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 методов обеспечения информационной безопасности в профессиональной образовательной организации

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

Проверка на объем заимствований:
70,52 % авторского текста

Работа рекомендована к защите
«22» 12 2025 г.
Зав. кафедрой АТИТ и МОТД
_____ Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Рыбакова Юлия Максимовна

Научный руководитель:
д.п.н., профессор
Уварина Наталья Викторовна

Челябинск
2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Информационные технологии проникают во все сферы нашей жизни, и одной из наиболее важных является сфера образования. Современные образовательные учреждения активно используют информационные системы и сети для обеспечения эффективного обучения и работы со студентами. Однако, с увеличением количества и сложности информационных технологий, возникают и все новые угрозы информационной безопасности.

Существуют угрозы информационной безопасности, которые могут привести к серьезным последствиям для образовательных учреждений и их участников. Это может быть утечка конфиденциальной информации, взлом сетевой инфраструктуры, распространение вредоносных программ и многое другое. При этом, сфера профессионального образования, на которую направлена данная диссертация, имеет свои особенности и требования к информационной безопасности. Такая ситуация обусловлена несколькими основными факторами.

Во-первых, профессиональное образование находится на перепутье развития. С ростом информационных технологий и цифровизации процессов обучения и работы, возникают новые требования к безопасности информации. Профессиональные образовательные организации должны эффективно защищать свою информацию и информацию своих студентов, чтобы не допустить ее утечки и не создать угрозы для их дальнейшей карьеры.

Во-вторых, существующие методы обеспечения информационной безопасности не всегда эффективны и не отвечают особенностям профессионального образования. Они могут быть устаревшими, не учитывать специфику образовательного процесса или не применяться достаточно широко. Поэтому, требуется разработка новых методов, которые будут адаптированы к особенностям профессионального

образования и учитывать современные угрозы информационной безопасности.

В-третьих, ситуация с информационной безопасностью постоянно меняется и развивается. Новые угрозы и методы атак появляются с каждым годом, поэтому необходимо постоянное совершенствование методов обеспечения информационной безопасности в профессиональных образовательных организациях. Только так они смогут быть более эффективными и противостоять постоянно меняющимся угрозам.

Но, что касаемо профессиональных образовательных организаций, расположенных в регионах, возникает очевидное **противоречие:** стремление администрации образовательной организации к совершенствованию обеспечения информационной безопасности в профессиональной образовательной организации и ограничение ресурсами, такими как: бюджет, персонал, техническое оснащение.

Таким образом, исследование может найти наилучшие методы обеспечения информационной безопасности, но их внедрение может оказаться слишком затратным или непрактичным для данной организации. Поэтому следует искать более гибкие методы решения имеющейся проблемы, что приводит к тому, что в этой связи становится **актуальной тема исследования:** «Совершенствование методов обеспечения информационной безопасности в профессиональной образовательной организации».

Цель исследования: разработать и апробировать комплекс мероприятий по совершенствованию методов обеспечения информационной безопасности в профессиональной образовательной организации.

Объект исследования: система обеспечения информационной безопасности в профессиональном образовании.

Предмет исследования: комплекс мероприятий по совершенствованию методов обеспечения информационной безопасности в профессиональной образовательной организации.

Гипотеза исследования: если внедрить комплекс мероприятий, включающий: разграничение прав доступа в локальной сети и на обучающих платформах, установку и настройку средств контентной фильтрации в сети Интернет, организацию средств защиты от несанкционированного проникновения в организацию, разработку регламента организации по обслуживанию парка вычислительной техники и его соблюдение, организацию системы обнаружения уязвимостей в сети, то система информационной безопасности профессиональной образовательной организации будет устойчивее к внешним и внутренним негативным воздействиям.

В соответствии с объектом, предметом и целью исследования были поставлены следующие **задачи:**

1. Раскрыть основные понятия, принципы и уровни информационной безопасности в профессиональной образовательной организации, дать оценку фактора интегральной безопасности.

2. Определить основные виды угроз и причины уязвимостей информационной безопасности в образовательной организации.

3. Установить методы защиты информации в профессиональной образовательной организации в соответствии с наиболее вероятными угрозами и уязвимостями в системе.

4. Проанализировать единое информационное пространство организации профессионального образования, определить исходный уровень защищенности информационных систем персональных данных.

5. Разработать комплекс мероприятий по совершенствованию методов обеспечения информационной безопасности в ГБПОУ «Южно-Уральский государственный колледж» Кыштымского филиала.

6. Провести контрольную оценку эффективности комплекса мероприятий по совершенствованию методов обеспечения информационной безопасности в профессиональной образовательной организации.

Методологической основой исследования являются фундаментальные работы в области:

– педагогических и психологических наук (Ю.К. Бабанский, Л.С. Выготский, И.Я. Лернер, А.С. Макаренко, С.Л. Соловейчик, К.Д. Ушинский и др.);

– организации непрерывного педагогического образования, профессиональной подготовки и переподготовки педагогических работников (Г.А. Бордовский, Д.В. Квеквескири, Г.А. Минаев, С. Н. Никифоров, В.А. Сластенин и др.);

– применения педагогического сопровождения и консультирования в психологических и педагогических сферах (О.С. Газман, Н.Ф. Голованова, В.А. Калягин, Е.С. Маренцева, Т.С. Овчинникова, О.С. Орлов и др.);

– цифровой трансформации образования (Д.В. Буданцев, А.А. Евкова, В.В. Ерохин, Е.В. Карташова, А.В. Морозов, Д.А. Погонышева, Б.Е. Стариченко, И.Г. Степченко, А.Ю. Уваров и д.р.);

– применения компетентностного подхода в организации учебного процесса (А.А. Вербицкий, И.А. Зимняя, О.Г. Ларионова, А.П. Огурцов, В.В. Платонов, С.Л. Троянская, А.В. Хуторской и др.);

– применения системного подхода в педагогике (А.П. Беляев, Т.А. Ильина, В.В. Краевский, Н.В. Кузьмина, И.Ф. Скляров и др.);

– создания и применения отечественных компьютерных обучающих технологий в образовании (В.М. Вымятин, В.П. Демкин, Д.А. Короченцев, О.И. Мезенцева, Е. А. Ревякина, А.Л. Ундозерова, и др.);

– нормативно-правового сопровождения безопасности информации (А.В. Александрова, И.С. Бедеров, Г.О. Крылов, и др.);

– защиты информации в педагогическом контексте (Н. Б. Трофимова, Е. М. Беспаленко, А.Р. Шарафутдинова, В.С. Пядышева и др.);

– применения аппаратных и программных средств поиска уязвимостей при эксплуатации информационных систем (А.С. Алешкин, С.А. Лесько, Д. О. Жуков, А.В. Ксендзов, Д.В. Маршаков, и др.);

– защиты информации при помощи различных категорий средств безопасности (Р.Р. Лаляутдинов, Н.В. Гришина, А.Ю. и др.);

– проблематики обучения персонала и развития навыков в сфере информационной безопасности (И.В. Капгер, А.С. Шабуров, Е.Н. Каширская, М.А. Макаров, И.В. Мандрица, В.И. Петренко, О.В. Мандрица и др.);

– практических подходов к системе информационной безопасности (Е.К. Баранова, А.В. Бабаш, Е.В. Вострецова, Е.О. Карпухин, Ю.В. Конкин, Ю. М. Кузьмин, Ю.М. Краковский, В.И. Ярочкин и др.).

Научная новизна заключается в обосновании возможности внесения необходимых изменений в текущую систему информационной безопасности профессиональной образовательной организации путем внедрения комплекса мероприятий в соответствии с требованиями действующего законодательства и современных технологий в области защиты данных.

Теоретическая значимость исследования определяется расширением научных знаний в области методов обеспечения информационной безопасности, таких как: теоретические, организационные, правовые, инженерно-технические и сервисы сетевой безопасности профессиональных образовательных организаций.

Практическая значимость диссертации определяется тем, что разработанный комплекс мер может использоваться для повышения уровня информационной безопасности в других профессиональных образовательных организациях.

Для решения поставленных задач и проверки гипотезы используются следующие **методы исследования:** анализ теоретической и методической литературы, нормативных документов и материалов, регулирующих процесс обеспечения защиты персональных данных; изучение методических разработок, монографий и технической литературы по вопросу обеспечения информационной безопасности организаций на различных уровнях защиты; обобщение, систематизация и анализ собранных данных; наблюдение и оценка системы безопасности; проектирование комплекса мер на основании проделанной работы.

База исследования: Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный колледж», г. Кыштым.

Основные этапы исследования.

На первом этапе формулировались тема исследования и план диссертации. Выполнялся сбор информации по вопросу исследования из различных источников информации, осуществлялась формулировка гипотезы, постановка цели и задач.

На втором этапе проводилась комплексная работа, включающая в себя: изучение научной и технической литературы, отбор необходимых источников информации, анализ современных методов обеспечения информационной безопасности профессиональной образовательной организации на различных уровнях защиты, публикация научных статей по теме исследования.

На третьем этапе осуществлялся анализ текущего состояния системы безопасности базы исследования, обработка данных, разработка комплекса мероприятий по совершенствованию методов обеспечения информационной безопасности в профессиональной образовательной организации, а также оформление материалов исследования, формулировка выводов.

Апробация результатов исследования осуществлялась путем публикации научных статей:

1. Рыбакова Ю.М. Развитие стратегии обеспечения информационной безопасности в педагогике: вызовы и перспективы // Студенческий вестник [Текст]: научный журнал / под. ред. Н.П. Ходаковой – Москва: изд-во «Интернаука», 2024. – Выпуск 2 (288), часть 2. – 33с.

2. Рыбакова Ю.М. Современные методы обеспечения информационной безопасности в колледже // Студенческий вестник [Текст]: научный журнал / под. ред. Н.П. Ходаковой – Москва: изд-во «Интернаука», 2024. – Выпуск 7 (293), часть 4 – 12с.

3. Рыбакова Ю.М. Анализ уязвимостей сетевой инфраструктуры колледжа и методы их устранения // Студенческий вестник [Текст]: научный журнал / под. ред. Н.П. Ходаковой – Москва: изд-во «Интернаука», 2024. – Выпуск 14 (300), часть 1 – 37с.

4. Рыбакова Ю.М. Информационная культура педагога, как аспект информационной безопасности профессиональной образовательной организации // Профессиональное образование: методология, технологии, практика [Текст]: сборник научных статей / под. ред. Е.А. Гнатышиной. – Челябинск: изд-во «ЗАО Библиотека А. Миллера», 2024. – Выпуск 17. – 108с.

5. Рыбакова Ю.М. Комплекс мероприятий по совершенствованию методов обеспечения информационной безопасности в колледже // Студенческий вестник [Текст]: научный журнал / под. ред. Н.П. Ходаковой – Москва: изд-во «Интернаука», 2024. – Выпуск 43 (329).

Личное участие соискателя состоит в анализе системы информационной безопасности организации, выявлении рисков и угроз в системе, а также разработке комплекса мероприятий для совершенствования уже имеющихся методов обеспечения информационной безопасности ГБПОУ «Южно-Уральский государственный колледж» Кыштымского филиала.

Структура диссертации: введение, две главы, выводы по главам, заключение, приложение, список использованной литературы, включающего в себя 60 источников.

ГЛАВА 1. ТЕОРЕТИКО-МЕТОДИЧЕСКИЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1 Основные понятия, принципы и уровни информационной безопасности в профессиональной образовательной организации

Термин «информационная безопасность» в различных областях человеческой деятельности может обладать различными значениями. Рассмотрим подробнее некоторые определения из разных источников информации.

Доктрина информационной безопасности Российской Федерации. Термин «информационная безопасность» определяется в ней, как состояние защищенности субъектов и объектов от различных информационных угроз, обозначенных целостностью согласованных национальных потребностей [13].

ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Термин «информационная безопасность» определяется в нем, как состояние защищенности потребностей организации в условиях опасности в информационной сфере [10].

Основы информационной безопасности: учебное пособие для студентов вузов (Е.В. Вострецова) [7]. Термин «информационная безопасность» определяется в нем, как состояние защищенности информационной среды от различных информационных угроз, способных причинить вред национальным интересам.

Таким образом, основываясь на приведенных выше понятиях, можно выделить следующие аспекты, с учетом специфики исследуемой области, что информационная безопасность – это состояние защищенности информационного пространства учебной организации, а также защита объектов (обучающихся) от запрещенной законом информации.

Все вышеприведенные понятия связаны между собой несколькими терминами и одним из таких более значимых является «защита».

Согласно ГОСТ Р 50922-2006, под защитой информации понимается, следующее [9]: защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

То есть, информационная безопасность является одним из главных факторов интегральной безопасности. Яркой иллюстрацией данного фактора является статистика преступлений [4,48], связанных с информацией, например, преступления, совершенные с использованием информационно-телекоммуникационных технологий (график 1) и принятых мер законодательством, по отношению к данной проблеме.

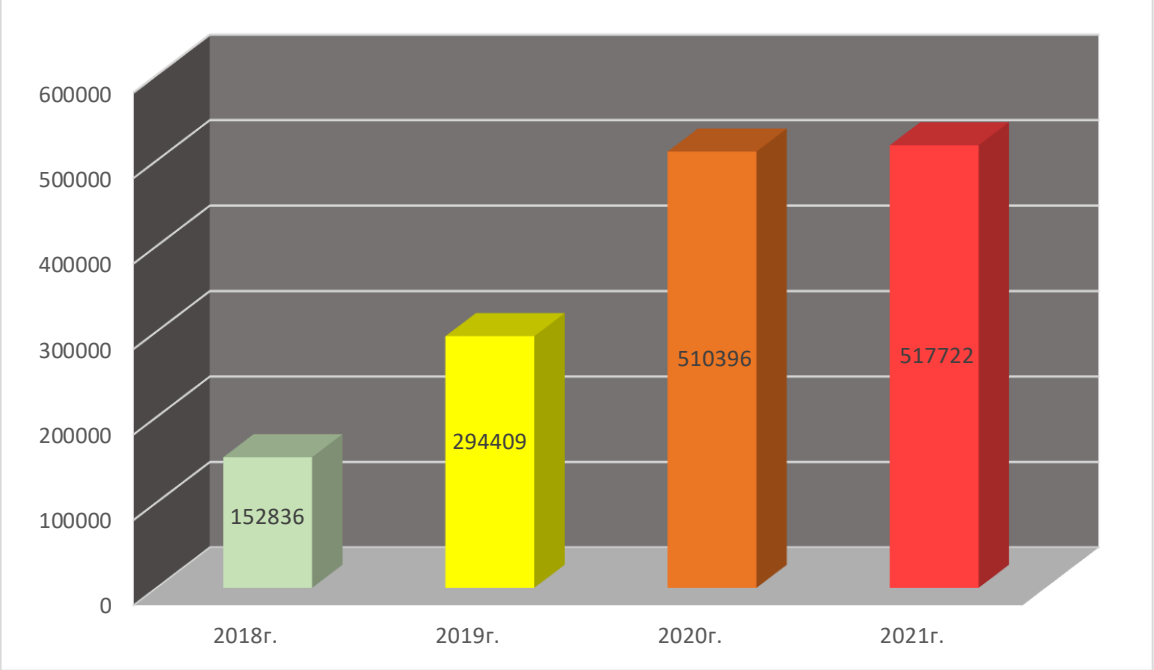

График 1 – Статистика количества преступлений, совершенных с использованием информационно-телекоммуникационных технологий

Основываясь на данных представленных министерством внутренних дел Российской Федерации (график 1), можно наблюдать резкий скачок зафиксированных преступлений с 2019-2020 гг., что объясняется введением режима самоизоляции и массовым переходом бизнес-процессов и торговли в сферу онлайн, откуда и умножилась киберпреступность [50]. Но даже со снятия режима самоизоляции, данный показатель не падает, а только растет. Данный факт связан с неотъемлемой частью нашей жизни – технологический прогресс, когда информационные технологии составляют базу нашей жизнедеятельности во всех сферах, из-за чего доля преступлений в сфере IT приближается к половине от общего числа преступлений в целом [18].

