности ГБПОУ «ЮУГК» представлено документом «Политика безопасности», которая определяет цели и задачи СОИБ и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области ИБ, которыми руководствуются работники образовательной организации при осуществлении своей деятельности.

Основной целью «Политики безопасности» является защита информации при осуществлении уставной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных.

Ознакомиться с нормативной документацией в области информационной безопасности можно непосредственно в организации. Политика безопасности разработана в соответствии с:

1. Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральным законом от 27.07.2006 № 152-ФЗ «О 27 персональных данных».
3. Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».
4. Федеральным законом от 29.12. 2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
5. Приказом Министерства связи и массовых коммуникаций РФ от 16 июня 2014 г. № 161 «Об утверждении требований к административным и

организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию».

6. Указом Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».

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

8. Постановлением Правительства от 15.09.2008 РФ №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

9. Приказом ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и иными нормативными правовыми актами в сфере защиты информации.

Выполнение требований «Политики безопасности» является обязательным для всех структурных подразделений, ответственность за соблюдение информационной безопасности несет каждый сотрудник ГБПОУ «ЮУГК».

Проанализировав образовательную организацию, удалось выявить следующие уязвимости:

1. Отсутствие сертификата SSL. Сайт колледжа активно используется студентами и родителями, через сайт осуществляется вход в «Систему электронного обучения», где находятся образовательные материалы колледжа, а также «Электронный журнал», в котором отражена успеваемость студентов. На сайте расположено расписание и информация для сторонних организаций (портфолио педагогов, нормативные документы). Но отсутствие сертификата SSL может вызвать проблемы.

В данном случае это может быть сбой даты на компьютере или же вирусное программное обеспечение, с помощью которого злоумышленник может завладеть персональными данными пользователей или нарушить свойство доступности информации на сайте.

2. Несанкционированный доступ на территорию. На входе осуществляется термометрия сотрудников, обучающихся колледжа, при этом студент должен предъявить на входе студенческий билет. Уязвимостью является то, что никто не сверяет этот студенческий билет с оригиналом, и не ведет учет лиц, попадающих на территорию колледжа, потенциальный злоумышленник может пройти под видом родителя студента, либо пройти под видом студента, предъявив любой документ вахтеру.

3. Неквалифицированный персонал. Следует выделить отдельным пунктом данную уязвимость, которая может привести к потере важной документации, краже оборудования, разглашению персональных данных и т.д. Если мы говорим об обслуживающем персонале (уборщица, электрик, дворник, сантехник), то они спокойно перемещаются по территории колледжа и имеют доступ ко всем помещениям организации, уборка кабинетов происходит после занятий, поэтому сложно отследить их действия. Сюда же относится незнание базовых правил информационной безопасности педагогами и сотрудниками колледжа, которые могут привести к сбою в работе информационной системы. Невнимательность обучающихся при авторизации приводит к блокировке всей локальной сети, что ведет за собой нарушение доступности.

4. Отсутствие видеонаблюдения в учебных лабораториях. В колледже есть система видеонаблюдения, но она направлена на территорию при колледже. Хотя отсутствие видеонаблюдения в компьютерных классах оправдано, тем его что наличие может нарушать права несовершеннолетних обучающихся, но это приводит к тому, что перечисленные выше уязвимости приводят к более серьезным угрозам. Стоит отметить, что при случаях кражи или доступа на внутрь организации посторонних лиц будет тяжело опознать

злоумышленника, так как видеонаблюдение на входе может быть не достаточным для опознания источника угрозы.

9. Некорректная работа программного обеспечения, приводящая к потере или порче данных из-за: ошибок в прикладном или сетевом программном обеспечении; заражения систем компьютерными вирусами.

10. Технические сбои оборудования. Могут быть вызваны отключением электропитания; отказом дисковых систем и систем архивации данных; нарушением работы серверов, рабочих станций, сетевых карт, модемов, неправильная эксплуатация оборудования.

11. Отсутствие в общем доступе документов, регулирующих информационную безопасность в организации.

2.2 Мероприятия и средства по совершенствованию модели и методов информационной безопасности колледжа на основе физической защиты

При отладке процессов информационной безопасности в образовательной организации могут создаваться частные политики и модели.

Модели могут быть как статические, так и динамические (то есть оценки могут меняться в зависимости от изменений в объекте защиты или в зависимости от данных мониторинга или аудита ИБ) [5].

До начала процесса моделирования угроз и нарушителей ИБ обязательно происходит процесс моделирования и описания структуры объекта защиты. Данный этап не всегда формализован, но он всегда присутствует.

В стандарте СТО БР ИББС-1.0-2010 [2] введена следующая структурированная модель объекта защиты:

1. Уровень физический (линии связи, аппаратные средства и пр.).
2. Уровень сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и пр.).
3. Уровень сетевых приложений и сервисов.
4. Уровень операционных систем (ОС).

5. Уровень систем управления базами данных (СУБД).

Следует отметить, что данная модель является моделью информационной инфраструктуры и не охватывает аспекты физической защиты.

Для охвата также уровня физической защиты целесообразно использовать семирубежную модель защиты информации (ЗИ) [6]:

1. Периметр контролируемой территории.
2. Здания, расположенные на территории.
3. Помещения внутри здания, в которых расположены ресурсы автоматизированной системы (АС) и защищаемая информация.
4. Ресурсы, используемые для обработки и хранения информации, и сама защищаемая информация.
5. Линии связи, проходящие в пределах одного и того же здания.
6. Линии (каналы) связи, проходящие между различными зданиями, расположенными на одной и той же охраняемой территории.
7. Линии (каналы) связи, проходящие по неконтролируемой территории.

Определим следующую структуру объекта защиты (модель объекта защиты) (см. таблицу 1).

Таблица 1 – Структура ГБПОУ «Южно-Уральский государственный колледж» как объекта защиты

Название	Описание
Внешний контур	Средства внешней видеорегистрации, периметрическая защита, контроль доступа сотрудников или посетителей в здания организации – объекта защиты, также контроль за утечкой информации по побочным электромагнитным излучениям и наводкам, виброакустическому и прочим техническим каналам
Помещение	Разграничение на уровне помещений: система контроля и управления доступом в помещения объекта защиты, видеорегистрация коридоров
Внутри помещений	Регистрация и контроль действий субъекта доступа внутри помещения, в которое он получил доступ: система внутренней видеорегистрации, также контроль за использованием аппаратуры съема информации (например, фотоаппарат, устройство съема звуковой информации).
СЗИ от НСД	Контроль и разграничение доступа к объектам вычислительной техники внутренней сети организации: система защита информации от несанкционированного доступа

Продолжение таблицы 1

Контроль ввода/вывода	Контроль за входящей/исходящей информацией: включает в себя контроль устройств ввода/вывода, проверку входящей информации на наличие вредоносного программного обеспечения, реализацию и контроль за реализацией отделения сегментов внутренней сети организации от сети, из которой имеется доступ к сети Интернет, а также средства разработки, на уровне не выше сетевого уровня эталонной модели взаимодействия открытых систем (OSI), а также контроль за информацией, поступающей по электронной почте. Сюда не входит контроль за информацией, поступающей по специальным защищенным каналам
Операционные системы	Контроль и разграничение доступа субъекта на уровне операционной системы средства вычислительной техники, к которому он получил доступ
ЛВС	Контроль и разграничение доступа субъекта доступа между объектами внутренней сети организации (уровень локальной вычислительной сети – ЛВС)
Приложения	Контроль и разграничение доступа на уровне приложений, в частности учетных операционных систем (УОС)
СУБД	Контроль и разграничение доступа на уровне баз данных
Защищенные каналы	Контроль за информацией, поступающей по защищенным каналам, и контроль состояния самих каналов
Антивирусная защита	Защита информации от воздействия вредоносного кода

Данная модель изображена на рисунке 8.