Так как новые технологии несут в себе новые угрозы, органы власти так же работают в усиленном режиме, только за 8 месяцев 2021г. были приняты и внесены корректировки в огромное количество нормативно-правовых актов касающихся следующих направлений [37,46]:

- цифровые экономические отношения,
- национальная безопасность,
- импортозамещение,
- защита информации,
- биометрия,
- персональные данные,
- средства криптографической защиты информации,
- аттестация объектов информатизации и т.д.

Вследствие чего нововведений и изменений стало так много, что проконтролировать каждого просто стало невозможным. Поэтому президент РФ издал Указ от 01.05.2022 г. № 250, направленный на возложение персональной ответственности на первых лиц ключевых компаний России за информационную безопасность. К таким компаниям относятся некоторые органы власти, предприятия с государственным

участием, субъекты критической информационной инфраструктуры, стратегические и системообразующие организации [56].

И все же независимо от того государственная ли эта организация или частная компания в любом случае данные предприятия должны качественно и эффективно обеспечивать свою информационную безопасность. Поэтому зачастую цели (они же принципы) информационной безопасности формируют исходя из поставленных задач перед системой (рисунок 1) [3,45]. Они должны безоговорочно включать в себя три основных положения, защищаемые информационной безопасностью, в совокупности известной как триада CIA [11]:

– конфиденциальность (предотвращение огласки какой-либо информации);

– целостность (отсутствие искажений в информации);

– доступность (гарант существования информации в ее исходном виде).

Рисунок 1 – Цели защиты информации

Итак, проблему обеспечения информационной безопасности, следует рассматривать в обязательном порядке при комплексном подходе, который в совокупности и будет обеспечивать защиту информации и информационных систем от негативных последствий [44].

Существует три уровня формирования режима информационной безопасности [6]:

– законодательно-правовой,

– административный,

– программно-технический.

Законодательно-правовой уровень. Данный уровень включает в себя совокупность законодательных актов, стандартов, спецификаций и различную правовую информацию, устанавливающую правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус [26]. Примером такой основополагающей документации является:

– доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895;

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»;

– указ Президента Российской Федерации № 351 от 17 марта 2008 года «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Административный уровень. К данному уровню относят действия общего характера, предпринимаемые руководством учреждения. Главная цель состоит в том, чтобы сформировать комплекс работ в области информационной безопасности и гарантировать их реализацию, выделяя необходимые ресурсы и контролируя состояние дел [1]. Такой документацией может выступать:

– политика безопасности организации (подход к защите информационных ресурсов);

– распоряжение о назначении ответственных лиц по обеспечению безопасности обработки персональных данных [36];

– распоряжение о правилах хранения электронных и бумажных носителей ценных сведений, определения порядка допуска к ним;

– должностные инструкции специалистов, обеспечивающих функционирование информационных систем.

Программно-технический уровень. Обеспечивает контроль над информационными системами. Подразделяется на три подуровня [15]:

– физический (ограничение доступа к информационной системе, посредством реализации средств безопасности: охранные и охранно-пожарные системы, видеонаблюдение, естественные и искусственные барьеры, особые конструкции сейфов и хранилищ) [55];

– технический (ограничение доступа к аппаратным средствам обработки информации, посредством реализации средств: система оповещения о попытках вторжения, ключевой доступ и т.д.) [29];

– программный (ограничение доступа к системе обработки информации, посредством реализации средств: антивирусное программное обеспечение, средства аутенфикации, межсетевое экранирование, криптография и т.д.).

Таким образом, освоение ключевых понятий позволяет осознать риски, связанные с использованием информационных технологий, а также возможность применить соответствующие стратегии для защиты данных. Также принципы информационной безопасности помогают сформировать правильное поведение в цифровом пространстве, в то время как уровни безопасности дают возможность структурировать подходы к защищенности информации на разных этапах деятельности образовательной организации.

1.2 Основные виды угроз и причины уязвимостей информационной безопасности в образовательной организации

Согласно ГОСТ Р 53114-2008 под термином «угроза информационной безопасности» принято понимать совокупность различных событий, осуществление которых может привести к нанесению ущерба системе безопасности организации [10].

В настоящее время насчитывается более 120 положений и модификаций угроз системы безопасности, которые проявляются за счет факторов уязвимости [2,43]. Основополагающими факторами являются:

- некорректная настройка оборудования;
- использование нелицензированного программного обеспечения;
- не компетентность персонала.

Классифицируют уязвимости, в большинстве случаев, по следующим классам:

– объективные (рисунок 2) – полноценная защита от данных уязвимостей невозможна, но минимизация риска реализуется за счет инженерно-технических приемов [14];

– случайные (рисунок 3) – невозможно предусмотреть, но важно быть готовым к их оперативному устранению (устранить такие неполадки можно с помощью проведения инженерно-технического разбирательства и ответного удара, нанесенного угрозе информационной безопасности) [19,35];

– субъективные (рисунок 4) - устранение уязвимостей данного класса осуществляется при помощи различных приемов с использованием специализированной аппаратуры и ПО [24].

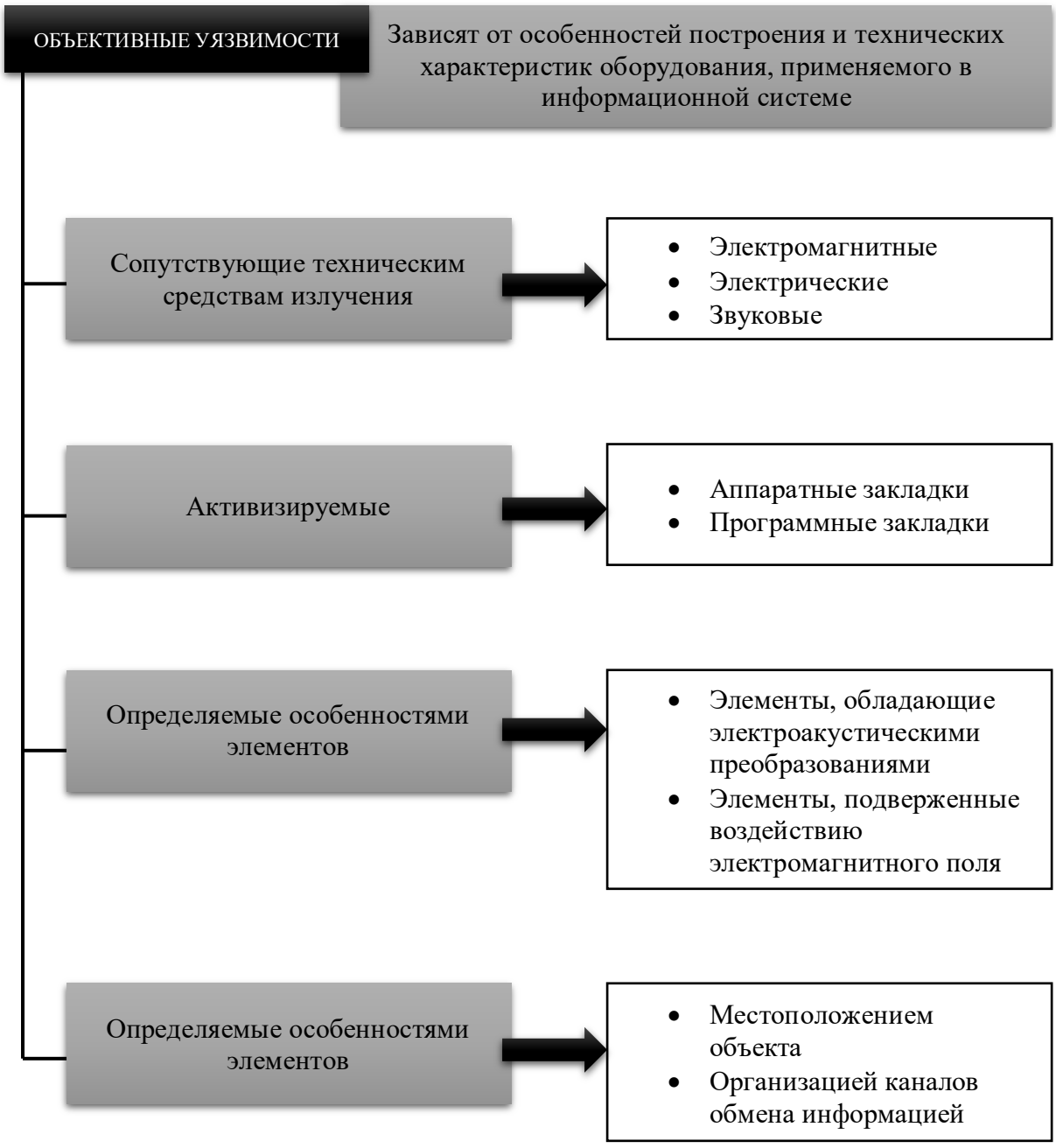

Рисунок 2 – Объективные уязвимости

Рисунок 3 – Случайные уязвимости

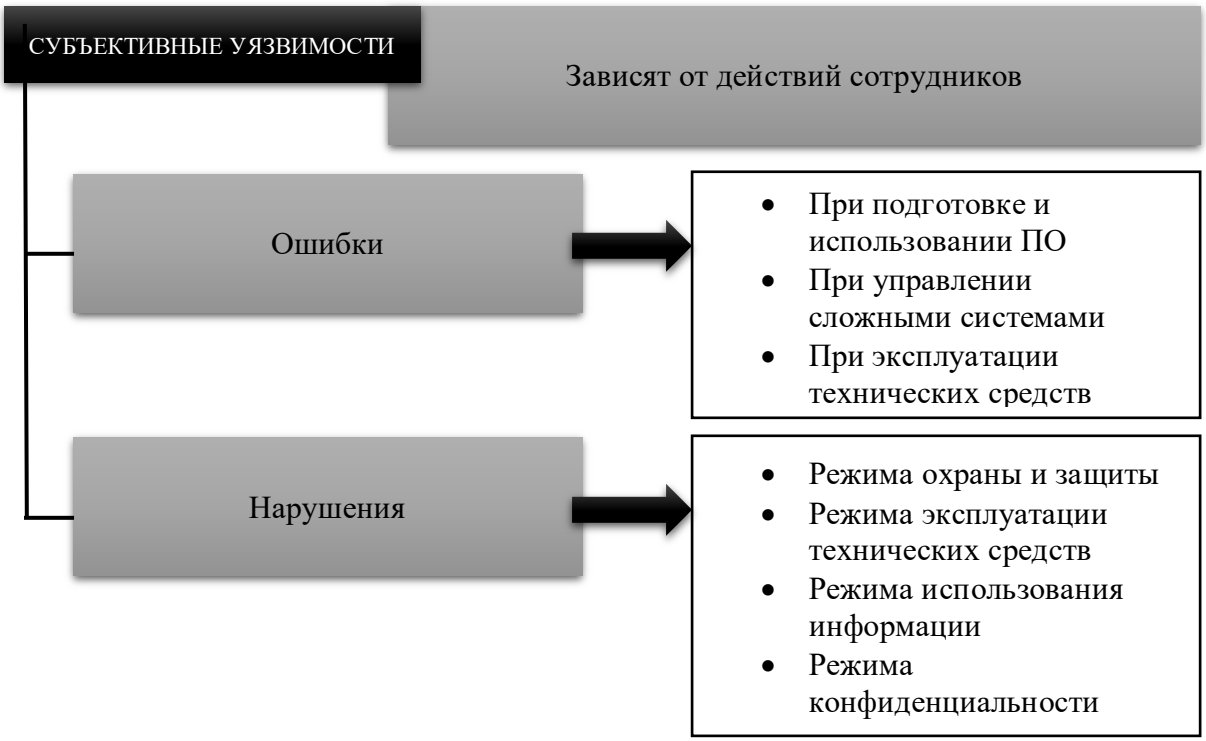

Рисунок 4 – Субъективные уязвимости

В свою же очередь сами угрозы классифицируются по определенному ряду признаков – таблица 1 [5,34]. Каждый из признаков классификации отображает аспект из предъявляемых требований к системе защиты. Необходимость классификации угроз информационной безопасности обусловлена архитектурой актуальных и инновационных технических средств обработки информации [28,54].

Таблица 1 – Классификация угроз информационной безопасности

№ п/п	Признак	Тип угрозы	Характеристика
1	По природе возникновения	Естественные	Направлены на автоматизированную систему; источники угроз: объективные физические процессы и стихийные бедствия (землетрясения, наводнения, лесные пожары и т.д.)
		Искусственные	Направлены на автоматизированную систему; источник угроз: деятельность человека
2	По степени преднамеренности проявления	Случайные	Проявляются за счет ошибок и халатного отношения персонала организации к своей деятельности (повреждение оборудования, ошибочный ввод данных и т.д.)
		Преднамеренного действия	Организованы злоумышленниками с целью хищения информации и нарушения функционирования организации
3	По непосредственному источнику угроз	Источник – природная среда	Источник выступает в качестве таких явлений, как: стихийные бедствия, магнитные бури и т.д.
		Источник – человек	Осуществляется за счет: внедрения в персонал «агента»; вербовки сотрудников внутри организации; неправомерного копирования и распространения коммерческой информации сотрудниками
		Источник – санкционированные программные средства	Осуществляется за счет некомпетентного использования технологических программ и нарушения работы операционной системы

Продолжение таблицы 1

		Источник – несанкционированные программные средства	Осуществляется за счет установки нелегального программного обеспечения и заражения системы различными типами вирусов
4	По положению источник угроз	Источник вне контролируемой зоны	Направлены на перехват передаваемых данных, посредством: фиксирования информации фотооборудованием; наводки активным излучением на линии связи, линии электроснабжения и отопления
		Источник в пределах контролируемой зоны	Организуется за счет кражи производственного мусора (документы из шредера, распечатки, заметки), отключения электроснабжения и водоснабжения, прослушки каналов связи
		Источник с доступом к периферии	Все действия, которые можно осуществить при помощи терминала внутренней сети
		Источник внутри автоматизированной системы	Организуется за счет проектирования топологии системы и технологии обработки данных, разработки прикладных программ, которые представляют опасность для работоспособности системы и информационной безопасности
5	По степени зависимости от активности системы	Проявляются независимо от активности системы	Осуществляется за счет обнаружения ключа шифрования систем и кражи носителей данных
		Проявляются только в процессе обработки информации	Организуется за счет заражения и распространения вирусов в системе
6	По степени воздействия на систему	Пассивные	Не несут за собой изменений в системе, например, копирование секретных данных
		Активные	Изменяют структуру и содержание автоматизированной системы посредством включения несанкционированного оборудования и нелегального программного обеспечения, перенастройки системы безопасности и ее компонентов

Продолжение таблицы 1

7	По этапам доступа пользователей или программ к ресурсам системы	Проявляются на этапе доступа к ресурсам системы	Реализуется за счет несанкционированного доступа
		Проявляются после разрешения доступа к ресурсам системы	Реализуется за счет некорректного использования ресурсов системы
8	По способу доступа к ресурсам системы	Направлены на использование прямого стандартного пути доступа к ресурсам системы	Осуществляется за счет хищения паролей и других средств разграничения доступа, а также несанкционированное использование АРМ
		Направлены на использование скрытого нестандартного пути доступа к ресурсам системы	Осуществляется за счет доступа в систему в обход средств защиты информационной безопасности
9	По текущему месту расположения информации, хранимой и обрабатываемой в системе	Внешнее запоминающее устройство	Действия направлены на несанкционированное копирование и модификацию секретной информации
		Оперативная память	Действия направлены на извлечение остаточных данных, как защищаемой информации, так и данных по системе защиты
		Информация циркулирующая в линиях связи	Осуществляется за счет несанкционированного подключения к линиям телекоммуникации
		Информация отображаемая на терминале или печатаемой на принтере	Направлены на фиксирование информации на фото и видео съемке

Также, вне зависимости от конкретных видов угроз, АС удовлетворяет потребности эксплуатирующих ее лиц [23]. Соответственно можно выделить, также обобщенную классификацию значимых угроз:

– *угроза нарушения конфиденциальности* - возникает, когда данные становятся известными личности, не располагающей полномочиями [42];

– *угроза нарушения целостности* - возникает при несанкционированной модификации данных [53];

– *угроза нарушения доступности* - возникает, когда в результате преднамеренных действий, злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы.