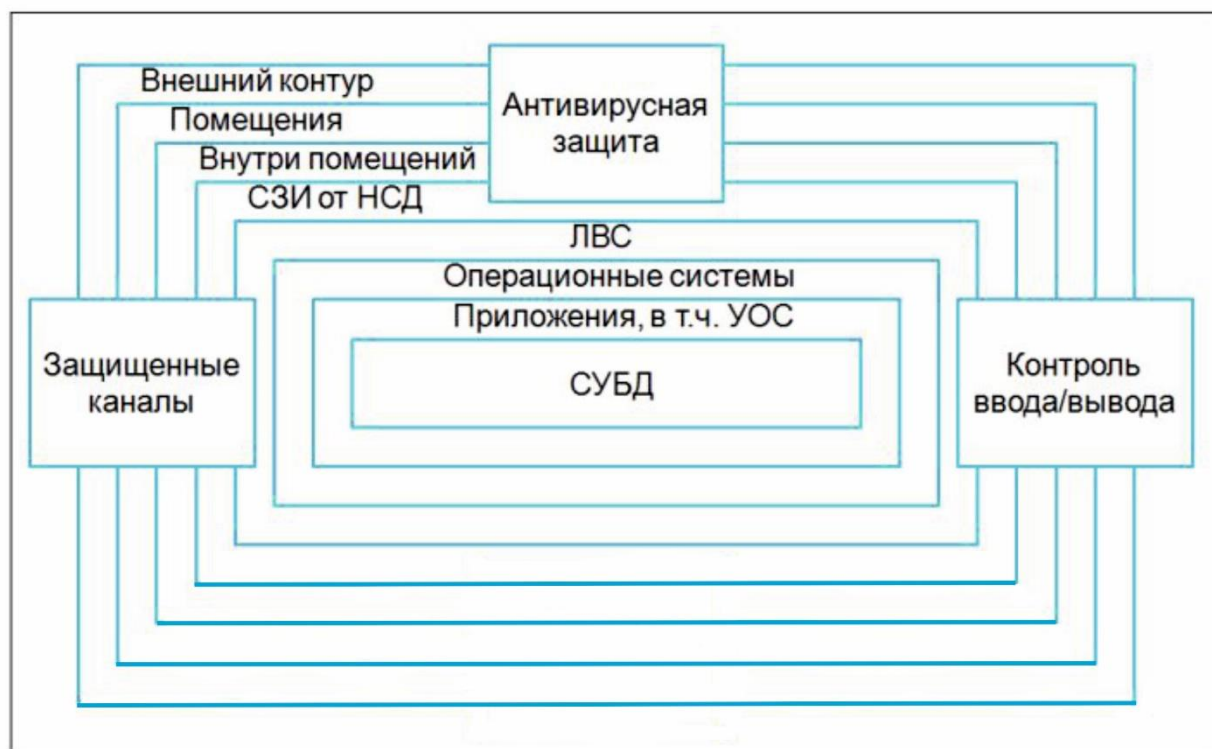


Рисунок 8 – Модель образовательной организации как объекта защиты

Выделение специализированных уровней, таких как контроль за входящей/исходящей информацией и уровень антивирусной защиты, позволяет предполагать, что в критически важных сегментах сети колледжа отсутствует вредоносное ПО и средства разработки ПО. Ввиду этого на уровнях СЗИ от НСД, операционных систем, ЛВС, прикладного ПО и СУБД можно применить единый подход по обеспечению ИБ: осуществить разграничение доступа для уменьшения возможности злоумышленных действий и осуществлять мониторинг ИБ. Причем для разграничения доступа и уменьшения возможностей привилегированных пользователей желательно применить эшелонированную (двойную) систему разграничения.

Целесообразно осуществлять мониторинг ИБ всех уровней (возможно, кроме уровня внешнего контура) из единого центра. Это позволяет оператору системы мониторинга получить полную картину происходящего в образовательной организации.

Для построения четкой структуры разграничения доступа на подконтрольном объекте крайне желательно реализовать структуру с жесткой групповой привязкой.

Для выполнения каждой из существующих функций создается группа. Роль взаимно-однозначно идентифицируется набором групп. Для каждой роли каждого сотрудника образовательной организации создается отдельная (персонифицированная) учетная запись. Эта структура обеспечивает прозрачность ролевой структуры на уровне мониторинга ИБ и дает возможность однозначно идентифицировать сотрудника и роль, которую он выполняет. Данная структура изображена на рис. 9.



Рисунок 9 – Ролевая структура подконтрольного объекта с жесткой привязкой по группам

Проведя исследование объекта, удалось выделить характерные виды угроз, с помощью кого или чего может произойти реализация, а также меры защиты, которые следует организовать это представлено в таблице 2.

Таблица 2 – Угрозы ГБПОУ «Южно-Уральский государственный колледж»

Угроза	Реализация	Меры защиты
Естественные угрозы (природные явления)		
Грозы	Погодные явления	Резервное копирование данных
Внутренние случайные угрозы (персонал)		
Неумышленный запуск вредоносных программ	Запуск вредоносного программного обеспечения сотрудником	Наличие антивирусного программного обеспечения, обучение персонала, разграничение прав доступа
Модификация, удаление или блокирование информации в результате неумышленных действий	Непреднамеренные действия сотрудников	Резервное копирование важной информации по расписанию, настройка теневого копирования на рабочих станциях, обучение персонала правилам работы при обработке информации
Неумышленное разглашение информации ограниченного доступа в результате разговора с персоналом фирмы	Ведение разговоров сотрудниками организации в присутствии посторонних лиц	Инструктаж сотрудников с записью под подпись об ответственности

Продолжение таблицы 2

Неумышленная утрата или порча документируемой информации	Халатное отношение персонала к своим обязанностям	Наличие ответственности в трудовом договоре; хранение важных документированной информации в сейфах
Некорректное уничтожение бумажных носителей информации	Халатное отношение персонала к своим обязанностям; незнание о возможных потерях информации	Инструктаж сотрудников, обучение правилам документооборота
Внутренние преднамеренные угрозы (персонал)		
Хищение или копирование информации на бумажном или электронном носителе	Злоумышленные действия персонала при работе с электронными или бумажными документами	Наличие ответственности в трудовом договоре; хранение важных документированной информации в сейфах, инструктаж об ответственности
Несанкционированный доступ к серверам, ЛВС, рабочим станциям	Злоумышленные действия персонала	Антивирусное ПО; парольная защита, запрещение неавторизованного доступа
Сговор со злоумышленником и помощь ему	Злоумышленные действия персонала	Наличие ответственности в трудовом договоре
Фото и видеосъемка документов	Злоумышленные действия персонала	Хранение важных документов в сейфах Наличие ответственности в трудовом договоре
Вандализм	Злоумышленные действия персонала и/или обучающихся колледжа	Резервное копирование данных инструктаж об ответственности Наличие ответственности в трудовом договоре
Внешние угрозы (злоумышленник)		
Физическое хищение или разрушение средств вычислительной техники	Проникновение в организацию; нарушение штатного режима функционирования СВТ	Сигнализация; Резервное копирование данных Хранение важных документов в сейфах
Несанкционированный доступ к серверам, ЛВС, рабочим станциям	Атака на сервера организации, коммутационное оборудование и рабочие станции	Антивирусное программное обеспечение; резервное копирование; внутренние механизмы защиты операционной системы, межсетевое экрана.
Программные закладки	Перехват информации	Использование сертифицированного программного обеспечения; использование средств антивирусной защиты

Приведенные в таблице 2 меры защиты будут статичны, то есть следует их выполнять всегда, а, чтобы контролировать исполнение этих защитных мер необходимо проводить целенаправленные мероприятия по информационной безопасности.

Достижение заданных целей возможно в ходе решения следующих основных задач:

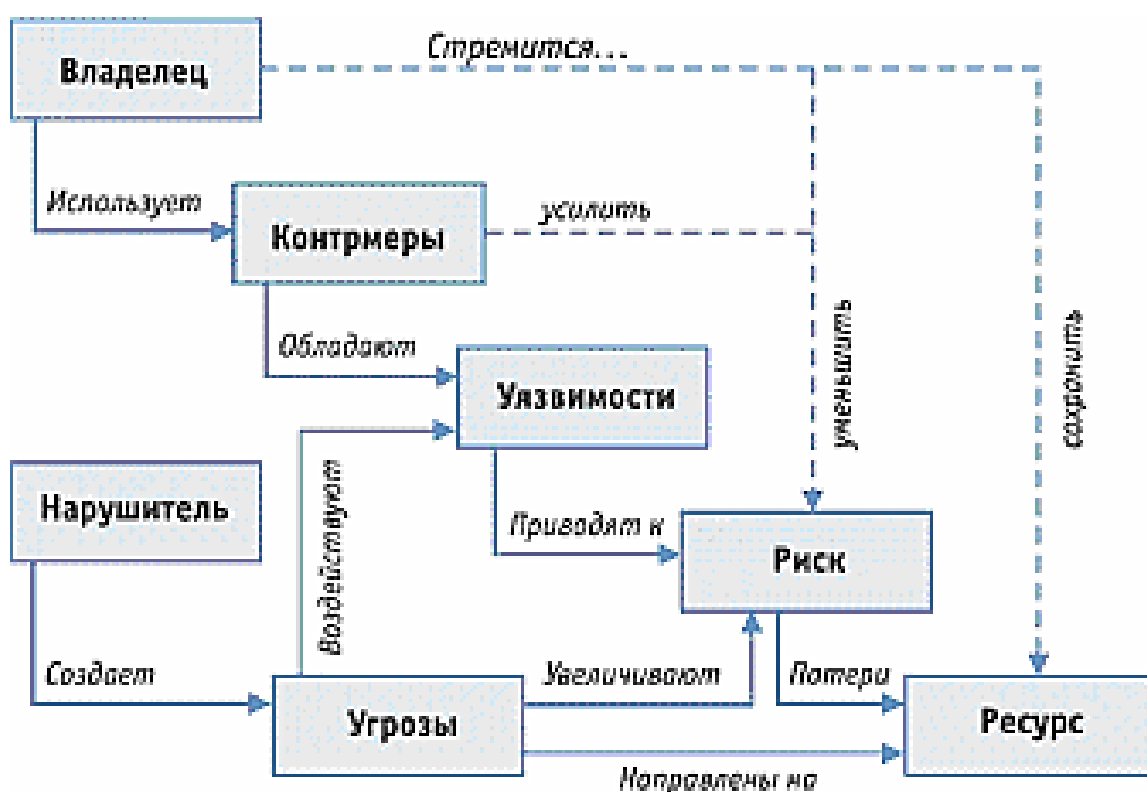
- отнесение информации к категории ограниченного доступа (служебной тайне);
- прогнозирование и своевременное выявление угроз безопасности информационным ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
- создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;
- создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения информационной безопасности на достижение стратегических целей.

Проектирование системы защиты, обеспечивающей достижение поставленных перед защитой информации целей и решение задач, проводится путем системного анализа существующей и разработки вариантов требуемой. Построение новой модели или ее модернизация предполагает:

- определение источников защищаемой информации и описание факторов, влияющих на ее безопасность;

- выявление и моделирование угроз безопасности информации;
- определение слабых мест существующей системы защиты информации;
- выбор рациональных мер предотвращения угроз;
- сравнение вариантов по частным показателям и глобальному критерию, выбор одного или нескольких рациональных вариантов;
- обоснование выбранных вариантов в докладной записке или в проекте для руководства организации;
- доработка вариантов или проекта с учетом замечаний руководства.