Исходя из вышеизложенного, можно сказать, что в организациях существуют различные виды угроз информационной безопасности, которые негативно сказываются на защите данных. К основным угрозам относятся: кибератаки (фишинг, вирусы, вредоносное ПО), утечки данных, внутренние угрозы (действия недобросовестных сотрудников) и физические угрозы (потеря оборудования, стихийные бедствия). Причины уязвимостей могут варьироваться от недостаточной осведомленности пользователей о мерах безопасности и слабых паролей до устаревшего программного обеспечения, и отсутствия надлежащих политик защиты информации.

1.3 Методы защиты информации в профессиональной образовательной организации

После того, как были определены основные виды угроз и причины уязвимостей информационной безопасности, необходимо соответственно рассмотреть, как защитить информацию и минимизировать риск возникновения уязвимостей в системе. Методы защиты, в общем случае, всегда применяются в комплексе друг с другом [12]. Такими положениями являются:

- организационная защита,
- инженерно-техническая защита,
- аппаратные средства защиты,
- программные средства защиты.

Организационная защита. Представляет собой упорядочивание деятельности организации и коммуникации исполнителей на законодательном уровне.

Включает в себя:

– режим работы предприятия и его непосредственная охрана (например, задекларированное начало и окончание времени рабочего дня, пропускной пункт, пост охраны и т.д.) [25];

– работа с персоналом - осуществляется посредством подбора сотрудников и их обучения по работе с информационным банком;

– работа с документами - осуществляется полный перечень работ документооборота (обработка, хранение, утилизация и т.д.) [47];

– анализ внутренних и внешних угроз - выявляется конфиденциальная информация и осуществляется выработка мер по обеспечению ее защиты (политика безопасности) [33];

– проведение систематического контроля за работой сотрудников - осуществляется с целью выявления нарушений правил по работе с данными внутри организации и устранения найденных недочетов.

Инженерно-техническая защита. Подразумевает использование различных цифровых устройств и специализированного оборудования, входящих в состав единого информационного пространства организации и выполняющих, как самостоятельные, так и комплексные функции по обеспечению сохранности информационного фонда [16]. К таким средствам по защите периметра организации относятся:

– система охранной сигнализации - предназначена для оповещения в случае несанкционированного проникновения на защищаемый объект; в соответствии с ГОСТ Р 52435-2015 состоит из следующих компонентов: модули извещения (система датчиков: шум, температура, движение и т.д.), приемно-контрольный блок (прием и обработка показаний с датчиков), модули оповещения (извещение о состоянии системы), устройство управления сигнализацией (управление режимами работы охранной сигнализации) [38];

– система пожарной сигнализации - представляет собой комплекс технических средств (датчики дыма, тепловые извещатели, извещатели

пламени и т.д.) для обнаружения возгорания, сообщения о месте его возникновения и обработки сигнала [52];

– системы цифрового видеонаблюдения - осуществляют контроль по идентификации доступа к определенным объектам, посредством фиксации изображения;

– системы контроля и управления доступом - комплекс программно-аппаратных технических средств контроля и средств управления, имеющих целью ограничение и регистрацию входа-выхода объектов (человек, автомобиль) на определенной территории через «пункты взаимодействия»: входные группы, КПП; могут, как идентифицировать лицо, так и вести учет рабочего времени или расчет заработанной платы по отработанным сменам [49].

К методам и мероприятиям предотвращения утечки информации через технические каналы связи также можно отнести:

– использование экранирования линий связи и различного электротехнического оборудования с целью защиты от помех и электромагнитных излучений [32];

– установка на линиях связи высокочастотных фильтров, которые исключают (ослабляющий) шунтирующее действие шин подстанций и отпаек линии электропередачи на линейный тракт канала ВЧ-связи [51];

– построение экранированных помещений - согласно ГОСТ Р 51317.4.3-99, такое помещение необходимо для отделения внутренней электромагнитной обстановки от внешней в целях предотвращения ухудшения качества функционирования ТС при воздействии внешних полей и ослабления электромагнитных излучений от ТС во внешнее пространство;

– установка активных систем зашумления - необходимы для «глушения» несанкционированных систем связи (работают, создавая «шум» или дополнительные данные, которые затрудняют злоумышленникам анализ и извлечение полезной информации из сигнала);

– создание контролируемых зон - создаются с целью контроля доступа, а также осуществляемой работы в пределах защищаемой зоны (например, в лабораториях при работе с опасными возбудителями болезней) [60].

Аппаратные средства защиты информации. Предполагает использование любых устройств, которые встраиваются в информационные и телекоммуникационные системы, с целью блокировки доступа к защищаемой информации, в том числе и с помощью ее сокрытия [8]. Подробнее об основных аппаратных средствах защиты информации - таблица 2.

Таблица 2 – Характеристика основных аппаратных средств

№	Категория	Описание	Средство
1	Регистры для хранения реквизитов защиты	Могут хранить пароли, идентифицирующие коды, грифы и уровни секретности документов	USB-идентификатор, смарт-карта, электронный замок, USB-ключ
2	Идентификация характеристик человека	Определение доступа к защищаемой информации по заданным параметрам человека: лицо, голос, сетчатка глаза, отпечаток пальца/руки и т.д.	Биометрические сканеры
3	Прерывание передачи информации	Принудительное прерывание потока информации по линиям связи с целью проверки пакета адресата	Сетевые фильтры
4	Шифрование данных	Преобразование информации, делающее ее нечитаемой для посторонних	Ключ шифрования Ключ дешифрования
5	Бесперебойное питание	Обеспечивает аварийное питание нагрузки при отказе входного источника питания или сетевого питания	Источники бесперебойного питания, генераторы напряжения

Программные средства защиты информации. Представляет собой простое и комбинированное программное обеспечение, предназначенное для решения задач, связанных с обеспечением информационной безопасности. Включают себя: средства от НСД, CASE-системы, систему мониторинга сетей, анализаторы протоколов, антивирусные средства, межсетевые экраны, криптографические средства, системы резервного

копирования, системы аутентификации, инструментальные средства анализа систем защиты [40].

Средства защиты от несанкционированного доступа (НСД) - позволяют предотвратить попытки несанкционированного доступа, такие как неавторизованный физический доступ, доступ к файлам, хранящимся на АРМ, ликвидация конфиденциальных данных. Подробнее об основных средствах защиты от НСД - таблица 3 [22].

Таблица 3 – Характеристика основных средствах защиты от НСД

№ п/п	Категория	Краткая характеристика
1	Авторизация	Получение права доступа к чему-либо
2	Мандатное управление доступом	Разграничение доступа с фиксированным набором полномочий. Базирующиеся на назначении метки конфиденциальности для данных, содержащихся в объектах, и выдаче официальных разрешений лицам на обращение к информации такого уровня доступа
3	Избирательное управление доступом	Управление доступом субъектов к объектам на основе списков матрицы доступа
4	Управление доступом на основе ролей	Позволяет управлять доступом пользователей к информационным ресурсам организации, посредством ограничений возможностей по рабочей функции
5	Аудит	Специальная независимая экспертиза, основанная на проведении плановых, комплексных, внеочередных или тематических проверок

Системы анализа и моделирования информационных потоков - средства разработки программных и организационно-управляющих систем [17]. Такие системы обладают следующими возможностями:

– единый графический язык - позволяет всем участникам проекта участвовать в деятельности друг друга, отслеживать процесс разработки проекта [27];

– единая база данных проекта - обеспечивает всех участников проекта единым хранилищем данных, что позволяет получить своевременный доступ к любой информации на различных этапах разработки [21];

– поддержка коллективной разработки и управления проектом;

– макетирование - позволяет выстраивать структуру проекта, что предоставляет возможность своевременного отслеживания;

– генерации документации - автоматическая генерации документации по проекту, что позволяет экономить значительную долю времени на операции данного типа [41];

– автоматическая генерация объектного кода.

Системы мониторинга сетей – непрерывный процесс отслеживания сети на предмет отклонений в работе. Существует 2 протокола, позволяющих проводить такой анализ:

– SNMP - позволяет производить опрос ПК и затребовать у системы различные параметры [31];

– ICMP - позволяет узнать, отвечает ли система (может использоваться для функций: ping, FPS).

Анализаторы сетевых протоколов. Осуществляет процесс анализа протоколов, который включает в себя захват циркулирующих в сети пакетов, реализующих какой-либо сетевой протокол, а также изучение содержимого этих пакетов. Общая схема работы анализатора сетевых протоколов представлена на рисунке 5 [57,59].

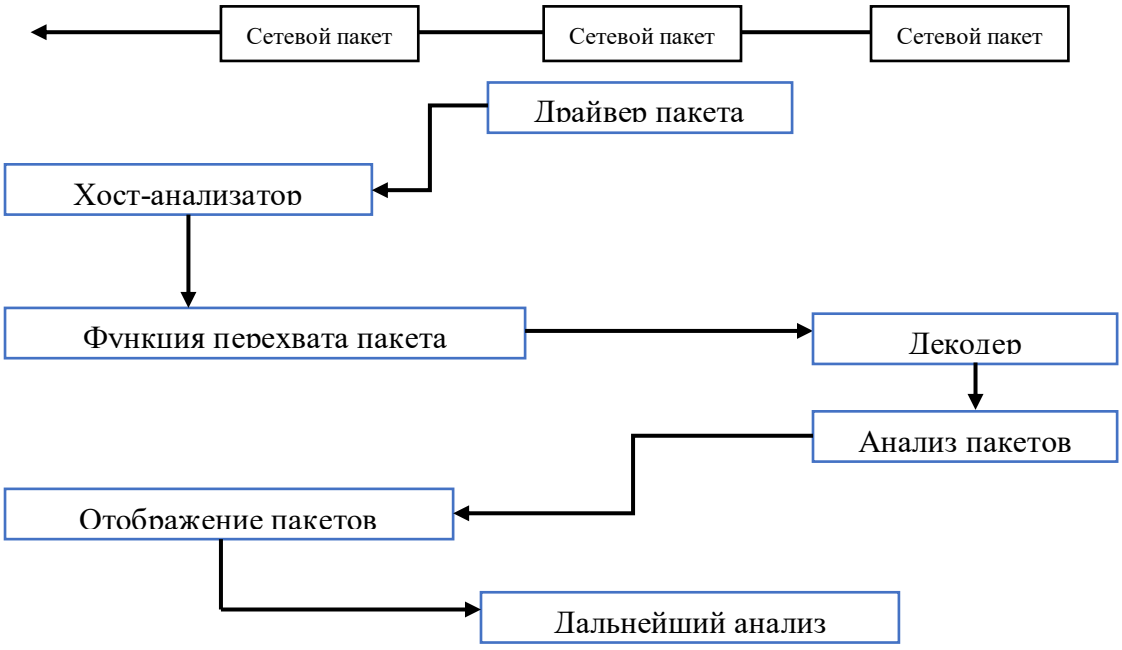

Рисунок 5 – Общая схема работы анализатора сетевых протоколов

Антивирусные средства - программное обеспечение, которое противодействует компьютерным вирусам [20]. По механизму защиты они подразделяются на:

– не сигнатурные - производят анализ кода и поведение всех новых установленных приложений на ПК, чтобы найти признаки, характерные для вирусов;

– сигнатурные - осуществляют поиск и сравнение вирусов с имеющейся базой данных;

– сторожа - активны непрерывно в фоновом режиме, что позволяет отслеживать действующие процессы;

– полифаги - организуют скан ОС и файлов, которые запускаются в настоящий момент времени;

– ревизоры - запоминают исходное состояние системы и контролируют изменения в ней.

Криптографические средства – отвечают за шифрование и дешифрование данных, а также проверку того, что вносились ли в них изменения [30].

Системы резервного копирования – выполняют функцию создания копий данных в системе, которые предназначены для их восстановления в случаи повреждения [58].

Системы аутентификации – отвечают за проверку подлинности предоставляемых данных, таких как логин и пароль [39].

Итак, организации применяют различные методы защиты информации. Эти методы могут включать в себя технологии шифрования, системы контроля доступа, регулярные аудиты безопасности, обучение сотрудников и разработку политик информационной безопасности. Эффективная защита информации требует комплексного подхода и постоянного обновления мер, чтобы адаптироваться к новым угрозам и рискам в цифровом пространстве.

Выводы по главе 1

В первой главе магистерской диссертации мы рассмотрели теоретико-методические основы обеспечения информационной безопасности в профессиональной образовательной организации.

В первом параграфе, определили значения терминов: информационная безопасность и защита информации. Основываясь на данных представленных министерством внутренних дел Российской Федерации, проанализировали статистику преступлений, совершенных с использованием информационно-телекоммуникационных технологий, в ходе которой проследили за резким скачком преступлений начиная с 2019г. Рассмотрели триаду CIA, которая включает в себя такие положения, как: конфиденциальность, целостность и доступность. Определили цели защиты информации, которые направлены на предотвращение утечки информации, воспрещение несанкционированного доступа, сохранение достоверности данных, соблюдение конфиденциальности и авторских прав. Также подробно рассмотрели уровни формирования режима информационной безопасности: законодательно-правовой, административный и программно-технический.

Во втором параграфе, определили значение термина: угроза информационной безопасности, а также самые распространенные факторы уязвимости систем безопасности, которыми являются: некорректная настройка оборудования, использование нелицензированного ПО и не компетентность персонала. Рассмотрели классификацию уязвимостей в системе, которые в свою очередь, зависят от особенностей построения и технических характеристик используемого оборудования, особенностей окружающей среды и непредвиденных обстоятельств, действий сотрудников. Определили ряд признаков угроз безопасности, где каждый из признаков классификации отображает аспект из предъявляемых требований к системе защиты.

В третьем параграфе, раскрыли вопрос «как защитить информацию и минимизировать риск возникновения уязвимостей в системе», который рассматривался на разных уровнях защиты: организационный, инженерно-технический, аппаратный и программный. Каждый уровень включал в себя свои методы и средства:

– организационный – режим работы предприятия и его непосредственная охрана, подбор персонала и его обучение по работе с ИС, работа с документацией, анализ внутренних и внешних угроз;

– инженерно-технический – применение средств защиты периметра (система охранной и пожарной сигнализации, видеонаблюдения, контроля и управления доступом), использование экранирования линий связи, установка высокочастотных фильтров и т.д.;

– аппаратный - использование систем регистров, идентификации и шифрования;

– программный – использование средств от НСД, CASE-системы, систему мониторинга сетей, анализаторы протоколов, антивирусные средства, межсетевые экраны, криптографические средства, системы резервного копирования, системы аутентификации, инструментальные средства анализа систем защиты.

ГЛАВА 2. ЭКСПЕРИМЕНТАЛЬНАЯ РАБОТА ПО АПРОБАЦИИ КОМПЛЕКСА МЕР ПО СОВЕРШЕНСТВОВАНИЮ МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1 Анализ единого информационного пространства организации профессионального образования и определение исходного уровня защищенности информационных систем персональных данных

Базой исследования стал ГБПОУ «Южно-Уральский государственный колледж» Кыштымского филиала, располагающийся по адресу: Челябинская область, г.Кыштым, улица Ленина, здание 13 – рисунок 6. Организационная структура колледжа, с функциональным назначением ролей в ней, представлена на рисунке 7.