При выполнении работ можно использовать следующую модель построения системы информационной безопасности, приводимую на рисунке 10 и основанную на адаптации ОК (ISO 15408) и проведении анализа риска (ISO 17799).



Условные обозначения:

- > – естественное воздействие,
- - - - -> – управляющее воздействие.

Рисунок 10 – Модель построения системы информационной безопасности

Эта модель соответствует специальным нормативным документам по обеспечению информационной безопасности, принятым в международном стандарте ISO/IEC 15408 «Информационная технология» - методы защиты - критерии оценки информационной безопасности», стандарту ISO/IEC 17799 «Управление информационной безопасностью», и учитывает тенденции развития отечественной нормативной базы по вопросам информационной безопасности.

Представленная модель информационной безопасности — это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Рассматриваются следующие объективные факторы:

- угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;
- уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;
- риск - фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери - прямые или косвенные).

Для построения сбалансированной системы информационной безопасности предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для организации на основе заданного критерия. Систему информационной безопасности (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

Анализ состояния дел в сфере защиты информации показывает, что уже сложилась вполне сформировавшаяся концепция и структура защиты, основу которой составляют:

- хорошо развитый ассортимент технических средств защиты информации;
- значительное число, имеющих необходимые лицензии организаций, специализирующихся на решении вопросов защиты информации;
- четкая система взглядов на проблему защиты информации и наличие некоторого практического опыта.

Тем не менее, несмотря на это число злоумышленных действий над информацией не только не уменьшается, но и имеет достаточно устойчивую тенденцию к росту. Опыт показывает, что для борьбы с этой тенденцией необходима стройная и целенаправленная организация процесса защиты информационных ресурсов. Причем в этом должны активно участвовать профессиональные специалисты, администрация, сотрудники и пользователи, что и определяет повышенную значимость организационной стороны вопроса.

Мероприятия и средства по совершенствованию модели и методов информационной безопасности колледжа на основе физической защиты

Разработка политики защиты контролируемой зоны.

Для обеспечения защиты периметра контролируемой зоны были разработаны следующие положения и методы, необходимые к внедрению:

- замки и двери. Надежный замок в двери - первая строка физического обеспечения безопасности. Лучше использовать кодовый замок, который поддерживает безопасность на уровне пользователя. Необходимо установить различные комбинации для каждого пользователя и периодически менять их. Ввести процедуру блокировки доступа пользователя, который покидает организацию. Лучше использовать замок, имеющий защитный экран, такой, что только пользователь, вводящий комбинацию, может видеть вспомогательную клавиатуру. Замок нужно сконфигурировать для записи в журнал событий регистрации пользователей, входящих в закрытую область. Компании предоставляют блокирующие системы, которые поддерживают регистрацию. Эти замки имеют встроенный инфракрасный порт (IR), который можно задействовать для печати журнала событий и списка пользователей.

Кроме того, можно использовать замки с магнитными картами и идентификационные бейджи (proximity badges), которые поддерживают регистрацию событий. Основной риск для любой системы, которая требует от пользователей ввода кода, наличия идентификационной карточки или ключа связан с тем, что не имеющие на самом деле прав доступа пользователи все равно могут его получить;

- необходимо укрепить дверную раму и обшивку, петли расположить так, чтобы злоумышленники не могли снять дверь снаружи, или установите несъемные петли. Использовать для крепления петель и несущей конструкции длинные винты, уходящие в стену. Приварить гайки любых болтов, которые выходят на поверхность стальных дверей;

- потолки и полы. Чтобы перекрыть возможность доступа для злоумышленников, на стенах, которые наращаются до реального потолочного покрытия и пола, устанавливаются датчики движения в помещении. Стены, пол и потолок заэкранировать металлом;

- электроэнергия. Если основные панели выключателей находятся возле центра данных (например, снаружи за дверью), перенести их, либо запереть.

Один из возможных способов проникновения в систему - отключение энергии в надежде заблокировать сигнал тревоги и другое оборудование защиты периметра. Установить UPS для серверов и расположить оборудование контроля доступа так, чтобы иметь некоторую защиту на время отключения энергии.

Обеспечение защиты помещения проведения совещаний

Для организации усиления защиты помещения для проведения совещаний, в соответствии с категориями хранимой информации должны разработаны следующие меры по контролю доступа в помещение и документации:

- организована системы контроля управления доступом к помещению. Доступ в кабинет должен осуществляться только

уполномоченными на это лицами. Лица, не имеющие прав доступа к помещению, могут находиться там только с разрешения или в присутствии уполномоченного на это лица. В целях повышения защиты от несанкционированного проникновения необходимо установить на дверь электронный замок со считывателем карт. Владельцем карт может быть только доверенное лицо;

- на дверь установлена охранная сигнализация, для предупреждения взлома двери, электронного замка и получения несанкционированного доступа к помещению;

- для исключения утечки акустической информации сквозь дверной проем в коридор, использован звукопоглощающий материал, устанавливаемый между стеной и дверной рамой;

- на шкафы с хранящейся в них документацией будут установлены механические замки;

- вентиляционные шахты и вентиляционные люки в целях предотвращения утечки информации по акустическому каналу оборудованы специальными шумо-поглощающими перегородками, как показано на рисунке 11, где 1 - стенки короба вентиляции, 2 - звукопоглощающий материал;

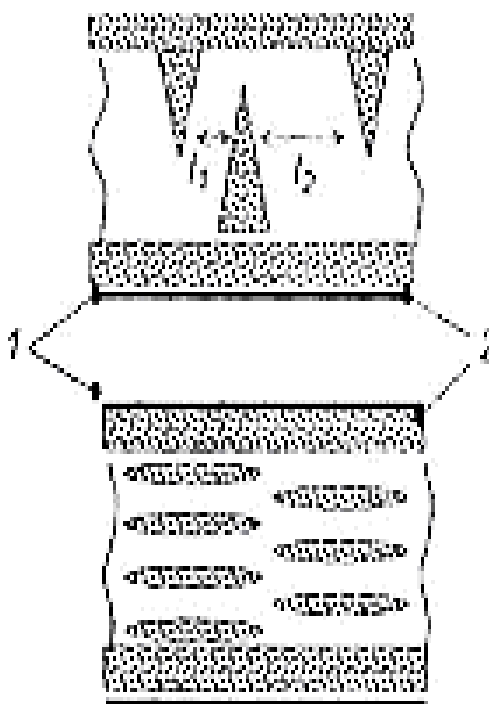


Рисунок 11 - Вентиляционная перегородка

- оконные стеклопакеты виброизолируются от рам с помощью резиновых прокладок для снижения возможности прямого акустического снятия информации. Так же на окна целесообразно установить подвижные жалюзи для перекрытия возможности прямого визуального снятия информации;

- предусматривается установка оконных решеток, для предотвращения проникновения посторонних лиц сквозь оконный проем;

- для защиты от утечки информации по параметрическому каналу целесообразно использование антистатических браслетов, а также специальных резиновых уплотнителей, которые устанавливаются на проводящие коммуникации - системы отопления в местах их входа и выхода в помещение.

Обеспечение защиты помещения директора (зам. директора).

Правила защиты кабинета директора имеют положения правил защиты комнаты для совещаний.

Тем не менее, ввиду наличия в данном помещении персонального компьютера с хранимой на ней конфиденциальной информацией, в добавок к разработанным методам усиления безопасности для помещения проведения совещаний вводятся нижеследующие положения:

- для защиты от утечки информации с ПЭВМ по параметрическому каналу целесообразно использование антистатических браслетов, а также специальных резиновых уплотнителей;

- по возможности расположить лицевую часть монитора таким образом, чтобы предотвратить возможность снятия визуальной информации через оконный или дверной проем;

- установка на персональный компьютер соответствующего программного обеспечения для защиты данных.

Обеспечение защиты помещения серверной.

В соответствии с ТИА/ЕИА 568А серверная комната - это местонахождение кросса для связи магистрали и горизонтальной проводки.

Кроме того, она служит для размещения оборудования связи, оконцевания кабеля и перекрестной проводки.

В соответствии с вышеназванным стандартом, правила проектирования защиты для серверных имеют следующие основные пункты, которые применены мной, для усиления информационной защиты объекта:

- на дверь установлена охранная сигнализация, для предупреждения взлома двери, электронный замок для предотвращения получения несанкционированного доступа к помещению;
- в соответствии с положениями о правилах организации серверных комнат, в данном проекте серверная комната располагается в центральной части этажа и не имеет наружных стен;
- в целях сокрытия местоположения серверной, на дверях отсутствуют какие-либо таблички и отличительные информационные знаки;
- в помещении устанавливаются датчики движения, камеры видеонаблюдения;
- перед входом телефонных линий в распределительный щиток устанавливается устройство защиты телефонных линий SEC - 2003;
- перед входом цепей питания и электроснабжения в распределительный щиток устанавливается генератор шума по сети 220 В - SEL SP - 41/С;
- для развязки линий электропитания вводится использование сетевых фильтров;
- в обязательном порядке производится заземление серверных стоек, в соответствии со схемой заземления, приведенной на рисунке 12;
- разрабатывается политика доступа доверенных лиц в помещение.