Рисунок 6 – Общая схема расположения корпусов колледжа

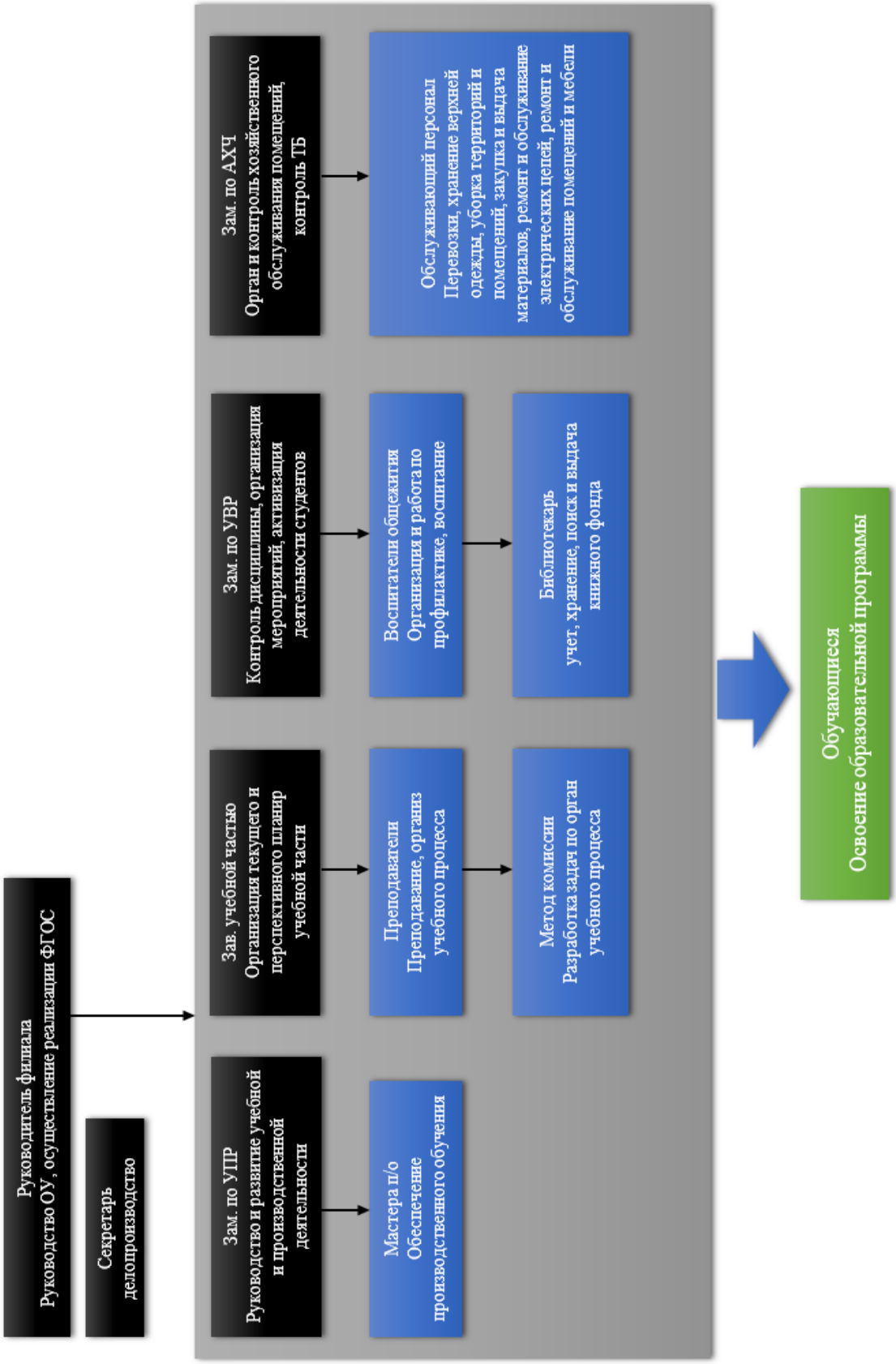

Рисунок 7 – Организационная структура колледжа с функциональным назначением ролей

Данный филиал ведет образовательную деятельность по следующим направлениям подготовки СПО и НПО: компьютерные системы и комплексы, техническое обслуживание и ремонт автомобильного транспорта, радиоаппаратостроение, технология машиностроения, сварщик, экономика и бухгалтерский учет (по отраслям) и повар-кондитер.

Учебно-материальная база филиала по объему и содержанию отвечает лицензионным требованиям и условиям осуществления образовательной деятельности по образовательным программам, заявленным в лицензии. Образовательный процесс в филиале организован в зданиях и помещениях общей площадью 13698 кв.м. Материальная база Кыштымского филиала включает в себя: три учебных корпуса, стрельбище, столовую и медпункт.

Учебно-лабораторная база включает в себя: 20 учебных кабинетов, 17 лабораторий, 5 компьютерных зала, 6 мастерских (радиомонтажная, слесарная, авто-слесарная, механическая, сварочная и кулинарно-кондитерская), спортивный зал, тренажерный зал, библиотеку и актовый зал.

В свою очередь в компьютерных залах в общем размещено 70 компьютеров, все учебные кабинеты оборудованы автоматизированным рабочим местом преподавателя с мультимедийным оборудованием (проектор, экран, колонки). В колледже функционирует компьютерная сеть, которая подразделяется на локальную и административную части. Со всех рабочих станций присутствует выход в сеть Интернет, максимальная пропускная способность внутренней сети составляет 100 Мбит/с, а входящего канала – 12 Мбит/с. Имеется 2 сервера локальной сети, которые необходимы для следующей работы: обновление программного обеспечения (драйвера на оборудование, обновления операционной системы и антивирусного обеспечения, патчи к специализированным программам), работа с системой «Консультант-Плюс», работа с системой «Компас 3Д», работа с системой дистанционного обучения «АСУ ProCollege», контроль и фильтрация выхода в сеть Интернет (Traffik Inspector, NAT).

Таким образом, информационно-техническая база Кыштымского филиала включает в себя: персональные компьютеры (127 штук), видеопроекторы (28 штук), принтеры (25 штук), сканеры (13 штук), копировальные аппараты (6 штук). Применяется, следующее программное обеспечение: операционные системы (Windows XP, Windows 7, Windows 10, виртуальная машина), прикладные пакеты (MS Office 2016, 1-С Бухгалтерия, 1-С Предприятие, Microsoft Visual, Studio, Arduino IDE, Компас, Picad 2001).

Также, как упоминалось ранее, в колледже используется автоматизированная информационная система «АСУ ProCollege», которая осуществляет следующие решения: регистрация персональных данных абитуриентов во время приемной комиссии на набор нового учебного года по аккредитованным направлениям подготовки, непосредственный процесс обучения с использованием дистанционных технологий при помощи различного инструментария (анкетирование, видеоконференции, вики по изучаемому курсу, глоссарий, семинары, тестирование, форумы, чат с преподавателем, размещение обучающих материалов, ведение электронного журнала успеваемости и посещаемости), проектирование и ведение электронного расписания занятий синхронизированного с учебными планами специальностей, разграничение доступа согласно должностным обязанностям в системе, автоматизация всех видов административной деятельности образовательной организации, планирование тарификации сотрудников.

Помимо, автоматизированной системы управления, в состав средств информационного воздействия входят следующие компоненты: рабочий чат в мессенджере Viber для сотрудников, рабочий чат в социальной сети «Вконтакте», личные чаты обучающихся групп в социальной сети «Вконтакте», официальная группа в социальной сети «Вконтакте» образовательной организации. Личный сайт у филиала отсутствует, но существует у головного учреждения.

После проведенного анализа единого информационного пространства колледжа, создадим рабочую группу из 5 человек и определим уровень исходной защищенности информационных систем персональных данных (далее ИСПДн), а также комплексную оценку опасности угроз ИСПДн. Для этого воспользуемся методикой, утвержденной ФСТЭК России (приказ от 18 февраля 2013 г. N 21), согласно которой может быть выделено три уровня, показатель - «Y_1»: высокий, средний и низкий. Первым этапом заполняется таблица, где отмечается положительное соотношение критериев (таблица 4).

Таблица 4 – Показатель исходного уровня защищенности ИСПДн колледжа

Технические и эксплуатационные критерии	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:			
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий	-	+	-
2. По наличию соединения с сетями общего пользования			
ИСПДн, имеющая многоточечный выход в сеть общего пользования	-	-	+
3. По встроенным (легальным) операциям с записями баз персональных данных			
модификация, передача	-	-	+
4. По разграничению доступа к персональным данным			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект персональных данных	-	+	-
5. По наличию соединений с другими базами персональных данных иных ИСПДн			
интегрированная ИСПДн (организация использует несколько баз персональных данных ИСПДн, при этом организация не является владельцем всех используемых баз персональных данных)	-	-	+
6. По уровню обобщения (обезличивания) персональных данных			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	-	+	-
7. По объему персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки			
ИСПДн, предоставляющая всю базу данных с персональными данными	-	-	+

После заполнения таблицы 4, подсчитываем сумму положительных критериев по каждому столбцу, а также выявляем процентное соотношение – таблица 5.

Таблица 5 – Процентное соотношение критериев по таблице 4

Критерий	**Уровень защищенности ИСПДн**		
	Высокий	**Средний**	**Низкий**
Сумма положительного соотношения	∑=0	∑=3	∑=4
Процент от общего значения	0%	42,86%	57,14%
ИТОГО	∑<70%	∑<70%	∑>0%

Таким образом, согласно выявленным ранее данным и табличным значениям ФСТЭК, числовой коэффициент Y_1 равен 10, что предполагает низкую степень исходной защищенности.

Далее определим вероятность реализации различных типов угроз в рассматриваемой ИСПДн. Под вероятностью реализации угрозы понимается показатель – Y_2, характеризующий, насколько вероятным является реализации конкретной угрозы безопасности в складывающихся условиях обстановки. Такая вероятность определяется по следующим критериям:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы ($Y_2 = 0$);
- низкая вероятность – предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y_2 = 2$);
- средняя вероятность –предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны ($Y_2 = 5$);
- высокая вероятность – предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты ($Y_2 = 10$).

Заполняем таблицу, выполняя оценку вероятности реализации угрозы безопасности по различным категориям нарушителей – таблица 6.

Таблица 6 – Вероятность реализации угроз

Угроза безопасности персональных данных	**Вероятность реализации угрозы нарушителем Kn**								**Итог Y_2**
	K_1	**K_2**	**K_3**	**K_4**	**K_5**	**K_6**	**K_7**	**K_8**	
Угрозы утечки акустической информации	5	5	5	2	5	2	0	2	5
Угрозы утечки видовой информации	2	5	2	2	2	0	0	5	5
Угрозы утечки по каналу побочных электромагнитных излучений и наводок	2	5	5	5	5	10	0	10	10
Угрозы, реализуемые в ходе загрузки операционной системы	2	0	0	0	2	0	0	0	2
Угрозы, реализуемые после загрузки операционной системы	10	2	5	2	10	2	10	2	10
Угрозы внедрения вредоносных программ	5	2	2	5	5	10	0	2	10
Угрозы анализа сетевого трафика с перехватом передаваемой по сети информации	2	0	0	2	2	2	0	2	2
Угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.	2	0	0	2	2	2	0	2	2
Угрозы внедрения ложного объекта сети	2	0	0	2	2	2	0	2	2
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	2	0	0	2	2	0	0	2	2
Угрозы типа «Отказ в обслуживании»	5	2	5	0	5	0	0	5	5
Угрозы выявления паролей	5	2	2	5	5	5	0	5	5
Угрозы удаленного запуска приложений	2	0	0	2	2	2	2	2	2
Угрозы внедрения по сети вредоносных программ	10	2	2	2	10	2	10	2	10

По итогам оценки уровня исходной защищенности и вероятности реализации угрозы, рассчитывается коэффициент реализуемости угрозы (показатель - Y) и в соответствии с результатом определяется возможность реализации угрозы (таблица 7). Коэффициент реализуемости угрозы рассчитывается по формуле 1.

$$Y = (Y_1+Y_2)/20 \quad (1)$$

где Y_1 –уровень исходной защищенности;

Y_2 –вероятность реализации угрозы.

Таблица 7 - Коэффициент реализуемости угрозы

Угроза безопасности персональных данных	**Коэффициент реализуемости угрозы (Y)**	**Возможность реализации угрозы**
Угрозы утечки акустической (речевой) информации	0,75	Высокая
Угрозы утечки видовой информации	0,75	Высокая
Угрозы утечки по каналу побочных электромагнитных излучений и наводок	1	Очень высокая
Угрозы, реализуемые в ходе загрузки операционной системы	0,6	Средняя
Угрозы, реализуемые после загрузки операционной системы	1	Очень высокая
Угрозы внедрения вредоносных программ	1	Очень высокая
Угрозы анализа сетевого трафика с перехватом передаваемой по сети информации	0,6	Средняя
Угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.	0,6	Средняя
Угрозы внедрения ложного объекта сети	0,6	Средняя
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	0,6	Средняя
Угрозы типа «Отказ в обслуживании»	0,75	Высокая
Угрозы выявления паролей	0,75	Высокая
Угрозы удаленного запуска приложений	0,6	Средняя
Угрозы внедрения по сети вредоносных программ	1	Очень высокая

По значению коэффициента Y формируется интерпретация реализуемости угрозы следующим образом:

- если Y <= 0,3, то возможность реализации угрозы - низкая;
- если 0,3 < Y <= 0,6, то средняя;
- если 0,6 < Y <= 0,8, то высокая;
- если Y > 0,8, то очень высокая.

После производится оценка опасности на основе опроса технического отдела, определяется критериями опасности, которые имеют 3 уровня: низкая, средняя и высокая опасность. Оценка опасности с учетом приведенных критерием представлена в таблице 8.

Таблица 8 – Оценка опасности

Угроза безопасности персональных данных	**Опасность угроз**
Угрозы утечки акустической (речевой) информации	Высокая
Угрозы утечки видовой информации	Низкая
Угрозы утечки по каналу побочных электромагнитных излучений и наводок	Средняя
Угрозы, реализуемые в ходе загрузки операционной системы	Низкая
Угрозы, реализуемые после загрузки операционной системы	Средняя
Угрозы внедрения вредоносных программ	Средняя
Угрозы анализа сетевого трафика с перехватом передаваемой по сети информации	Низкая
Угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.	Низкая
Угрозы внедрения ложного объекта сети	Низкая
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	Низкая
Угрозы типа «Отказ в обслуживании»	Высокая
Угрозы выявления паролей	Высокая
Угрозы удаленного запуска приложений	Низкая
Угрозы внедрения по сети вредоносных программ	Средняя

Отнесение угрозы к актуальной производится по правилам, приведенным в таблице 9.

Таблица 9 – Правила соотношения актуальных угроз по ФСТЭК

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	Неактуальная	неактуальная	актуальная
Средняя	Неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

В соответствии с правилами соотнесения угроз безопасности к актуальным, существуют следующие угрозы для рассматриваемой базы исследования – таблица 10.

Таблица 10 – Актуальные угрозы ИСПДн колледжа

Угроза безопасности персональных данных	Опасность угроз
Угрозы утечки акустической (речевой) информации	Актуальная
Угрозы утечки видовой информации	Актуальная
Угрозы утечки по каналу побочных электромагнитных излучений и наводок	Актуальная
Угрозы, реализуемые в ходе загрузки операционной системы	Неактуальная
Угрозы, реализуемые после загрузки операционной системы	Актуальная
Угрозы внедрения вредоносных программ	Актуальная
Угрозы анализа сетевого трафика с перехватом передаваемой по сети информации	Неактуальная
Угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.	Неактуальная
Угрозы внедрения ложного объекта сети	Неактуальная
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	Неактуальная
Угрозы типа «Отказ в обслуживании»	Актуальная
Угрозы выявления паролей	Актуальная
Угрозы удаленного запуска приложений	Неактуальная
Угрозы внедрения по сети вредоносных программ	Актуальная

Таким образом, актуальными угрозами безопасности ПДн в ИСПДн ГБПОУ «Южно-Уральского государственного колледжа» Кыштымского филиала, согласно проведенной комплексной оценке, являются:

- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки по каналу побочных электромагнитных излучений и наводок;
- угрозы, реализуемые после загрузки операционной системы;
- угрозы внедрения вредоносных программ;
- угрозы типа «Отказ в обслуживании»;
- угрозы выявления паролей;
- угрозы внедрения по сети вредоносных программ.

Также, помимо комплексной объективной оценки, был проведен эксперимент. Цель которого заключалась в том, чтобы определить на сколько результаты анализа ИСПДн были точны и актуальны ли они в целом.