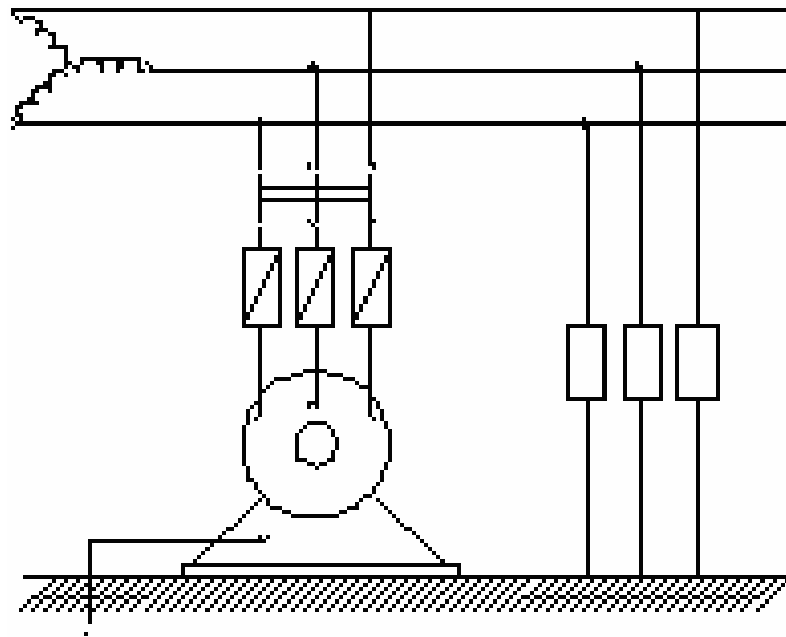


Рисунок 12 – Схема защитного заземления

Согласно требованиям, к противопожарной защите серверных помещений, серверные площадью более 24 м² оборудуются автоматическими установками пожаротушения. Серверные с меньшей площадью оснащаются автоматической системой пожарной сигнализации.

Системы пожаротушения, использующие в качестве огнетушащего состава воду, не подходят для пожарной безопасности серверной. Контакт воды с серверами недопустим.

Системы порошкового и аэрозольного пожаротушения также не подходят, потому что они не могут бороться с огнём в труднодоступных местах (например, если сервер находится в шкафу). Из труднодоступного места появляется дым, система открывает модуль пожаротушения над шкафом, система подаёт сигнал о срабатывании, возгорание же в это время разрастается. Очистить серверную и работать в ней дальше после попадания аэрозоля или порошка практически невозможно.

Остаётся один метод – газовое пожаротушение серверной по объёму (газовое огнетушащее вещество распространяется по всему помещению).

На сегодняшний день используются несколько модификаций газовых огнетушащих составов:

- углекислый газ (углекислый газ опасен для здоровья людей и достаточно сложен в хранении);

- инерген (для человека более безопасен чем углекислый газ, имеет меньше побочных эффектов, но на современном рынке пока не очень распространён);

- хладоны (Хладон 125, Хладон 227 ea, Хладон ФК-5-1-12 («Новек»)).

Для серверных помещений чаще всего используют хладоны.

Особенности серверной, как защищаемого объекта:

1. В серверной находится дорогостоящее оборудование. Газовая система пожаротушения максимально быстро определяет факт возгорания и сводит к минимуму ущерб. Газовый огнетушащий состав не причинит вред защищаемому оборудованию.

2. Останавливать функционирование серверной на длительное время нельзя. Это может нанести значительный ущерб. По этой причине в серверной необходимо использовать диэлектрики, что делает возможным борьбу с пожаром без отключения техники от напряжения.

3. Персоналу, находящемуся во время работы в серверной, должна быть обеспечена безопасность. Во время газового пожаротушения людей в помещении быть не должно.

Преимущества газового пожаротушения в серверной:

1. Установка автоматического газового пожаротушения работает круглосуточно.

2. Система газового пожаротушения оповещает сотрудников о возникновении пожара для эвакуации людей и принятия действий необходимых для локализации возгорания.

3. Газовая система пожаротушения для помещения серверной принимает, обрабатывает, контролирует и отображает сведения, поступающие от пожарных датчиков.

Газовую систему пожаротушения необходимо обеспечить электропитанием по 1-й категории. В вентиляции и системах

кондиционирования серверной предусматривают пожарные клапаны или заслонки для автоматического закрытия в случае срабатывания пожарных датчиков и выключения в помещении серверной системы автоматического газового пожаротушения.

На рисунке 13 представлено автономное-устройство-шкафного-пожаротушения-R-Line.



Рисунок 13 - Автономное-устройство-шкафного-пожаротушения-R-Line

Помещения серверных должны быть защищены современными установками газового пожаротушения, которые безопасны для людей и дорогостоящего оборудования.

Система контроля и управление доступом в колледж.

Система контроля и управление доступом в колледж рекомендуется построить на базе системы PERCo-S-20, это специально созданная версия для учебных заведений, которая не только предотвращает проникновение посторонних лиц в колледж, но и обеспечивает контроль прогулов и опозданий обучающихся, что способствует улучшению посещаемости и, как следствие, росту качества знаний.

Принципы работы системы. В зданиях колледжа необходимо оборудовать контрольно-пропускные пункты. Контрольно-пропускные пункты представляют собой огороженную часть помещения напротив

центрального входа в здание колледжа, оснащенную турникетами и пунктом контроля и учёта доступа.

Вход в здания колледжа и выход должен осуществляться строго через контрольно-пропускные пункты. Контрольно-пропускные пункты оснащены:

- автоматическими турникетами;
- пультами управления турникетами, позволяющих охраннику обеспечить свободный проход людей, в том числе и в случае возникновения чрезвычайных ситуаций, в обход турникетов;
- для огораживания контрольно-пропускных пунктов используются ограждения системы «антипаника», позволяющие в случае возникновения чрезвычайных ситуаций обеспечить свободный проход людей в обход турникетов (рис. 14).



Рисунок 14 - Контрольно-пропускной пункт

Проход через турникеты обеспечивается посредством персонифицированных карт доступа – пропуска. Пропуск представляет собой пластиковую карту с микрочипом для открытия электронного замка турникета. Пропуск имеет свой оригинальный код идентификации, который присваивается один на каждого отдельного пользователя в базе данных Системы.

Для прохода через контрольно-пропускные пункты колледжа владелец пропуска прилагает пропуск к считывателю (достаточно без касания), установленному на турникете. Считыватель считывает код доступа, соотносит его с базой данных Системы, автоматически открывает замок турникета (при

наличии права нахождения в колледже). Разрешение на проход подтверждается соответствующим звуковым и световым сигналом (зеленым индикатором на турникете). Далее необходимо в течение 4 секунд пройти через турникет.

Если владелец карты осуществил вход в здание, он должен обязательно осуществить и выход из здания с использованием пропуска, осуществить повторный вход невозможно до тех пор, пока не осуществлён выход.

Все события – входы и выходы по пропуску или по команде охранника фиксируются в энергонезависимой памяти Системы.

Системы контроля доступа и учета рабочего времени.

Еще одним вариантом системы контроля доступа в здание образовательной организации - автономная биометрическая система контроля доступа и учета рабочего времени. Терминал подключается к компьютеру по локальной сети (TCP/IP). Идентификация осуществляется с помощью отпечатков пальцев, карт и пароля. Прямое управление замком позволяет подключать к считывателю замки и турникеты различных производителей. В данном комплекте представлен расчет с подключение терминалов к роторному турникету-триподу.

Биометрическая система контроля, как и все оборудование СКУД предназначена для управления доступом на заданную территорию, для обеспечения:

- защиты материальных ценностей, информации, имущества, оборудования;
- безопасности сотрудников и посетителей;
- контроля, учета и управления доступом на объект (идентификация личности, определение зон и времени доступа, открытие дверей, турникетов, шлагбаумов и др.);
- рационального управление персоналом (при интеграции с соответствующим ПО).

К основным преимуществам биометрического оборудования СКУД относятся:

- высокая точность идентификации личности человека, проходящего контроль;
- сложность фальсификации биометрических признаков;
- высокая степень надежности, так как биометрический идентификатор нельзя забыть, как пароль, потерять как пластиковую карту, или воспользоваться чужими данными или картой, или пропуском.

К основным функциям:

1. Контроль и управление доступом, в том числе:

- идентификация личности по отпечаткам пальцев (или иным биометрическим признакам) и RFID-картам;
- доступ только зарегистрированных сотрудников и посетителей и определение их полномочий (право, зоны и время прохода);
- управление устройствами доступа в рамках полномочий личности (замки, турникеты, шлагбаумы, и т.д.);
- формирование сигнала тревоги при попытке несанкционированного доступа;
- ведение журналов событий и посещения;
- разграничение доступа по временным зонам;
- мониторинг событий в реальном времени возможность комбинированного доступа (отпечаток пальца или карта, карта и отпечаток пальца).

2. Система учета рабочего времени персонала, в том числе:

- автоматизированный учет времени прихода и ухода сотрудников;
- ведение табелей учета рабочего времени, при интеграции с соответствующим ПО (1С или SAP);
- формирование отчетов о наличии или отсутствии сотрудника на рабочем месте, об опоздании и ранних уходах;

– мониторинг персонала в режиме реального времени (кто и в каком месте находится в определенный или текущий момент времени);

– создание и ведение электронных баз и картотек сотрудников; импорт данных в интегрированные программы Microsoft, 1С Бухгалтерия, SAP и др.

3. Обеспечение безопасности помещения, в том числе:

– интеграция с любыми существующими системами безопасности зданий и сооружений (видеонаблюдение, охранная и пожарная сигнализация и др.);

– предотвращение несанкционированного доступа, инициация тревоги при соответствующих попытках проникновения.

Благодаря дружелюбному интерфейсу и подробной документации, работа с системой контроля и управления доступом понятна любому пользователю ПК. При этом, гибкая система настроек и прав доступа позволяет ограничить возможности того или иного сотрудника по работе с программой (рис. 15, 16).

Дата	Время	Комментарий	IP-адрес	Компьютер	Пользователь windows
Пользователь : Коновалов Дмитрий Александрович (Кол-во: 94)					
+ Событие : Вход в модуль (Кол-во: 47)					
+ Событие : Выход из модуля (Кол-во: 18)					
+ Событие : Просмотр журнала событий (Кол-во: 2)					
- Событие : Редактирование интервалов (Кол-во: 17)					
23.03.2010	10:28	Добавление интервала. Сотрудник: Бубнов Олег Игорьевич. Новый период: 23.03.2010 10:00:00-23.03.2010 19:00:00.	192.168.10.100	MEGA	Admin
23.03.2010	10:28	Добавление интервала. Сотрудник: Валуева Мария Александровна. Новый период: 23.03.2010 10:00:00-23.03.2010 19:00:00.	192.168.10.100	MEGA	Admin
23.03.2010	10:28	Добавление интервала. Сотрудник: Виленский Семен Дмитриевич. Новый период: 23.03.2010 10:00:00-23.03.2010 19:00:00.	192.168.10.100	MEGA	Admin
23.03.2010	10:28	Добавление интервала. Сотрудник: Иванов Алексей Дмитриевич. Новый период: 23.03.2010 10:00:00-23.03.2010 19:00:00.	192.168.10.100	MEGA	Admin
23.03.2010	10:28	Добавление интервала. Сотрудник: Коновалов Дмитрий Александрович. Новый период: 23.03.2010 10:00:00-23.03.2010 19:00:00.	192.168.10.100	MEGA	Admin
23.03.2010	10:28	Добавление интервала. Сотрудник: Кузнецов Сергей Васильевич. Новый период: 23.03.2010 10:00:00-23.03.2010 19:00:00.	192.168.10.100	MEGA	Admin
23.03.2010	10:28	Добавление интервала. Сотрудник: Лаптев Иван Николаевич. Новый период: 23.03.2010 10:00:00-23.03.2010 19:00:00.	192.168.10.100	MEGA	Admin
23.03.2010	10:29	Добавление интервала. Сотрудник: Лебедев Александр Денисович. Новый период: 23.03.2010 10:00:00-23.03.2010 19:00:00.	192.168.10.100	MEGA	Admin
23.03.2010	10:29	Добавление интервала. Сотрудник: Липова Татьяна Николаевна. Новый период: 23.03.2010 10:00:00-23.03.2010 19:00:00.	192.168.10.100	MEGA	Admin
23.03.2010	10:29	Добавление интервала. Сотрудник: Макаров Олег Петрович. Новый период: 23.03.2010	192.168.10.100	MEGA	Admin

Рисунок 15 – Журнал событий

Место и дата регистрации		Информация о сотруднике				ФАКТ				ПЛАН		Дополнительно				
Месяц	Дата	ФИО	Таб.	Должность	Подразделение	Приход	Уход	Прод.	Прогул	Приход	Уход	Прод.	Сп.	Р.ух.	< норм.	> норм.
Февреля 2010	08.02.2010	Администратор				08:53	18:00	8 ч. 7 мин.		09:00	18:00	8 ч.				7 мин.
Февреля 2010	08.02.2010	Коновалов Дмитрий Александрович	101	Директор	Администрация	09:00	18:00	8 ч.		09:00	18:00	8 ч.				
Февреля 2010	08.02.2010	Агеева Елена Викторовна	102	Бухгалтер	Бухгалтерия	09:05	18:05	8 ч.		09:00	18:00	8 ч.	5 мин.			
Февреля 2010	08.02.2010	Петров Алексей Викторович	103	Менеджер отдела	Отдел продаж "Це	09:10	19:00	8 ч. 50 мин.		09:00	18:00	8 ч.	10 мин.			50 мин.
Февреля 2010	08.02.2010	Сергеев Анатолий Михайлович	104	Маркетолог	Маркетинг	09:00	18:00	8 ч.		09:00	18:00	8 ч.				
Февреля 2010	08.02.2010	Кучина Мария Алексеевна	105	Кадровик	Отдел кадров	09:00	18:10	8 ч. 10 мин.		09:00	18:00	8 ч.				10 мин.
Февреля 2010	08.02.2010	Синев Александр Анатольевич	106	Специалист отдела	Отдел продаж "Це	08:50	18:00	8 ч. 10 мин.		09:00	18:00	8 ч.				10 мин.
Февреля 2010	08.02.2010	Малинов Сергей Алексеевич	111	Менеджер отдела	Отдел продаж "Юс	09:00	18:11	8 ч. 11 мин.		09:00	18:00	8 ч.				11 мин.
Февреля 2010	08.02.2010	Воронина Анна Николаевна	121	Менеджер отдела	Отдел продаж "Се	09:15	17:55	7 ч. 40 мин.		09:00	18:00	8 ч.	15 мин.	5 мин.	20 мин.	
Февреля 2010	08.02.2010	Уровев Виктор Петрович	122	Специалист отдела	Отдел продаж "Се	09:33	18:00	7 ч. 27 мин.		09:00	18:00	8 ч.	33 мин.		33 мин.	
Февреля 2010	08.02.2010	Морозова Оксана Петровна	112	Специалист отдела	Отдел продаж "Юс	08:45	18:00	8 ч. 15 мин.		09:00	18:00	8 ч.				15 мин.
Февреля 2010	08.02.2010	Калина Валерия Викторовна	109	Бухгалтер	Бухгалтерия	09:05	18:14	8 ч. 9 мин.		09:00	18:00	8 ч.	5 мин.			9 мин.
Февреля 2010	08.02.2010	Иванов Михаил Юрьевич	107	Работник склада	Склад	09:53	18:00	7 ч. 7 мин.		09:00	18:00	8 ч.	53 мин.		53 мин.	
Февреля 2010	08.02.2010	Сидоров Иван Иванович	123	Специалист отдела	Отдел продаж "Се	09:10	18:11	8 ч. 1 мин.		09:00	18:00	8 ч.	10 мин.			1 мин.
Февреля 2010	08.02.2010	Иванов Иван Петрович	124	Специалист отдела	Отдел продаж "Се	09:02	18:25	8 ч. 23 мин.		09:00	18:00	8 ч.	2 мин.			23 мин.
Февреля 2010	08.02.2010	Валерьев Василий Петрович	113	Специалист отдела	Отдел продаж "Юс	09:12	18:00	7 ч. 48 мин.		09:00	18:00	8 ч.	12 мин.			12 мин.
Февреля 2010	08.02.2010	Горюнова Елена Петровна	114	Специалист отдела	Отдел продаж "Юс	09:00	18:00	8 ч.		09:00	18:00	8 ч.				
Февреля 2010	08.02.2010	Степанова Светлана Игоревна	201	Маркетолог	Маркетинг	09:25	17:55	7 ч. 30 мин.		09:00	18:00	8 ч.	25 мин.	5 мин.	30 мин.	
Февреля 2010	08.02.2010	Макаров Иван Иванович	202	Работник склада	Склад				Прогул	09:00	18:00	8 ч.			9 ч.	

Рисунок 16 – Приходы/уходы

Биометрический терминал не требует постоянного подключения к компьютеру. При отключении питания или обрыве соединения с терминалом данные не будут потеряны, а подгрузятся в базу данных системы автоматически после устранения проблемы.

Подключение терминалов к локальной сети позволяет монтировать терминал там, где есть (или может быть протянута) локальная сеть Вашей организации или интернет. Это позволяет размещать биометрические терминалы контроля доступа на большом расстоянии от сервера, на котором установлена программа.

Помимо этого, сетевое подключение обеспечивает обмен данными в реальном режиме времени. События регистрации приходов и уходов персонала будут мгновенно записаны в базу данных системы и отображены на мониторе сотрудника отдела кадров или охраны.

Сетевой интерфейс терминалов позволяет быстро масштабировать систему. Для подключения новой проходной с новым турникетом, достаточно установить там терминалы и подключить его к локальной сети (рис. 17).











Рисунок 17 – Схема подключения терминала к локальной сети

Функционал системы TimeControl позволяет решить любую задачу контроля доступа и учета рабочего времени. Ниже перечислены основные возможности системы представлены в таблице 3.

Таблица 3 - Функционал системы TimeControl

	<p>Ведение графика работ сотрудников. Учет больничных, командировок, отпусков, отгулов и т.д. Гибкий график работ. Учет обеденного перерыва (фиксированного, плавающего, адаптивного).</p>
	<p>Мгновенная регистрация и мониторинг опозданий, ранних уходов, прогулов. Контроль сотрудников на пропускных пунктах организации.</p>
	<p>Возможность добавления собственных событий. Регистрации местных командировок и отгулов. Учет задач и поручений.</p>
	<p>Расчет заработной платы (премий, удержаний) на основе заданного графика работ и фактически отработанного времени. Почасовая тарификация. Учет опозданий, прогулов, ранних уходов при расчете заработной платы.</p>

Продолжение таблицы 3

	Использование временных пропусков и учет посетителей организации. Печать пропусков для сотрудников и создание шаблонов пропусков.
	Более 60 отчетов , покрывающих весь спектр учета рабочего времени сотрудников. В том числе, унифицированный табель T-13 и T-12 .
	Импорт справочников из DBF, XLS, XML, TXT . Экспорт данных в XLS и PDF . Интеграция с 1С 7.7 и 1С 8.1, 8.2, 8.3 . Возможность импорта сотрудников, подразделений, должностей из 1С. Экспорт табеля учета рабочего времени в 1С.
	Автоматическое построение отчетов по расписанию с отправкой по электронной почте и FTP .
	Дополнительно можно приобрести модуль фотофиксации, позволяющий получать фото сотрудников с IP камер при регистрации прихода\ухода.
	Разграничение прав доступа сотрудников по работе с программой.
	Интервальный доступ в подконтрольные помещения. Разграничение времени прохода и уровня доступа сотрудников в контролируемые зоны.
	SMS информирование о приходах\уходах, опоздания сотрудников и днях рождениях.