Эксперимент заключался в следующем. Были организованы 3 экспериментальные группы, участники которых отличались между собой по определенным признакам. Им было предложено выполнить ряд определенных задач любым известным им способом, работа участников в группе проводилась по отдельности.

Подробнее о составе экспериментальных групп (таблица 11) и поставленными перед ними задачами (рисунки 8-10)

Таблица 11 – Состав экспериментальных групп

№	Шифр участника	Характеристика участника
Группа 1 – обучающиеся колледжа		
1	1.1э	Студент 2 курса, группа 281-К
2	1.2э	Студент 3 курса, группа 374-К
3	1.3э	Студент 4 курса, группы 467-К
Группа 2 – выпускники специальности КСиК		
1	2.1э	Выпускник, год выпуска 2021
2	2.2э	Выпускник, год выпуска 2022
3	2.3э	Выпускник, год выпуска 2023
Группа 3 –третьи лица		
1	3.1э	Обучающийся 11 класса МОУ СОШ №2
2	3.2э	Сотрудник компании «Интерсвязь»
3	3.3э	Пенсионерка

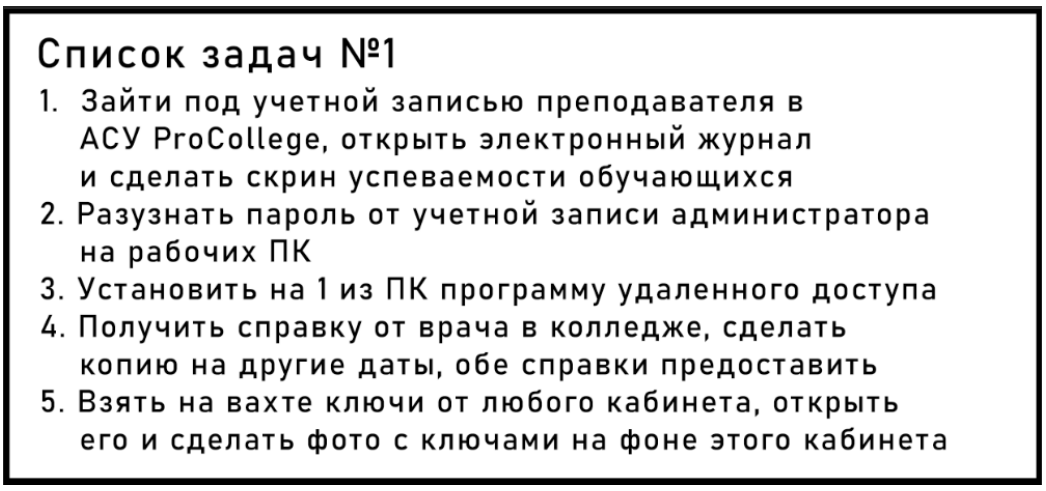

Рисунок 8 – Список задач для группы 1

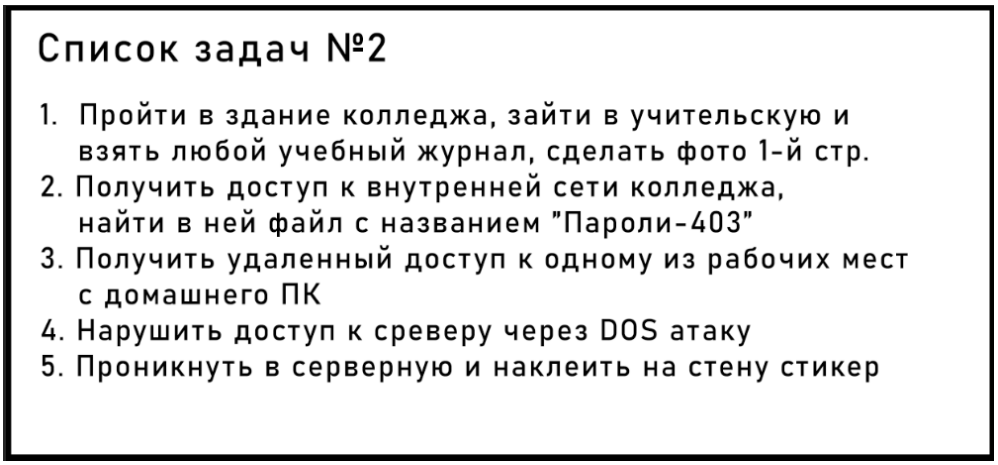

Рисунок 9 – Список задач для группы 2

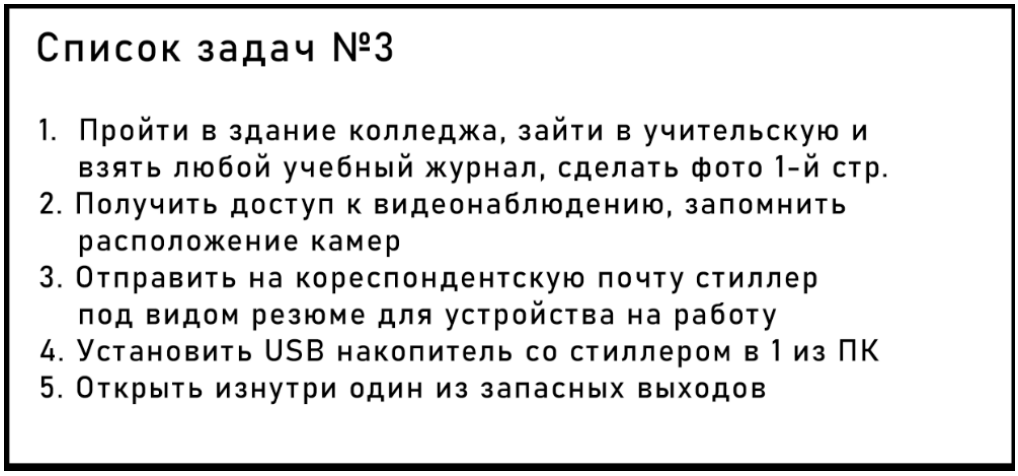

Рисунок 10 – Список задач для группы 3

На выполнение задач участникам отводилось 6 дней, по истечению которых им необходимо было предоставить отчет о выполнении данной работы (результат выполнения задачи: если результат был положительным, то ход его выполнения и если результат был отрицательным, то, что этому препятствовало; сколько времени было затрачено на каждую задачу; предложения по устранению недостатков системы безопасности).

Далее результаты были обработаны и представлены на графиках 2-4.

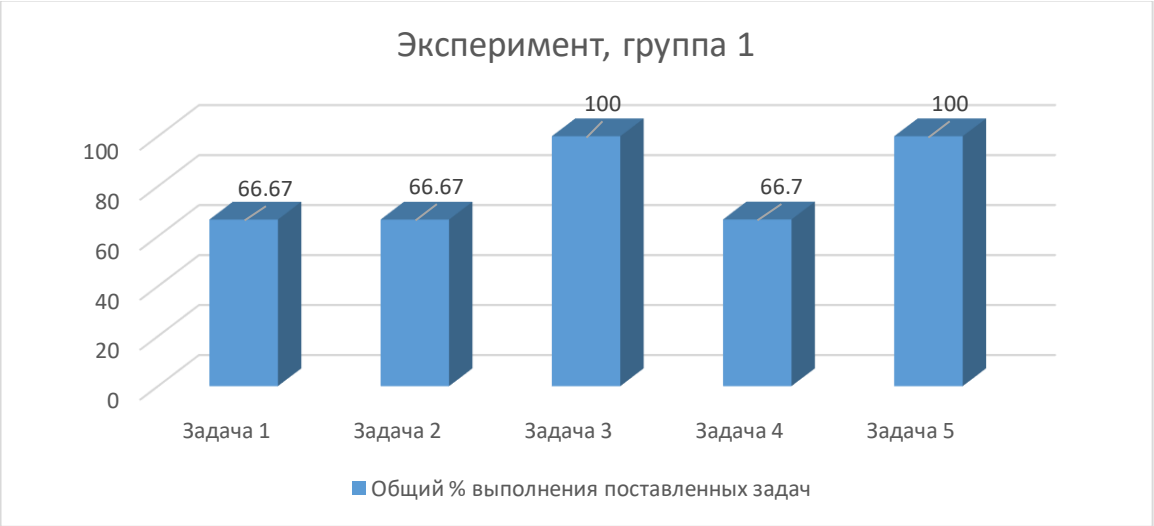

График 2 – Результаты эксперимента, группа 1

Согласно обработанным данным по группе 1, интерпретация результатов следующая:

– задача 1: справилось 2 участника, которым не представило труда узнать логин и пароль от АСУ, так как преподаватели сами выдавали их обучающимся для заполнения электронного журнала;

– задача 2: справилось 2 участника, которым преподаватель сам ввел пароль от администратора во время практической работы, так как «Компас 3Д» открывается на некоторых ПК «от имени администратора»;

– задача 3: все участники справились с выполнением – это объясняется тем, что под учетной записью «Студент» в компьютерном классе 401, отсутствуют ограничения в установке любого программного обеспечения;

– задача 4: справилось 2 участника, которые сделали шаблон имеющейся у них справки, распечатали, заполнили и подделали подпись;

– задача 5: все участники справились с выполнением, так как сотрудники «вахты» по необходимости выдают ключи всем.

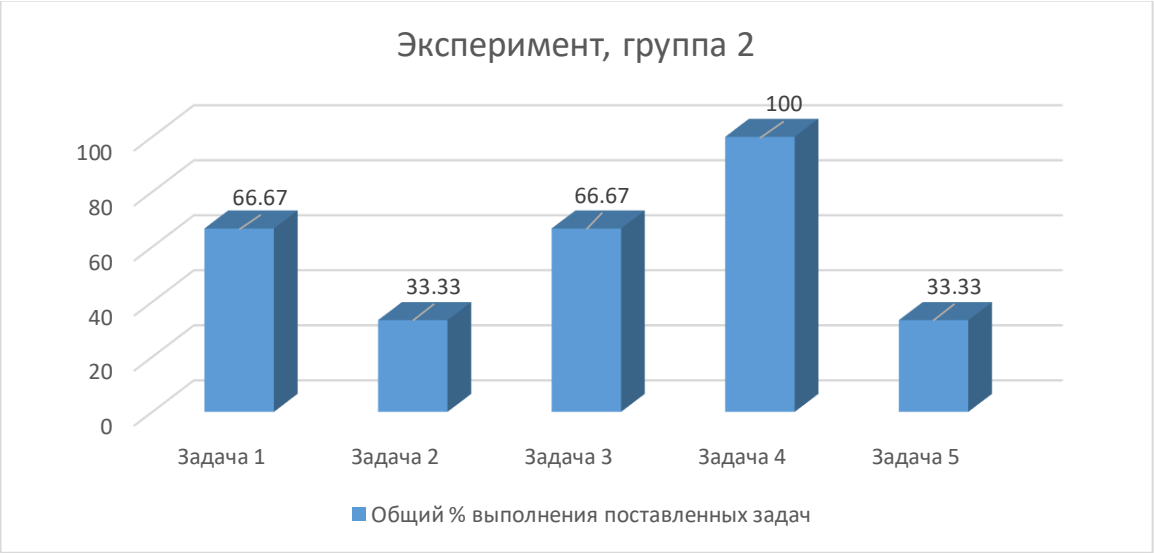

График 3 – Результаты эксперимента, группа 2

Исходя из следующих обработанных данных, интерпретация результатов для группы 2:

– задача 1: справилось 2 участника, которые беспрепятственно проникли в колледж через главный вход во время обеденного перерыва;

– задача 2: справился 1 участник, который воспользовался персональным компьютером, подключенным ко внутренней сети колледжа, располагавшимся в библиотеке;

– задача 3: справилось 2 участника, которые воспользовались компьютером в 401 кабинете для установки стороннего ПО, пока ответственного лица за аудиторию не было на месте;

– задача 4: все участники справились с выполнением, так как внутренние сервера филиала никак не защищены от атак такого типа;

– задача 5: справился 1 участник, который взял ключ от серверной комнаты непосредственно у сотрудника технического отдела.

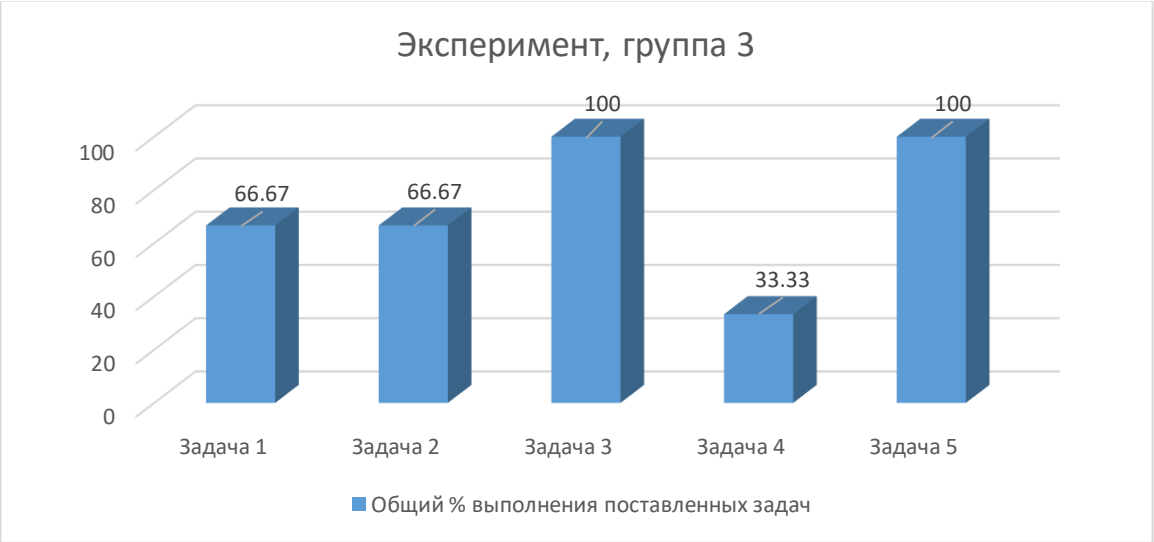

График 4 – Результаты эксперимента, группа 3

Исходя из следующих обработанных данных, интерпретация результатов для группы 3:

– задача 1: справилось 2 участника, которые прошли через главный вход колледжа под разными предлогами (забыл студенческий билет, вызвали на беседу к заведующей по учебной части);

– задача 2: справилось 2 участника – это объясняется тем, что мониторы системы видеонаблюдения никак не скрыты от посторонних глаз и находятся в поле зрения обучающихся, находящихся рядом с доской расписания занятий или проходящих через «карусель» главного хода;

– задача 3: все участники справились с выполнением, так как уполномоченные сотрудники организации открыли и скачали приложенное резюме из всех отправленных электронных писем;

– задача 4: справился 1 участник, который воспользовался персональным компьютером в библиотеке колледжа;

– задача 5: все участники справились с выполнением, так как запасные выходы не закрыты на замок, а на щеколду, что не представляет труда ее открыть.

Таким образом, согласно проведенному анализу единого информационного пространства колледжа, можно обнаружить огромный ряд недостатков в системе безопасности образовательной организации (утечки акустической и видовой информации; утечки по каналу побочных электромагнитных излучений и наводок; угрозы, реализуемые после загрузки операционной системы; внедрение вредоносных программ; угрозы типа «Отказ в обслуживании» и выявления паролей; внедрение по сети вредоносных программ), который был не только выявлен при оценке рабочей группы исходного уровня защищенности информационной системы персональных данных, но и экспериментально подтверждён.

2.2 Комплекс мероприятий по совершенствованию методов обеспечения информационной безопасности в ГБПОУ «Южно-Уральский государственный колледж» Кыштымского филиала

Проведя ранее анализ единого информационного пространства организации, удалось выявить актуальные угрозы безопасности. В связи с чем был разработан следующий комплекс мероприятий применительно к ним.