В комплект включено:

1. Турникет Ростов Дон Т9М1.
2. Два биометрических терминала FP30+RFID для подключения на вход и на выход (с обеих сторон турникета).
3. Блок питания 12В 3,5А.
4. Три преграждающих планки к роторному турникету.
5. CD диск с программным обеспечением TimeControl и лицензией на 30 сотрудников. Количество сотрудников может быть увеличено покупкой

дополнительной лицензии. Например, стоимость комплекта на 50 сотрудников будет на 1 800 р. дороже.

6. Инструкции по установке и настройке системы.

7. Один год подписки на обновления на новые версии программного комплекса и технической поддержки по почте и телефону.

8. Неограниченное количество дополнительных рабочих мест.

9. Один год бесплатной технической поддержки при старте.

На рисунке 18 представлен турникет по отпечаткам.



Рисунок 18 – Турникет по отпечаткам

Преимущества применения биометрической системы контроля доступа в образовательной организации:

- ограничение доступа в образовательную организацию;
- информирование родителей о приходе-уходе студента в учебное заведение с помощью SMS-сообщения;
- ограничение доступа в служебные помещения, компьютерные классы, преподавательские и др.;
- ограничение доступа к персональным данным студентов и сотрудников;

- контроль питания;
- автоматизация работы библиотеки (выдача и сдача книг по отпечатку).

Опишем общие права и обязанности сотрудников, обучающихся, родителей (законных представителей) обучающихся и посетителей колледжа.

Пропускной режим строится на принципах доброжелательности и взаимоуважения участников отношений.

Сотрудникам, обучающимся, родителям (законным представителям), посетителям колледжа запрещается вносить в здание взрывчатые вещества, горючие и легковоспламеняющиеся жидкости и материалы, другие материалы и вещества, способные нанести ущерб жизни и здоровью людей.

Сотрудники и обучающиеся колледжа обязаны:

- проходить через контрольно-пропускной пункт только по персональному пропуску;
- по требованию охранника или администрации колледжа (дежурного администратора) предъявлять персональный пропуск;
- бережно относиться к оборудованию Системы контроля и управления доступом и персональному пропуску;
- незамедлительно сообщать охраннику или ответственному лицу за Систему контроля и управления доступом об утере персонального пропуска;
- соблюдать правила пользования Системы контроля и управления доступом.

Лица, нарушающие пропускной режим (проход через турникет по чужому пропуску, по пропуску неустановленного образца, пронос запрещенных предметов) задерживаются охранником на контрольном пропускном пункте.

При угрозе проникновения в колледж лиц, нарушающих пропускной режим, администрация колледжа оставляет за собой право вызвать представителей правоохранительных органов.

Сотрудникам и обучающимся колледжа запрещается:

- передавать личный пропуск другим лицам;
- разбирать или ломать персональный пропуск.

За порчу оборудования Системы контроля и управления доступом, персонального пропуска, в том числе и его утерю, виновник обязан возместить в полном объеме расходы на восстановление имущества.

Электронный пропуск является собственностью колледжа, в случае его утери владелец пропуска несет за него материальную ответственность. На безвозмездной основе электронный пропуск выдается обучающимся и сотрудникам колледжа один раз.

Пропуски лиц, убывающих из колледжа на длительное время (отпуск, болезнь, командировка и т.п.) могут сдаваться на хранение лицам ответственными за Систему контроля и управления доступом.

Пропуск принадлежит обязательной сдаче:

- обучающимися, после окончания прохождения обучения в колледже;
- сотрудниками, при расторжении трудовых отношений.

Родители (законные представители) обучающихся и посетители колледжа обязаны соблюдать требования пропускного режима в колледж.

Сайт колледжа.

В качестве защитных мер для сайта колледжа можно перенести его на сервер CloudFlare — это сеть серверов по всему миру, к которой можно подключить свой сайт, чтобы увеличить скорость их загрузки и защитить от DDoS-атак. Cloudflare обеспечивает безопасность и надежность общедоступных ресурсов, а также защищает внутренние ресурсы: приложения за межсетевым экраном и устройства сотрудников.

Установка кондиционера в компьютерных классах.

Чтобы избежать технического сбоя аппаратуры необходимо поддерживать температурный режим помещения в пределах 20-24 °С, если в помещении с работающими ПК будет приближаться к 40, то жёсткий диск может быстро выйти из строя. Так же согласно СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или)

безвредности для человека факторов среды обитания» в оборудованных индивидуальными рабочими местами с персональным компьютером параметры температурного режима должны быть в пределах 18-24°C. [23].

Повышение температуры неблагоприятно сказывается на самочувствие обучающихся, что может привести таким угрозам как «ошибка пользователя» и т.д. Поэтому необходимо создавать благоприятные условия в учебной аудитории для этого можно установить систему кондиционирования. С ее помощью можно поддерживать такие параметры (температуры, влажности, чистоты, скорости движения воздуха). В данном случае установка кондиционера позволит значительно 40 в дальнейшем сэкономить средства, за счет правильной эксплуатации компьютерного оборудования. В качестве оптимального варианта подойдет настенная сплит-система – это бытовые системы кондиционирования большой мощности, так как подходят для небольших аудиторий и классов (рис. 19).



Рисунок 19 – Настенная сплит-система

Таким образом, предложена модель образовательной организации как объекта защиты, модель конкретного подконтрольного объекта на объекте защиты.

Внедрение и улучшение процессов моделирования, классификации учетных записей в образовательной организации позволяет осуществить эффективные мониторинг ИБ и защиту информации от несанкционированного

доступа, а также совершенствовать СОИБ образовательной организации в целом.

2.3 Расчет экономической эффективности внедрения рекомендаций по совершенствованию модели и методов информационной безопасности в организации профессионального обучения

Оценка эффективности является важным элементом разработки проектных и плановых решений, позволяющим определить уровень прогрессивности действующей структуры, разрабатываемых проектов или плановых мероприятий и проводится с целью выбора наиболее рационального варианта структуры или способа ее совершенствования. Эффективность защитных мероприятий (ЗМ) должна оцениваться на стадии проектирования, для получения наилучших показателей работоспособности системы в целом.

При разработке проекта важны экономические показатели, которые наряду с техническими результатами будут определять эффективность системы. В состав затрат на разработку и исследование включаются затраты на проведение всех этапов работ.

Затраты на обеспечение информационной безопасности следует считать эффективными, если они обеспечивают выполнение требований нормативных документов и стандартов, принятых государством, а также концепции информационной безопасности организации.

Совокупная стоимость владения для системы ИБ в общем случае складывается из стоимости: проектных работ; закупки и настройки программно-технических средств защиты, включающих следующие основные группы: межсетевые экраны, средства криптографии, антивирусы и ААА (средства аутентификации, авторизации и администрирования); затрат на обеспечение физической безопасности; обучения персонала; управления и поддержки системы (администрирование безопасности); аудита ИБ; периодической модернизации системы ИБ [8].

При этом затраты на приобретение и ввод в действие программно-технических средств могут быть получены из анализа накладных, записей в складской документации и т.п.

Величина выплат сотрудникам может быть взята из ведомостей. Объемы выплат заработной платы должны учитывать реально затраченное время на проведение работ по обеспечению информационной безопасности.

Суммарно ежегодные затраты на информационную безопасность складываются из трех показателей: затраты на административно-организационные мероприятия; затраты на технические мероприятия; затраты на ликвидацию последствий.

Затраты на административно-организационные мероприятия (АОМ) в образовательных организациях обычно меньше затрат на технические средства (таблица 4).

Таблица 4 – Расходы на предложенные АОМ по системе защиты информации в колледже

Мероприятие	Бюджет
Комплекс профилактических мер по соблюдению сотрудниками требований по ИБ (16000 руб.)	10000 руб.
Плановая проверка и обслуживание всех информационных систем и информационной инфраструктуры на работоспособность (20000 руб.)	22000 руб.
Всего: 36000 руб. в год	Всего: 32000 руб. в год

Суммарно расходы на административно-организационные мероприятия по повышению эффективности защиты информации в ГБПОУ «ЮУГК» составят 32000 рублей.

Предварительные расходы на мероприятия по совершенствованию модели и методов обеспечения информационной безопасности в ГБПОУ «ЮУГК» представлены в таблице 5.

Таблица 5 - Расходы на предложенные мероприятия по совершенствованию модели и методов обеспечения информационной безопасности в ГБПОУ «ЮУГК»

Мероприятие	Бюджет
Установка Системы контроля доступа и УРВ (от 105400 руб.)	40000 руб.
Преграждающая планка «Антипаника» (5100 руб.)	10000 руб.
Биометрические считыватели (14100 руб.)	15000 руб.
Бесконтактная карта Clamshell Card (за 1 шт) (30 руб.)	20000 руб.
Биометрические USB считыватели TimeControl U1 (6400 руб.)	10000
Автоматическая система пожаротушения для серверной (54000 руб.)	50000
Установка кондиционера в компьютерных классах (175000 руб.)	170000
Сервер CloudFlare (156000 руб.)	140000
Всего: 546000 руб.	Всего: 455000 руб.

Суммарно расходы на мероприятия по совершенствованию эффективности защиты информации в ГБПОУ «ЮУГК» составят 546000 тысяч рублей.

Из вышеприведенной таблицы следует, что реализация мероприятий по совершенствованию системы обеспечения информационной безопасности ГБПОУ «ЮУГК» требует значительных денежных вложений, которые позволяют устранить выявленные уязвимости и предотвратить возможные угрозы.

Соотношение оценки затрат на внедрение мероприятий к возможному ущербу составляет 21% и является достаточным, чтобы поддерживать СОИБ ГБПОУ «ЮУГК» на необходимом уровне. Следует отметить, что нет идеальной системы, которая будет обеспечивать защиту на 100 %, в данном случае предложенные мероприятия позволяют приблизиться к отметке в 90%, при условии, что все в организации будут к этому стремиться.

Рассчитаем отдачу от инвестиций на административно-организационные мероприятия и программно-аппаратные средства защиты конфиденциальной информации в ГБПОУ «ЮУрГТК» по формуле (1.1)

$$rosi(t, aom) = \frac{\Delta \text{Доходы} - \Delta \text{Расходы}}{\Delta \text{Инвестиции}}$$

где $rosi(t, aom)$ - отдача от инвестиций на программно-аппаратные средства и административно-организационные меры, $\Delta \text{Доходы}$ - изменения в доходах, обусловленные инвестициями ИБ (возможных поступлений средств от предотвращенных потерь), $\Delta \text{Расходы}$ - изменения в расходах, обусловленные инвестициями ИБ, $\Delta \text{Инвестиции}$ - инвестиции, сделанные в информационную безопасность.

$$rosi(t) = \frac{560000 - 546000}{455000} \approx 0,03$$

$$rosi(aom) = \frac{560000 - 36000}{32000} \approx 16,3$$

Далее, вычислим показатель отдачи от инвестиций в информационную безопасность после внедрения изменений в систему ИБ по формуле (1.2)

$$ROSI(t, aom) = ROSIold \frac{Iold - \Delta \text{Расходы}}{Iold + \Delta I} + rosi(t, aom) \frac{\Delta I}{Iold + \Delta I}$$

где $ROSI(t, aom)$ - показатель отдачи от инвестиций в информационную безопасность после внедрения программно-аппаратных средств и административно-организационных изменений в систему ИБ, $ROSIold$ - показатель отдачи от инвестиций до внесения изменений в систему ИБ, $Iold$ - уже сделанные инвестиции, $\Delta \text{Расходы}$ - изменения в расходах, обусловленные инвестициями ИБ, $rosi(t, aom)$ - отдача от инвестиций на программно-аппаратные средства и административно-организационные меры.

$$ROSI(t) = 2,55 \frac{0 - 546000}{0 + 455000} + 2,05 \frac{455000}{0 + 455000} \approx 0,8$$

$$ROSI(aom) = 4,73 \frac{0 - 36000}{0 + 32000} + 3,5 \frac{32000}{0 + 36000} \approx -0,7$$

В обоих случаях, видно, что $rosi(t, aom) > ROSI(t, aom)$, следовательно, внедрение проекта приведет к увеличению ROSI в ГБПОУ «ЮУГК» (в ИБ).

Итак, в результате анализа совокупных показателей существует возможность сделать обоснованный выбор в пользу предложенных мероприятий по совершенствованию системы защиты колледжа.

Таким образом, предложенные мероприятия по совершенствованию системы защиты информации колледжа несут в себе не только положительные моменты, такие как устранение основных проблем в организации среднего профессионального образования, касающихся информационной безопасности, но при этом они потребуют дополнительных вложений на разработку нормативных документов, касающихся политики безопасности. Потребуется дополнительных затрат труда и не исключат стопроцентно риски.

Всегда будет иметь место человеческий фактор, форс-мажорные обстоятельства. Но если такие меры не предпринять затраты на восстановление информации, потерянные возможности по стоимости превзойдут те затраты, что требуются для разработки системы безопасности.

Выводы по главе 2

ГБПОУ «Южно-Уральский государственный колледж» является старейшим в Уральском регионе государственным средним профессиональным образовательным учреждением повышенного типа.

Во второй главе магистерской диссертации на основе анализа состояния защиты информации в ГБПОУ «Южно-Уральский государственный колледж» были предложены рекомендации по совершенствованию модели и методов обеспечения информационной безопасности на основе физической защиты.

Одной из основополагающих составных частей успешной деятельности образовательной организации является развитие системы обеспечения информационной безопасности и защиты информации. Необходимость проведения мероприятий в этой области объясняется большим объёмом информации, находящимся в различных представлениях на территории колледжа.

В ходе анализа ГБПОУ «ЮУГК» были выявлены следующие уязвимости: отсутствие сертификата SSL/TLS на сайте колледжа из-за чего невозможно выполнить защищённое соединение с шифрованием данных, что существенно уменьшит шансы злоумышленнику провести атаку на целевой хост; контрольно-пропускной режим, на входе которого никто не проверяет этот студенческий билет, поэтому в колледж может пройти кто угодно под видом студента, предъявив документ вахтеру; участники образовательного процесса, которые могут действовать в своих интересах; незнание базовых правил информационной безопасности педагогами и сотрудниками колледжа, которые могут привести к сбою в работе информационной системы; отсутствие видеонаблюдения в учебных лабораториях; некорректная работа программного обеспечения, приводящая к потере или порче данных; технические сбои оборудования; отсутствие в общем доступе нормативно-правовой документации, регулирующей информационную безопасность в организации.

Основными методами физической защиты являются: железные двери, замки, камеры видеонаблюдения и сигнализации, охрана и ограничение доступа к объекту защиты.

В качестве объекта защиты были выбраны помещения проведения совещаний, помещения серверной и контроль доступа и учета рабочего времени.

Для ГБПОУ «Южно-Уральский государственный колледж» были предложены следующие рекомендации по совершенствованию модели и методов обеспечения информационной безопасности на основе физической защиты:

- I. Автоматическая установка пожаротушения.
- II. Система контроля и управление доступом в колледж на базе системы PERCo-S-20.
- III. Установка кондиционера в компьютерных классах.
- IV. Установка сервера CloudFlare.

Реализация данных мероприятий требует значительных денежных вложений, которые в свою очередь позволяют устранить выявленные уязвимости и предотвратить возможные угрозы.

Проведен расчет экономической эффективности внедрения рекомендаций по совершенствованию модели и методов обеспечения информационной безопасности на основе физической защиты в ГБПОУ «Южно-Уральский государственный колледж».

В результате вычисления подтверждают экономическую эффективность и целесообразность использования рекомендованных мер при внедрении их в процесс информационной безопасности образовательной организации. Предложенные рекомендации по совершенствованию модели и методов обеспечения информационной безопасности на основе физической защиты являются экономически оправданными.

ЗАКЛЮЧЕНИЕ

В магистерской диссертации предложены мероприятия и средства по совершенствованию модели и методов информационной безопасности ГБПОУ «Южно-Уральский государственный колледж» на основе физической защиты.

В качестве основных результатов диссертационной работы можно выделить следующие:

1. В первой главе были раскрыты сущность и содержание физической защиты информации, изучены модели обеспечения информационной безопасности и виды угроз в образовательной организации.

Физическая защита информации является таким методом защиты информационных ресурсов, при котором применяются организационные мероприятия и совокупности средств, способные препятствовать несанкционированному проникновению или доступу неуполномоченных физических лиц к защищаемому объекту. Основные организационные мероприятия, направленные на поддержание физической защиты информации, предусматривают установление режимных, пространственных, временных, территориальных и иных ограничений относительно условий использования и распорядка работы объекта защиты.

Как правило, при создании СОИБ организации происходит высокоуровневое моделирование, создаются неформализованные модели, которые образуют следующий возможный комплекс документов: концепция обеспечения ИБ организации; политика ИБ организации; модель угроз; модель нарушителей.

К основным моделям информационной безопасности относятся концептуальная, математическая и функциональная модели.

Под угрозами безопасности информационной системы понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации или

несанкционированными, непреднамеренными воздействиями на нее. Как правило, защита от угроз, в основном регламентируется инструкциями, разработанными и утвержденными в образовательной организации с учетом особенностей эксплуатации информационных систем организации и действующей нормативной базой образовательной организации.

2. Вторая глава отражает результаты анализа системы обеспечения информационной безопасности ГБПОУ «Южно-Уральского государственного колледжа», которые позволили выявить следующее: отсутствие сертификата SSL/TLS на сайте колледжа из-за чего невозможно выполнить защищённое соединение с шифрованием данных; возможность несанкционированного доступа на территорию организации; участники образовательного процесса, которые могут действовать в своих интересах; незнание базовых правил информационной безопасности педагогами и сотрудниками колледжа, которые могут привести к сбою в работе информационной системы; некорректная работа программного обеспечения, приводящая к потере или порче данных; технические сбои оборудования; отсутствие в общем доступе нормативно-правовой документации, регулирующей информационную безопасность в организации.

Также были сформулированы рекомендации по совершенствованию модели и методов обеспечения информационной безопасности колледжа и произведен расчёт эффективности предложенных мероприятий и средств.

В качестве рекомендаций по применению результатов диссертации предлагается: установить систему контроля управления доступом; установить систему кондиционирования для корректной работы компьютерного оборудования; перенести сайт на сервер CloudFlare; автоматическая установка пожаротушения.

Проведен расчет экономической эффективности внедрения рекомендаций по совершенствованию модели и методов обеспечения информационной безопасности на основе физической защиты в ГБПОУ «Южно-Уральский государственный колледж».

Реализация данных мероприятий требует значительных денежных вложений, которые в свою очередь позволяют устранить выявленные уязвимости и предотвратить возможные угрозы, при этом соотношение оценки затрат на внедрение мероприятий к возможному ущербу будет являться достаточным, чтобы поддерживать систему обеспечения информационной безопасности ГБПОУ «ЮУГК» на необходимом уровне.