Угроза несанкционированного доступа в здание колледжа. Представляет собой потенциальную возможность того, что злоумышленники или неавторизованные пользователи смогут получить доступ к системам, данным или сетям, к которым они не должны иметь доступа. В нашем случае, проникнуть непосредственно в организацию можно воспользовавшись одним из пяти проходов, поэтому необходимо применить к ним различные меры друг от друга, которые представлены в таблице 12.

Таблица 12 – Меры безопасности от несанкционированного доступа в здание

Наименование прохода	**Характеристика обстановки**	**Мероприятия по совершенствованию защиты**
Главный вход	Контролируется изнутри вахтёром пожилого возраста, который имеет доступ к камерам видеонаблюдения и оповестительным системам, также на входе установлена пропускная «карусель»	Установить при входе рамку металлоискателя Заключить договор с охранной организацией для предоставления услуг охраны колледжа
Вход с внутренней парковки в столовую (технический подъезд)	Никак не контролируется, вход и выход свободный, дверь в часы работы столовой постоянно открыта	Держать дверь закрытой, открывать только при необходимости (подвоз продуктов, выброс отходов)
Вход с внутренней парковки в мастерские	Дверь открывается при помощи специального домофонного ключа, но иногда обучающиеся и педагоги открывают дверь и подкладывают предмет, чтобы она не закрывалась	Поставить доводчик Провести профилактические беседы с обучающимися и сотрудниками
Эвакуационные выходы (корпус 1 и 3)	Согласно пожарной безопасности выходы должны быть постоянно открыты, но в целях угрозы террористической атаки и несанкционированного доступа они должны быть закрыты, возникает противоречие	Поставить изнутри на выходы задвижки Периодически проверять положение задвижек

Модернизация парка вычислительной техники колледжа. Все оборудование, применяемое в колледже, старше 15 лет. Оно часто выходит из строя, запас резервных запчастей исчерпал себя, оборудование стало не рентабельным. Также с технологическим прогрессом возросли системные требования к аппаратной части техники, что привело к регрессу процесса обучения по современным направлениям программы «Профессионалитет». Программа «Профессионалитет», в рамках ГБПОУ «ЮУГК» КФ, предполагает подготовку специалистов по двум направлениям «Компьютерные системы и комплексы» и «Разработка электронных устройств и систем», первый набор по данным специальностям был осуществлен в 2023г.

Реализация по данным направлениям освоения в полной мере специальных дисциплин не представляется возможной из-за отсутствия необходимого современного оборудования, а в дальнейшем и прохождения успешного демонстрационного экзамена обучающимися. Необходимо в срочном порядке закупить оборудование согласно чек-листу (таблица 13) площадки демонстрационного экзамена по осуществляемым направлениям. Это решит не только проблему с регрессом процесса обучения, но и угрозы типа «отказ в обслуживании», а также появится возможность организации более сложной и защищенной внутренней сети.

Старое оборудование все еще можно использовать в процессе обучения по профессиональным модулям, таких как: ПМ.01 «Сборка, монтаж и демонтаж электронных устройств и систем в соответствии с технической документацией», ПМ.03 «Техническое обслуживание и ремонт компьютерных систем и комплексов» - диагностика неисправностей с последующим ремонтом, замена или ремонт компонентов, чистка кулера и внутреннего пространства компьютера, обновление оборудования для повышения производительности системы.

Также помимо рабочих мест, необходимо выполнить закупку нового серверного оборудования, так как оно постоянно выходит из строя из-за не отвечающих требованиям помещения, где оно функционирует, а также самим ресурсом комплектующих. Данная мера решит следующие угрозы: повреждение данных, неполное резервное копирование, недостаток места при хранении данных, отказ в функционировании АСУ ProCollege – приостановка работы учебной части (тарификация, формирование отчетов, внесение изменений в электронном расписании и т.д.).

Таблица 13 – Минимальный перечень необходимого оборудования

№	Наименование	Минимальные хар-ки
1	Системный блок	Процессор: частота 2 ГГц, 2 ядра, 6 потоков Оперативное запоминающее устройство: 8 Гб Постоянное запоминающее устройство: 520Гб
2	Монитор	IPS, 1920x1080, 75 ГГц
3	Экран для проектора	Формат 16:9 Габариты: 2400*1350
4	Видеокамера	Разрешение: 1280*720 Сжатие MP4 Объектив: широкоугольный
5	ПО	Arduino IDE, Fritzing, Prozessing, Altium Designer, Kompas 3D 22v, Multisim
6	Браслет заземления антистатический	Браслет регулируемый, растягивающийся, с изолирующей поверхность, сопротивление к земле 1МОм, кнопка 10мм
7	Дымоуловитель с угольным фильтром	Напряжение питания 230 В, 50/60 Гц Номинальная производительность 1,7 м³/мин. Габариты: 200 × 208 × 130 мм.
8	Трехканальная паяльная станция с паяльником, вакуумным паяльником и термопинцетом	Электропитание: 220В, 50Гц. Диапазон температур: 37 - 482°C. С табильность температуры: ±1,1°C. Глубина вакуума: 20in Hg max (508 мм рт.ст.). Сопротивление заземления наконечника не более 2 Ом
9	Принтер для трафаретной печати	Регулируемое давление на ракель, размер ПП не менее 200 х 300мм, пневмопитание.
10	Автоматический установщик SMD-компонентов	Кол-во вакуумных захватов не менее 4х. Скорость установки, не менее 4000 компонентов в час Монитор: не менее 15", электропитание: 220 В/50 Гц
11	Конвейерная печь оплавления	Печь должна обеспечивать выполнение рекомендованного производителем паяльного материала термопрофиля для бессвинцовой пайки для плат габаритными размерами до 200 х 300мм
12	Компрессор	Производительность,180 л/мин Питание 220 В

Угрозы утечки видовой информации. В колледже на данный момент имеется 4 компьютерных класса, в одном из них, планировка выполнена, таким образом, что все, что делает педагог на своем АРМ видно окружающим (например, ввод пароля администрируемой учетной записи под которой открывается большой спектр возможностей по доступу к внутренней сети). Поэтому необходимо изменить планировку внутри помещений с такой же проблемой. Пример модернизации планировки компьютерная зала представлен на рисунке 11.

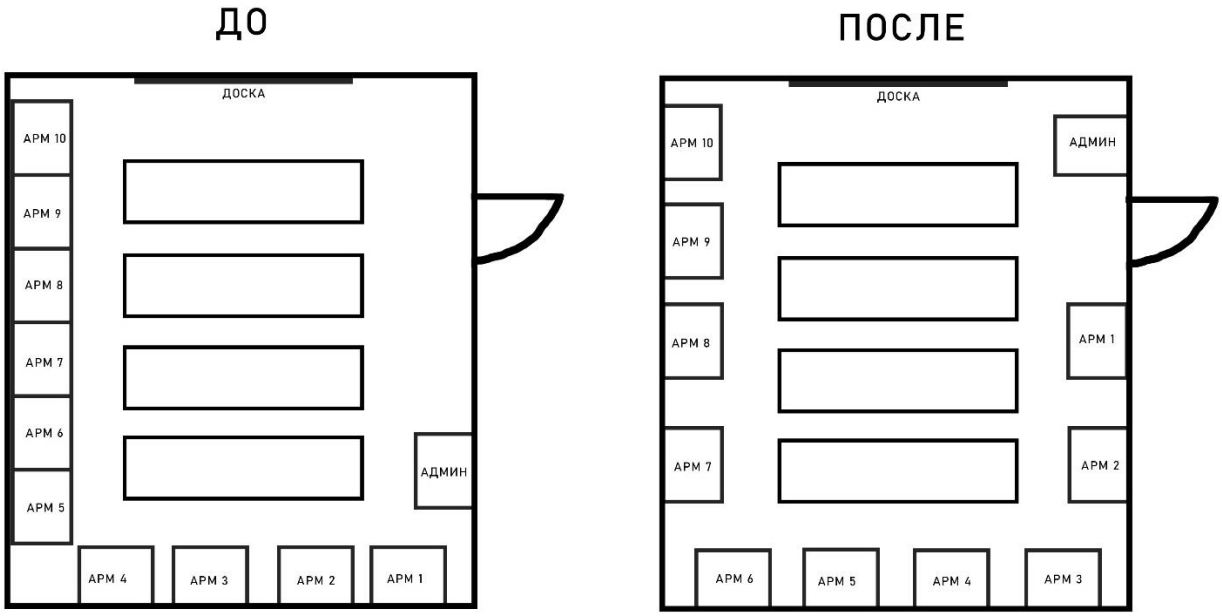

Рисунок 11 – Модернизация планировки в кабинете 403 (ГБПОУ «ЮУГК КФ)»

Угрозы утечки по каналу побочных электромагнитных излучений и наводок. На всем оборудовании, что есть в колледже, отсутствуют пломбы и маркеры, сигнализирующие о вскрытии прибора. Необходимо опломбировать корпуса техники во избежание подключения несанкционированных устройств к ним, а также выполнять ряд профилактических мероприятий в определенный промежуток времени (подробнее о них в приложение).

Угрозы, реализуемые после загрузки операционной системы. Так как используется устаревшее оборудование, то обновление системы и приложений невозможно из-за неподдерживаемых системных требований программного обеспечения. Необходимо установить на каждое рабочее место антивирус «Касперский» и через него организовать проверку подключаемых устройств, устанавливаемого программного обеспечения, скачиваемых файлов на предмет вирусов и «хакерских» программ. При модернизации парка вычислительной техники, установке современного программного обеспечения и его настройке, риски по данной проблеме сами по себе снизятся до минимума.

Угрозы утечки информации. В педагогическом коллективе присутствует много сотрудников пожилого возраста, которые не компетентны в области информационной безопасности, но при этом имеют полный доступ к внутренней сети колледжа. Такие сотрудники, часто записывают пароль от учетной записи на бумажку и кладут ее под клавиатуру или вовсе выбирают студента, выдают им свой логин и пароль от АСУ ProCollege и просят заполнить журнал за него. В связи с этим необходимо выполнить создание дополнительных учетных записей, которые будут сильно ограничены в функциях во внутренней и внешней сети. Категории таких пользователей будут иметь разграничение по итогам тестирования в области информационной безопасности (подробнее в приложении): 1 категория (прошел тестирование на высокий уровень), 2 категория (прошел на средний уровень), 3 категория (не справился с тестированием).

Угрозы утраты данных. В настоящее время почти половина от всего документооборота все еще осуществляется не в цифровом виде. Личные дела обучающихся, дипломные проекты, курсовые работы, дневники и отчеты по практикам, учебные журналы и журналы практик, приказы, распоряжения директора – ведутся в бумажном варианте, где по окончании хранятся в архивах. Огромный риск, что документация может быть утеряна, изменена, украдена или утрачена в пожаре. Необходимо переходить на электронную форму отчетности, но для этого нужно организовать работу в полной мере через сеть и расширить объем хранения данных на внутреннем сервере.

Таким образом, все предложенные меры на данный момент, были реализованы не в полном объеме: осуществляется перепланировка помещений, ведется работа по модернизации парка вычислительной техники (частично закуплено оборудование для демонстрационного экзамена, подана заявка на приобретение техники и оснащения одного нового компьютерного класса по программированию).

2.3 Контрольная оценка эффективности комплекса мероприятий по совершенствованию методов обеспечения информационной безопасности в профессиональной образовательной организации

Для проверки эффективности, внедренных мероприятий по совершенствованию методов обеспечения информационной безопасности в колледже, необходимо произвести контрольную оценку уровня защищенности ИСПДн и опасности угроз в ней, а также вновь провести эксперимент (ранее описанный в пункте 2.1).

В составе той же рабочей группы из 5 человек, что и в первый раз, воспользуемся, как и в подпункте 2.1, методикой, утвержденной ФСТЭК России. Первым этапом заполняется таблица, где отмечается положительное соотношение критериев (таблица 14).

Таблица 14 – Показатель уровня защищенности ИСПДн колледжа

Технические и эксплуатационные критерии	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:			
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий	-	+	-
2. По наличию соединения с сетями общего пользования			
ИСПДн, имеющая многоточечный выход в сеть общего пользования	-	-	+
3. По встроенным (легальным) операциям с записями баз персональных данных			
модификация, передача	-	+	-
4. По разграничению доступа к персональным данным			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект персональных данных	-	+	-
5. По наличию соединений с другими базами персональных данных иных ИСПДн			
интегрированная ИСПДн (организация использует несколько баз персональных данных ИСПДн, при этом организация не является владельцем всех используемых баз персональных данных)	-	+	-
6. По уровню обобщения (обезличивания) персональных данных			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	-	+	-

Продолжение таблицы 14

Технические и эксплуатационные критерии	Уровень защищенности		
	Высокий	Средний	Низкий
7. По объему персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки			
ИСПДн, предоставляющая всю базу данных с персональными данными	-	-	+

После заполнения таблицы 14, подсчитываем сумму положительных критериев по каждому столбцу, а также выявляем процентное соотношение – таблица 15.

Таблица 15 – Процентное соотношение критериев по таблице 13

Критерий	Уровень защищенности ИСПДн		
	Высокий	Средний	Низкий
Сумма положительного соотношения	∑=0	∑=5	∑=2
Процент от общего значения	0%	71,43%	28,57%
ИТОГО	∑<70%	∑>70%	∑>0%

Таким образом, согласно выявленным ранее данным и табличным значениям ФСТЭК, числовой коэффициент Y_1 равен 5, что предполагает среднюю степень исходной защищенности.

Далее определим вероятность реализации различных типов угроз в рассматриваемой ИСПДн. Под вероятностью реализации угрозы понимается показатель – Y_2, характеризующий, насколько вероятным является реализации конкретной угрозы безопасности в складывающихся условиях обстановки. Такая вероятность определяется по следующим критериям:

– маловероятно – отсутствуют объективные предпосылки для осуществления угрозы ($Y_2 = 0$);

– низкая вероятность – предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y_2 = 2$);

– средняя вероятность –предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны ($Y_2 = 5$);

– высокая вероятность – предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты ($Y_2 = 10$).

Заполняем таблицу, выполняя оценку вероятности реализации угрозы безопасности по различным категориям нарушителей – таблица 16.

Таблица 16 – Вероятность реализации угроз

Угроза безопасности персональных данных	**Вероятность реализации угрозы нарушителем Kn**								**Итог Y_2**
	K_1	**K_2**	**K_3**	**K_4**	**K_5**	**K_6**	**K_7**	**K_8**	
Угрозы утечки акустической информации	5	5	5	2	5	2	0	2	5
Угрозы утечки видовой информации	2	2	2	2	2	0	0	2	2
Угрозы утечки по каналу побочных электромагнитных излучений и наводок	2	5	5	5	5	5	0	5	5
Угрозы, реализуемые в ходе загрузки операционной системы	2	0	0	0	2	0	0	0	2
Угрозы, реализуемые после загрузки операционной системы	5	2	5	2	5	2	5	2	5
Угрозы внедрения вредоносных программ	5	2	2	5	5	5	0	2	5
Угрозы анализа сетевого трафика с перехватом передаваемой по сети информации	2	0	0	2	2	2	0	2	2
Угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.	2	0	0	2	2	2	0	2	2
Угрозы внедрения ложного объекта сети	2	0	0	2	2	2	0	2	2
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	2	0	0	2	2	0	0	2	2
Угрозы типа «Отказ в обслуживании»	5	2	5	0	5	0	0	5	5
Угрозы выявления паролей	2	2	0	2	2	2	0	2	2
Угрозы удаленного запуска приложений	2	0	0	2	2	2	2	2	2
Угрозы внедрения по сети вредоносных программ	5	2	2	2	5	2	5	2	5

По итогам оценки уровня исходной защищенности и вероятности реализации угрозы, рассчитывается коэффициент реализуемости угрозы (показатель - Y) и в соответствии с результатом определяется возможность реализации угрозы (таблица 17). Коэффициент реализуемости угрозы рассчитывается по формуле 1 (подпункт 2.1).