На основании вышеизложенного цель исследования достигнута, поставленные задачи выполнены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Абидарова А. А. Физические средства защиты информации / А. А. Абидарова // Наука, образование и культура. – 2019. – №2 (36). – URL: <https://cyberleninka.ru/article/n/fizicheskie-sredstva-zaschity-informatsii> (дата обращения: 13.06.2023).
2. Ажмухамедов И.М. Решение задач обеспечения информационной безопасности на основе системного анализа и нечеткого когнитивного моделирования / И. М. Ажмухамедов. – URL: <https://arxiv.org/ftp/arxiv/papers/1204/1204.3245.pdf> (дата обращения 13.03.2023).
3. Апатова Н. В. Информационная безопасность социально-экономических систем: монография / Апатова Н.В, Акинина Л.Н., Байздренко Е.А., Бойченко О.В., Гапонов А.И., Герасимова С.В., Королев О.Л., Писарюк С.Н., Потанина М.В., Рыбников А.М., Рыбников М.С., Ремесник Е.С., Смирнова О.Ю., Титаренко Д.В. и др. / под ред. проф. О.В Бойченко. – Симферополь: ИП Зуева Т.В., 2017 – 302 с.
4. Артем П. Модель информационной безопасности / П. Артем // CISO CLUB Информационная безопасность, октябрь 2020. – URL: <https://cisoclub.ru/model-informaczionnoj-bezopasnosti/#> (дата обращения: 16.05.2023).
5. Баранова Е.К. Основы информационной безопасности: учебник [Текст] / Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2019. — 202 с.
6. Белов Е. Б. Основы информационной безопасности: учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2016. – 544 с.
7. Бойченко О.В. МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ / О.В. Бойченко, Д. В. Иванюта // Экономика строительства и природопользования. 2021. №3 (80). – URL:

<https://cyberleninka.ru/article/n/modeli-informatsionnoy-bezopasnosti> (дата обращения: 06.05.2023).

8. Бойченко О.В. Система комплексной защиты данных в корпоративных сетях / О.В. Бойченко, А.С. Ивченко // Проблемы информационной безопасности: IV Междунар. Науч.-технич. Конф., 15-17 февраля 2018 г. – Симферополь- Гурзуф, 2018 – С.139-140.

9. Виды и источники угроз информационной безопасности http://infoprotect.net/note/vidyi_i_istochniki_ugroz_informacionnoy_bezopasnosti (дата обращения: 16.04.2023).

10. Вихорев С.В. Классификация угроз информационной безопасности / С.В. Вихров. – URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml/ (дата обращения: 22.04.2023).

11. Волков Д. Физические средства защиты информации / Д. Волков. – URL: <https://cyber-defence.ru/fizicheskie-sredstva-zaschity-informatsii/> (дата обращения: 15.05.2023).

12. Волхонский В., Малышкин С. Определение, состав и функции систем физической защиты / В. Волхонский, С. Малышкин // «Алгоритм Безопасности», № 4, 2014. – URL: <http://www.cprspb.ru/bibl/object/45.htm> (дата обращения: 15.05.2023).

13. Гришина Н.В. Основы информационной безопасности предприятия: учебное пособие / Н. В. Гришина. - Инфра-М., 2019. – 216 с.

14. Давлетханов М.А. Оценка затрат компании на ИБ [Текст] / М.А. Давлетханов. – URL: <http://www.getinfo.ru/article682.html> (дата обращения: 05.05.2023).

15. Долгий П. А. Актуальные вопросы физической защиты информации / П.А. Долгий, М.С. Костерев, А. Е. Сушков, Ю. А. Пылинская, В. В. Гудков // Инновации и инвестиции. – 2020. – №8. – URL: <https://cyberleninka.ru/article/n/aktualnye-voprosy-fizicheskoy-zaschity-informatsii> (дата обращения: 06.06.2023).

16. Жарникова Ю. С. Угрозы информационной безопасности образовательного учреждения / Ю. С. Жарникова. — Текст: непосредственный // Молодой ученый. — 2017. — № 11.2 (145.2). — С. 60-63. — URL: <https://moluch.ru/archive/145/40613/> (дата обращения: 30.05.2023).

17. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006. Взамен ГОСТ Р 50922-96. Введ. 2008-02-01 // СПС «КонсультантПлюс».

18. Информационная безопасность образовательных учреждений. — URL: <https://searchinform.ru/resheniya/otraslevyeresheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij/> (дата обращения 13.03.2023).

19. Исаев А. Н. Противодействие утечке информации по техническим каналам в системах связи в ГБПОУ «ЮУГК» / А. Н. Исаев, М. С. Подин. — Текст: непосредственный // МОЛОДЕЖНАЯ ПОЛИТИКА И СОЦИАЛЬНАЯ МИССИЯ ОБРАЗОВАНИЯ В ЭПОХУ ГЛОБАЛИЗАЦИИ И ЦИФРОВИЗАЦИИ: материалы Международной научно-практической конференции. — Челябинск: «ЗАО Библиотека А. Миллера», 2022. — С. 468-471.

20. Ищейнов В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие / В. Я. Ищейнов, М. В. Мещатунян. — 2-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 216 с.

21. Конкин Ю. В. Основы информационной безопасности: учебное пособие / Ю. В. Конкин, Ю. М. Кузьмин, В. Н. Пржегорлинский. — Рязань: РГРТУ, 2021. — 96 с.

22. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.

23. Маслова М.А. Анализ и определение рисков информационной безопасности / М. А. Маслова // Научный результат. Информационные технологии. — 2019. — № 1. — С. 31-37.

24. Метод оценки экономической эффективности подразделения по защите информации. – URL: <https://lib.itsec.ru/articles2/Oborandteh/metod-ocenki-ekonomicheskoeffektivnosti-podrazdeleniya-po-zashite-informacii> (дата обращения 23.11.2022).

25. Методы обеспечения информационной безопасности. – URL: https://libraryno.ru/9-5-1-metody-obespecheniya-informacionnoy-bezopasnosti-2015_informatika/ (дата обращения: 16.04.2023).

26. Методы организации защиты информации: учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55 / Ю. Ю. Громов и др. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2013. – 80 с.

27. Милютина О.В. Особенности защиты информации в образовательном учреждении [Текст] / О.В. Милютина. – URL: http://www.fcoit.ru/internet_conference/information_security_training_process/features_information_security_in_an_educational_institution.php (дата обращения: 15.04.2023).

28. Модели в информационной безопасности. – URL: <https://habr.com/ru/articles/467269/> (дата обращения: 16.05.2023).

29. Моргунов А. В. Информационная безопасность: учебно-методическое пособие / А. В. Моргунов. — Новосибирск: НГТУ, 2019. — 83 с.

30. Обеспечение информационной безопасности организации. – URL: <https://iccwbo.ru/blog/2016/obespechenieinformatsionnoy-bezopasnosti/> (дата обращения 13.03.2023).

31. Официальный сайт ГБПОУ «Южно-Уральский государственный колледж». – URL: www.ecol.edu.ru (дата обращения: 20.10.2022).

32. Планирование затрат на информационную безопасность – URL: www.anti-malware.ru (дата обращения: 02.05.2023).

33. Поздняк И. С. Управление информационной безопасностью: методические указания / И. С. Поздняк, И. С. Макаров. — Самара: ПГУТИ, 2019. — 43 с.

34. Постановление Правительства Российской Федерации № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». — URL: <http://base.garant.ru/70252506/> (дата обращения 23.11.2022).

35. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты». — URL: <https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskiematerialy/471-informatsionnoe-pismo-fstek-rossii-2> (дата обращения 23.11.2022).

36. Риск-модели информационной безопасности: учебное пособие / А. А. Корниенко, С. В. Корниенко, А. П. Глухов, М. Л. Глухарев. — Санкт-Петербург: ПГУПС, 2021. — 79 с.

37. Санжаров А.С. Методы оценки исследований информационной безопасности и компьютерных угроз / А.С. Санжаров, Ж.Т. Баранова // Известия Кыргызского государственного технического университета им. И.Раззакова. — 2018. — № 46. — С. 296- 301.

38. Стандарты информационной безопасности. — URL: <https://tvoi.biz/biznes/informatsionnaya-bezopasnost/prakticheskaya-polza-standartov-info.html> (дата обращения: 20.04.2023).

39. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс] — URL: <https://www.garant.ru/products/ipo/prime/doc/71456224/> (дата обращения: 16.05.2022).

40. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [Текст]. — Москва: Легион, 2022. — 144 с.

41. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Текст]. – Москва: Омега-Л, 2022. – 96 с.

42. Черяева О. А. Обеспечение информационной безопасности образовательной организации / О. А. Черяева // Проблемы современных интеграционных процессов. Пути реализации инновационных решений: сборник статей по итогам Всероссийской научно-практической конференции, Стерлитамак, 06 ноября 2020 года. – Стерлитамак: Общество с ограниченной ответственностью «Агентство международных исследований», 2020. – С. 35-37.

43. Шворнев М. С. Изучение актуальных вопросов физической защиты информации / М. С. Шворнев, Е. Д. Парфирьев // Инновации. Наука. Образование. – 2020. – № 24. – С. 1640-1644.

44. Шестерин А. А. Совершенствование системы обеспечения информационной безопасности как составляющей экономической безопасности кредитных организаций: диссертация ... кандидата экономических наук: 08.00.05 / Шестерин Александр Александрович; [Место защиты: Моск. акад. экономики и права]. – Москва, 2010. – 153 с.: ил. РГБ ОД, 61 10-8/2454 <http://www.dslib.net/economika-xoziajstva/sovershenstvovanie-sistemy-obespechenija-informacionnoj-bezopasnosti-kak.html>_(дата обращения: 16.04.2023).

45. Щеглов А.Ю. Математические модели и методы формального проектирования системы защиты информационных систем / А. Ю. Щеглов, К. А. Щеглов: учеб. пособие. СПб.: Университет ИТМО, 2015, 93 с.