Таблица 17 - Коэффициент реализуемости угрозы

Угроза безопасности персональных данных	**Коэффициент реализуемости угрозы (Y)**	**Возможность реализации угрозы**
Угрозы утечки акустической (речевой) информации	0,5	Средняя
Угрозы утечки видовой информации	0,35	Средняя
Угрозы утечки по каналу побочных электромагнитных излучений и наводок	0,5	Средняя
Угрозы, реализуемые в ходе загрузки операционной системы	0,35	Средняя
Угрозы, реализуемые после загрузки операционной системы	0,5	Средняя
Угрозы внедрения вредоносных программ	0,5	Средняя
Угрозы анализа сетевого трафика с перехватом передаваемой по сети информации	0,35	Средняя
Угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.	0,35	Средняя
Угрозы внедрения ложного объекта сети	0,35	Средняя
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	0,35	Средняя
Угрозы типа «Отказ в обслуживании»	0,5	Средняя
Угрозы выявления паролей	0,35	Средняя
Угрозы удаленного запуска приложений	0,35	Средняя
Угрозы внедрения по сети вредоносных программ	0,5	Средняя

По значению коэффициента Y формируется интерпретация реализуемости угрозы следующим образом:

- если Y <= 0,3, то возможность реализации угрозы - низкая;
- если 0,3 < Y <= 0,6, то средняя;
- если 0,6 < Y <= 0,8, то высокая;
- если Y > 0,8, то очень высокая.

После производится оценка опасности на основе опроса технического отдела, определяется критериями опасности. Оценка опасности с учетом приведенных критериев представлена в таблице 18.

Таблица 18 – Оценка опасности

Угроза безопасности персональных данных	Опасность угроз
Угрозы утечки акустической (речевой) информации	Средняя
Угрозы утечки видовой информации	Низкая
Угрозы утечки по каналу побочных электромагнитных излучений и наводок	Низкая
Угрозы, реализуемые в ходе загрузки операционной системы	Низкая
Угрозы, реализуемые после загрузки операционной системы	Средняя
Угрозы внедрения вредоносных программ	Средняя
Угрозы анализа сетевого трафика с перехватом передаваемой по сети информации	Низкая
Угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.	Низкая
Угрозы внедрения ложного объекта сети	Низкая
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	Низкая
Угрозы типа «Отказ в обслуживании»	Высокая
Угрозы выявления паролей	Низкая
Угрозы удаленного запуска приложений	Низкая
Угрозы внедрения по сети вредоносных программ	Средняя

Отнесение угрозы к актуальной производится по правилам, приведенным в таблице 9.

В соответствии с правилами соотнесения угроз безопасности к актуальным, существуют следующие угрозы для рассматриваемой базы исследования после ее совершенствования – таблица 19.

Таблица 19 – Актуальные угрозы ИСПДн колледжа

Угроза безопасности персональных данных	Опасность угроз
Угрозы утечки акустической (речевой) информации	Актуальная
Угрозы утечки видовой информации	Неактуальная
Угрозы утечки по каналу побочных электромагнитных излучений и наводок	Неактуальная
Угрозы, реализуемые в ходе загрузки операционной системы	Неактуальная
Угрозы, реализуемые после загрузки операционной системы	Актуальная
Угрозы внедрения вредоносных программ	Актуальная
Угрозы анализа сетевого трафика с перехватом передаваемой по сети информации	Неактуальная
Угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.	Неактуальная
Угрозы внедрения ложного объекта сети	Неактуальная
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	Неактуальная

Продолжение таблицы 19

Угроза безопасности персональных данных	Опасность угроз
Угрозы типа «Отказ в обслуживании»	Актуальная
Угрозы выявления паролей	Неактуальная
Угрозы удаленного запуска приложений	Неактуальная
Угрозы внедрения по сети вредоносных программ	Актуальная

Таким образом, актуальными угрозами безопасности ПДн в ИСПДн ГБПОУ «Южно-Уральского государственного колледжа» Кыштымского филиала, согласно проведенной комплексной оценке, являются:

- угрозы утечки акустической (речевой) информации;
- угрозы, реализуемые после загрузки операционной системы;
- угрозы внедрения вредоносных программ;
- угрозы типа «Отказ в обслуживании»;
- угрозы внедрения по сети вредоносных программ.

Контрольный эксперимент заключался в следующем. Были организованы 3 контрольные группы, участники которых не принимали ранее участие в эксперименте. Им было предложено выполнить тот же ряд задач, что и экспериментальным группам.

Подробнее о составе экспериментальных групп (таблица 20) и поставленными перед ними задачами (рисунки 8-10)

Таблица 20 – Состав экспериментальных групп

№	Шифр участника	Характеристика участника
Группа 1 – обучающиеся колледжа		
1	1.1к	Студент 2 курса, группа 281-К
2	1.2к	Студент 3 курса, группа 374-К
3	1.3к	Студент 4 курса, группы 467-К
Группа 2 – выпускники специальности КСиК		
1	2.1к	Выпускник, год выпуска 2021
2	2.2к	Выпускник, год выпуска 2022
3	2.3к	Выпускник, год выпуска 2023
Группа 3 –третьи лица		
1	3.1к	Обучающийся 11 класса МОУ СОШ №1
2	3.2к	Сотрудник компании «Интерсвязь»
3	3.3к	Пенсионерка

На выполнение задач участникам отводилось 6 дней, по истечению которых им необходимо было предоставить, также отчет.

Далее результаты были обработаны и представлены в сравнении (графики 5-7).

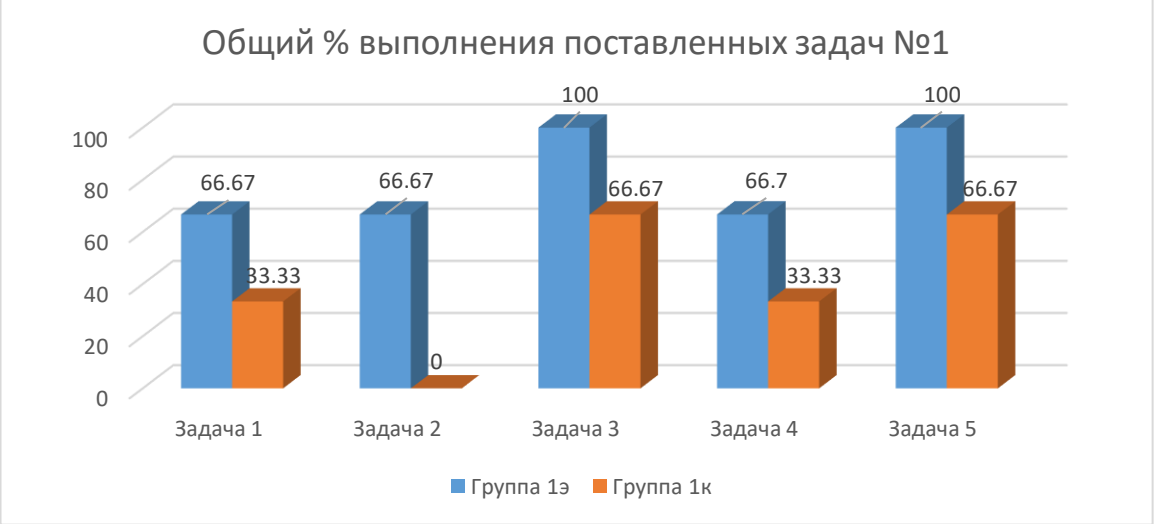

График 5 – Результаты контрольного эксперимента, группа 1

Согласно обработанным данным по группам 1 (экспериментальная и контрольная), интерпретация результатов следующая:

– задача 1: была проведена профилактическая беседа с персоналом по вопросу «информационная безопасность», осуществлена смена паролей от учетных записей, в результате задачу выполнил только 1 участник;

– задача 2: была осуществлена смена паролей категории «Администратор», в силу этого с заданием никто не справился;

– задача 3: была начата работа по настройке и модернизации локальной вычислительной сети, ввиду этого с заданием справилось 2 участника;

– задача 4: была проведена беседа с сотрудником здравоохранения, после чего на справках ставится печать, в результате с заданием справился 1 участник;

– задача 5: была проведена беседа с сотрудниками, ведется учет выданных ключей, в результате с заданием справились 2 участника.

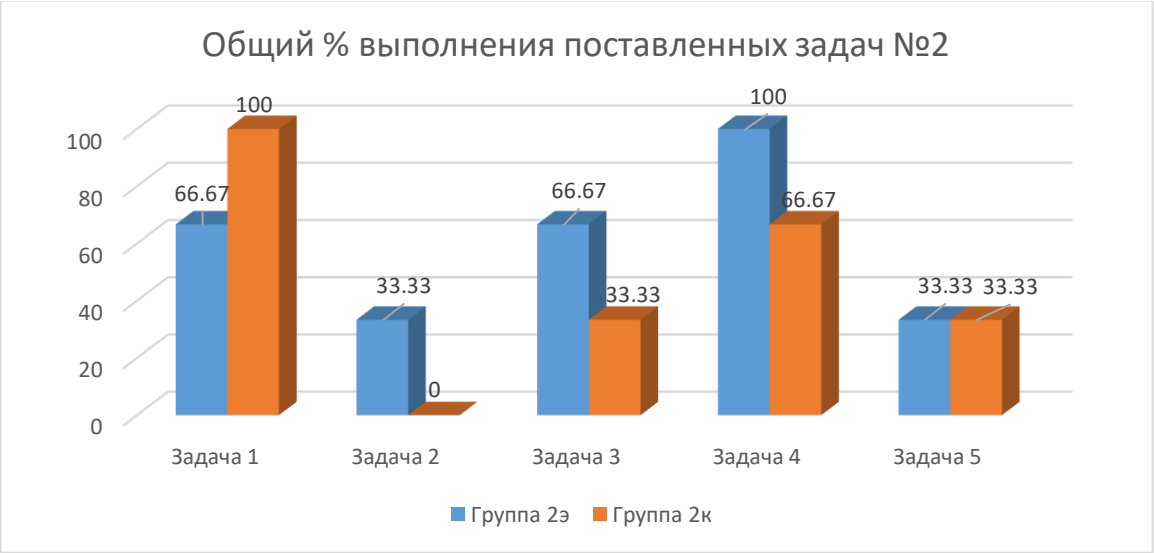

График 6 – Результаты контрольного эксперимента, группа 2

Исходя из следующих обработанных данных по группам 2 (экспериментальная и контрольная), интерпретация результатов следующая:

– задача 1: был заключен договор с охранной организацией, помимо вахтера, теперь имеется и сотрудник охраны, но во время обеденного перерыва, также не проверяются студенческие билеты, поэтому с данным заданием справились все участники;

– задача 2: была осуществлена смена паролей категории «Администратор», в силу этого с заданием никто не справился;

– задача 3: так как работа по модернизации локальной вычислительной сети была начата относительно недавно, то не на всех компьютерах в 401 кабинете настроены права администратора, в результате с заданием справился 1 участник;

– задача 4: 2 участника справились с выполнением, так как внутренние сервера филиала никак не защищены от атак такого типа;

– задача 5: справился 1 участник, который взял ключи от кабинета 403 и ключом от лаборантской открыл серверную комнату.

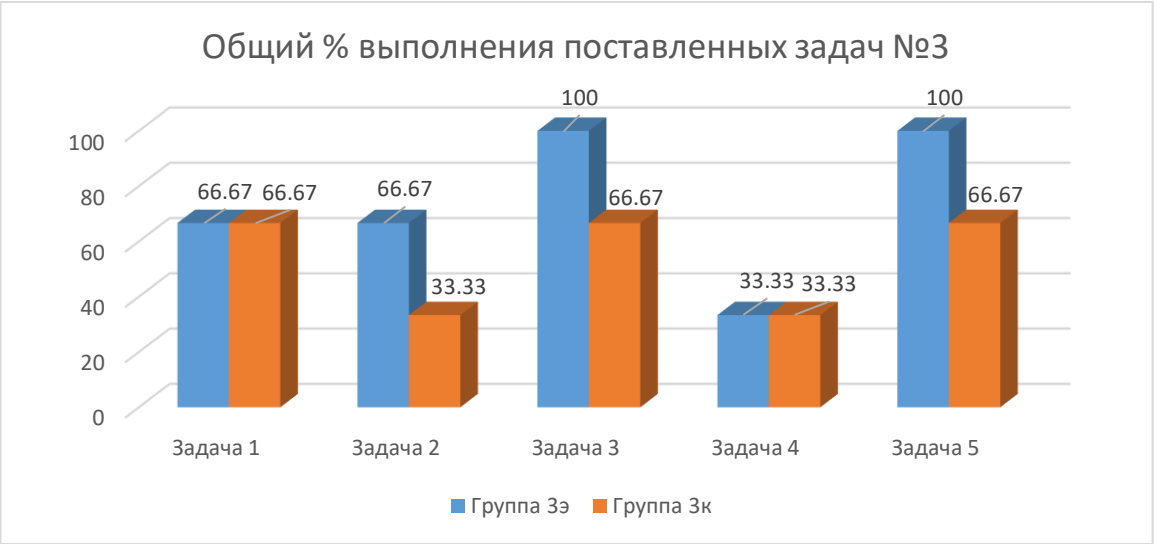

График 7 – Результаты контрольного эксперимента, группа 3

Исходя из следующих обработанных данных по группам 3 (экспериментальная и контрольная), интерпретация результатов следующая:

– задача 1: справилось 2 участника, которые прошли через главный вход колледжа под разными предлогами (забыл студенческий билет, вызвали в учебную часть «ЧелГУ» - записали данные паспорта);

– задача 2: мониторы системы видеонаблюдения расположили в отличную сторону от первоначального варианта, тем самым скрыли из общего поля зрения данную информацию, в итоге с заданием справился 1 человек;

– задача 3: была проведена профилактическая беседа с персоналом по вопросу «информационная безопасность», в связи с этим задачу выполнили 2 участника;

– задача 4: с данным заданием справился 1 участник, который воспользовался персональным компьютером в библиотеке колледжа, так как в данном помещении отсутствует какой-либо контроль;

– задача 5: с заданием справилось 2 участника, так как сотрудник охраны осуществляет контроль за внутренней организацией безопасности на физическом уровне.

Таким образом, исходя из полученных результатов и сравнения групп категорий «Э» и «К», можно сделать вывод о том, что предложенные и принятые меры по информационной безопасности в колледже по большей мере изменили обстановку в лучшую сторону. Таким образом, вероятность угроз выглядит, следующим образом:

- снижение на 2 пункта состоялось в 1 случае;
- на 1 пункт в 10 случаях;
- осталось неизменным в 3 случаях;
- вероятность возросла в 1 случае.

Следовательно, чтобы минимизировать еще вероятность реализации угроз, необходимо продолжить работу по направлению информационной безопасности в колледже.

Выводы по главе 2

Во второй главе магистерской диссертации мы провели экспериментальную работу по апробации комплекса мер по совершенствованию методов обеспечения информационной безопасности в профессиональной образовательной организации.

В первом параграфе, произвели анализ единого информационного пространства базы исследования, в ходе которого выделили организационную структуру колледжа с его функциональным назначением ролей, а также состав учебно-материальной, учебно-лабораторной и информационно-технической базы. Создали рабочую группу, в составе которой определили, что уровень исходной защищенности информационных систем персональных данных колледжа очень низок и согласно оценке угроз, актуальными угрозами в системе безопасности являются: утечки акустической и видовой информации; утечки по каналу побочных электромагнитных излучений и наводок; угрозы, реализуемые после загрузки операционной системы; внедрение вредоносных программ и угрозы типа «Отказ в обслуживании»; выявление паролей и внедрение по сети вредоносных программ. Также, помимо комплексной оценки был проведен эксперимент, в ходе которого ранее полученные результаты оценки были подтверждены.

Во втором параграфе, предложили и внедрили комплекс мероприятий по совершенствованию методов обеспечения информационной безопасности в колледже на основании выявленных ранее угроз в параграфе 1 главы 2, а именно: установили при главном входе в организацию рамку металлоискателя, заключили договор с охранной организацией, ограничили доступ к техническому подъезду столовой, установили доводчики на дверях, закупили новые персональные компьютеры для одного компьютерного класса, осуществили частичную перепланировку помещений и оборудования, начали работу по настройке и модернизации локальной вычислительной сети.

В третьем параграфе, провели повторную оценку уровня защищенности системы безопасности колледжа, после внедренного комплекса мероприятий, которая в результате изменила статус с низкого до среднего уровня защищенности, а количество опасности угроз в ИСПДн снизилось с 8 до 5. Результаты повторно проведенной оценки, также были подтверждены экспериментально, что дало возможность сравнить на графиках результаты экспериментальных и контрольных групп по каждой карточке заданий, а также проследить за их динамикой.

ЗАКЛЮЧЕНИЕ

В теоретической части магистерской диссертации рассмотрены основные положения проблематики обеспечения информационной безопасности в профессиональной образовательной организации.

Автором предложено определение информационной безопасности в профессиональной образовательной организации, как состояние защищенности информационного пространства учебной организации с учетом защиты ее объектов (обучающихся) от запрещенной законом информации.

Проанализированы статистические данные о количестве преступлений (с 2018г. по 2021г.), совершенных с использованием информационно-телекоммуникационных технологий. Выявлены нововведения и корректировки в законодательстве по следующим направлениям: цифровые экономические отношения, национальная безопасность, импортозамещение, защита информации, биометрия, персональные данные, средства криптографической защиты информации и аттестация объектов информатизации.

Описаны цели защиты информации: предотвращение, воспрещение, сохранение и соблюдение.

Рассмотрены уровни информационной безопасности в профессиональной образовательной организации: законодательно-правовой, административный и программно-технический.

Установлены основополагающие факторы уязвимостей в системе безопасностей образовательных учреждений: некорректная настройка оборудования, использование нелицензированного программного обеспечения и не компетентность персонала.

Классифицированы и подробно рассмотрены актуальные уязвимости по классам (объективные, случайные и субъективные), а также угрозы по определенным признакам: природе возникновения и степени преднамеренности проявления, непосредственному источнику угроз и его

положению, степени зависимости от активности системы и воздействия на нее, этапам доступа пользователей или программ к ресурсам системы, способу доступа к ресурсам системы и текущему месту расположения информации.

Выявлены области защиты информации: организационная, инженерно-техническая, аппаратные и программные средства.

Исследование теоретико-методических основ обеспечения информационной безопасности позволило получить более обширное представление об исследуемой проблематике: основные положения и цели защиты информации, способы регулирования государством преступлений с использованием информационных технологий, уровни информационной безопасности, основные виды угроз и причины уязвимостей, современные методы защиты.

Практическая часть магистерской диссертации была посвящена экспериментальной работе по апробации комплекса мер по совершенствованию методов обеспечения информационной безопасности в профессиональной образовательной организации. В соответствии с целью, предметом, гипотезой и задачами данного исследования экспериментальная работа проводилась в три этапа.

На первом этапе было проанализировано единое информационное пространство ГБПОУ «Южно-Уральский государственный колледж» (Кыштымский филиал). Собрана рабочая группа в составе которой был определен уровень исходной защищенности ИСПДн – Y1 равен 10, что означает низкую степень. Проведена оценка актуальных угроз ИСПДн колледжа, в ходе которой были выявлены следующие угрозы: утечки акустической и видовой информации, утечки по каналу побочных электромагнитных излучений и наводок, угрозы внедрения вредоносных программ, угрозы типа «Отказ в обслуживании» и выявления паролей, внедрение по сети вредоносных программ.

Также, помимо комплексной объективной оценки, был проведен эксперимент. Цель которого заключалась в том, чтобы определить на сколько

результаты анализа ИСПДн были точны и актуальны. По итогу цель была достигнута и результаты анализа подкреплены проведенным экспериментом.

На втором этапе исследования был разработан и внедрен комплекс мероприятий по совершенствованию методов обеспечения информационной безопасности, а также методические рекомендации по организации профилактических мероприятий в колледже на основании результатов параграфа 1 главы 2.

На третьем этапе экспериментальной работы была проведена контрольная оценка эффективности внедренного комплекса мероприятий по совершенствованию методов обеспечения информационной безопасности в профессиональной образовательной организации. Уровень исходной защищенности вырос с низкой до средней степени. Количество угроз сократилось с 8 до 5. Определена динамика вероятности угроз, результаты которой следующие:

- снижение на 2 пункта состоялось в 1 случае;
- на 1 пункт в 10 случаях;
- осталось неизменным в 3 случаях;
- вероятность возросла в 1 случае.

Таким образом, на основании вышеизложенного мы можем сделать вывод о том, что гипотеза исследования полностью подтвердилась, поставленная цель исследования достигнута, необходимые задачи решены.

Подводя итоги нашего исследования, необходимо отметить, что рассматриваемая проблема на базе исследования не исчерпала себя в полной мере. Дальнейшую работу можно продолжить все также по следующим существующим угрозам:

- угрозы утечки акустической (речевой) информации;
- угрозы, реализуемые после загрузки операционной системы;
- угрозы внедрения вредоносных программ;
- угрозы типа «Отказ в обслуживании»;
- угрозы внедрения по сети вредоносных программ.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Александрова, А.В. Информационная безопасность и конституционные права личности: статья [Текст] / А.В. Александрова, Е. И. Образумов. — Пенза: Изд-во Пенз. гос. ун-та., научный журнал «Наука. Общество. Государство», 2021. — №1. — с. 63-70.

2. Алешкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности): учебное пособие [Текст] / А.С. Алешкин, С.А. Лесько, Д. О. Жуков. — Москва: РТУ МИРЭА, 2020. — 152 с.

3. Баранова, Е.К. Основы информационной безопасности: учебник [Текст] / Е.К. Баранова, А.В. Бабаш. - ИНФРА-М, 2019. — 202 с.

4. Бедеров, И.С. Рост ИТ-преступности [Электронный ресурс]. URL: https://интернет-розыск.рф/blog/58 (дата обращения: 09.12.2022).

5. Безопасность предприятий: ключевые угрозы и средства защиты [Электронный ресурс]. URL: https://habr.com/ru/post/529178/ (дата обращения: 19.05.2023).

6. Введение. Сущность и понятие информационной безопасности [Электронный ресурс]. URL: https://studfile.net/preview/5150160/ (дата обращения: 13.12.2022).

7. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов [Текст] / Е.В. Вострецова. — Екатеринбург: Изд-во Урал. ун-та, 2019. — 204 с.

8. Галяутдинов, Р.Р. Информационная безопасность. Виды угроз и защита информации [Электронный ресурс]. URL: https://galyautdinov.ru/post/informacionnaya-bezopasnost (дата обращения: 30.05.2023).

9. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200058320 (дата обращения 08.12.2022).

10. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200075565 (дата обращения: 10.12.2022).

11. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем [Электронный ресурс]. URL: https://intelbit.ru/upload/iblock/119/r1u0umnn6sh70s6vh1w9qrudtql4xmtw.pdf (дата обращения: 30.05.2023).

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

13. Доктрина об информационной безопасности Российской Федерации, указ президента Российской Федерации В. В. Путина от 5 декабря 2016г. [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200075565 (дата обращения: 10.12.2022).

14. Евкова, А.А. Цели, задачи и принципы информационной безопасности [Электронный ресурс]. URL: https://www.evkova.org/kursovye-raboty/tseli-zadachi-i-printsipyi-informatsionnoj-bezopasnosti (дата обращения: 16.12.2022).

15. Ермакова, А. Ю. Методы и средства защиты компьютерной информации: учебное пособие [Текст] / А. Ю. Ермакова. — Москва: РТУ МИРЭА, 2020. — 223 с.

16. Ерохин, В.В. Безопасность информационных систем: учебное пособие [Текст] / В.В. Ерохин, Д.А. Погонышева, И.Г. Степченко. — Москва: Флинта, 2022. — 184 с.

17. Информационная безопасность [Электронный ресурс]. URL: https://shkolaartezianskaya-r08.gosweb.gosuslugi.ru/roditelyam-i-uchenikam/poleznaya-informatsiya/informatsionnaya-bezopasnost/ (дата обращения: 08.12.2022).

18. Информационная безопасность [Электронный ресурс]. URL: https://searchinform.ru/informatsionnaya-bezopasnost/ (дата обращения: 19.05.2023).

19. Информационная безопасность и защита информации [Электронный ресурс]. URL: https://www.sites.google.com/site/inftech11/home/sam/materialy-lekcii-informacionnaa-bezopasnost-i-zasita-informacii (дата обращения: 09.12.2022).

20. Ищейнов В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие [Текст] / В. Я. Ищейнов, М. В. Мецатунян. — Москва: ФОРУМ: ИНФРА-М, 2021. — 216с.

21. Капгер, И.В. Управление информационной безопасностью: учебное пособие [Текст] / И.В. Капгер, А.С. Шабуров. — Пермь: ПНИПУ, 2023. — 91с.

22. Карпухин, Е. О. Технологии и методы защиты инфокоммуникационных систем и сетей: учебное пособие [Текст] / Е.О. Карпухин — Москва: Горячая линия-Телеком, 2021. — 120 с.

23. Каширская, Е. Н. Защита информации в информационно - управляющих системах: учебное пособие [Текст] / Е. Н. Каширская, М. А. Макаров. — Москва: РТУ МИРЭА, 2020. — 67 с.

24. Классификация угроз безопасности информации. Классификация каналов утечки информации [Электронный ресурс]. URL: https://zpdn.dzamba.ru/index.php?page=22&type=1 (дата обращения: 30.05.2023).

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

26. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) [Электронный ресурс]. URL: http://www.consultant.ru/ (дата обращения 29.05.2023).

27. Короченцев, Д.А. Импортозамещающие технологии обеспечения информационной безопасности и защиты данных: учебное пособие [Текст] / Д. А. Короченцев, Л. В. Черкесова, Е. А. Ревякина. — Ростов-на-Дону: Донской ГТУ, 2021. — 335 с.

28. Краковский, Ю.М. Методы защиты информации: учебное пособие для вузов [Текст] / Ю.М. Краковский. — Санкт-Петербург: Лань, 2021. — 236 с.

29. Ксендзов, А.В. Защищенные системы передачи информации: учебное пособие [Текст] / А.В. Ксендзов. — Рязань: РГРТУ, 2021. — 96 с.

30. Мандрица, И.В. Управление проектами по информационной безопасности и экономика защиты информации. Часть 1: учебник для вузов [Текст] / И.В. Мандрица, В.И. Петренко, О.В. Мандрица. — Санкт-Петербург: Лань, 2023. — 124 с.

31. Маршаков, Д.В. Программно-аппаратные средства защиты информации: учебное пособие [Текст] / Д.В. Маршаков, Д.В. Фатхи. — Ростов-на-Дону: Донской ГТУ, 2021. — 228 с.

32. Метод оценки экономической эффективности подразделения по защите информации [Электронный ресурс]: URL: https://lib.itsec.ru/articles2/Oborandteh/metod-ocenki-ekonomicheskoieffektivnosti-podrazdeleniya-po-zashite-informacii (дата обращения 02.06.2023).

33. Методы и средства защиты информации: коммерческой тайны и персональных данных [Электронный ресурс]. URL: https://mcs.mail.ru/blog/metody-i-sredstva-zashchity-informacii-personalnyh-dannyh (дата обращения: 06.06.2023).

34. Методы и приемы обеспечения информационной безопасности [Электронный ресурс]. URL: http://med-sayansk.ru/wp-content/uploads/2020/05/12.05.20-2B-Lektsiya-15.-Metody-i-priemy-obespecheniya-informatsionnoj-bezopasnosti.pdf (дата обращения: 04.06.2023).

35. Минаев, Г. А. Образование и безопасность: учебное пособие [Текст] / Г. А. Минаев. — Москва: Логос, 2020. — 312 с.

36. Михнев, И.П. Информационная безопасность: учебное пособие [Текст] / И.П. Михнев. — Волгоград: Изд-во Волгоградского института управления – филиала РАНХиГС, 2019. — 82 с.

37. Мошенничество в сети: судебная практика и ключевые аспекты [Электронный ресурс]. URL: https://rtmtech.ru/research/online-fraud-research/ (дата обращения: 09.12.2022).

38. Нечай, А.А. Составляющие информационной безопасности [Электронный ресурс]. URL: https://infourok.ru/konspekt-po-discipline-ib-na-temu-sostavlyayuschie-informacionnoy-bezopasnosti-2839892.html (дата обращения: 20.05.2023).

39. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений: учебное пособие для СПО [Текст] / С. Н. Никифоров. — Санкт-Петербург: Лань, 2021. — 96 с.

40. Нурматова, Е.В. Инструменты и методы безопасного хранения данных: учебное пособие [Текст] / Е.В. Нурматова. — Москва: РТУ МИРЭА, 2021. — 64 с.

41. Поздняк, И. С. Управление информационной безопасностью: методические указания [Текст] / И. С. Поздняк, И. С. Макаров. — Самара: ПГУТИ, 2019. — 43 с.

42. Понятие, сущность, цели и значение защиты информации [Электронный ресурс]. URL: https://textarchive.ru/c-2525943.html (дата обращения: 14.12.2022).

43. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержден приказом ФСТЭК России от 29 апреля 2021 г. № 77 [Электронный ресурс]. URL: https://docs.cntd.ru/document/608228209 (дата обращения: 03.07.2023).

44. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации, утверждены решением Государственной технической комиссии при Президенте РФ от 25 июля 1997г [Электронный ресурс]. URL: https://docs.cntd.ru/document/901817222 (дата обращения: 16.07.2023).

45. Средства защиты информации [Электронный ресурс]. URL: https://www.gd.ru/articles/8803-zashchita-informatsii (дата обращения: 02.06.2023).

46. Стратегия повышения финансовой грамотности в Российской Федерации на 2017-2023 годы, утверждена распоряжением Правительства Российской Федерации от 25 сентября 2017 г. № 2039-р. [Электронный ресурс]. URL: https://docs.cntd.ru/document/436770389 (дата обращения 04.05.2023).

47. Технологии защиты информации в компании [Электронный ресурс]. URL: https://assistentus.ru/vedenie-biznesa/tehnologii-zashchity-informacii/ (дата обращения: 03.02.2023).

48. Трофимова, Н. Б. Кибербезопасность: информационная безопасность обучающихся в сети Интернет. Профилактика суицидальных рисков у детей и подростков: учебное пособие [Текст] / Н. Б. Трофимова, Е. М. Беспаленко. — Воронеж: ВГПУ, 2022. — 68 с.

49. Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» № 351 от 17 марта 2008 года [Электронный ресурс]. URL: https://base.garant.ru/192944/ (дата обращения: 13.12.2022).

50. Управление Генеральной прокуратуры Российской Федерации по Центральному федеральному округу Статданные о преступлениях, совершенных с использованием современных информационно-телекоммуникационных технологий от 27 января 2023г [Электронный ресурс].

URL: https://epp.genproc.gov.ru/web/proc_cfo/mass-media/news/archive?item=84860550 (дата обращения: 16.12.2022).

51. Уровни информационной безопасности [Электронный ресурс]. URL: https://cisoclub.ru/urovni-informaczionnoj-bezopasnosti/ (дата обращения: 21.05.2023).

52. Участие в разработке концепции электронного распространения правовой информации. Приложение 1 [Электронный ресурс]. URL: https://www.consultant.ru/about/nc/legalinfo/doklad/addition1/ (дата обращения: 11.02.2023).

53. Факторы уязвимости информационной технической системы [Электронный ресурс]. URL: https://natural-sciences.ru/ru/article/view?id=27099 (дата обращения: 30.05.2023).

54. Федеральный закон «О безопасности» от 28 декабря 2010 г. № 390-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_108546/ (дата обращения: 09.03.2023).

55. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 30.05.2023).

56. Федеральный закон РФ «Об информации, информатизации и защите информации» от 20 февраля 1995 г. №24-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_5887/ (дата обращения: 03.12.2022).

57. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 14.12.2022).

58. Фот, Ю. Д. Методы защиты информации: учебное пособие [Текст] / Ю. Д. Фот. — Оренбург: ОГУ, 2019. — 230 с.

59. Шарафутдинова, А.Р. Защита информации в образовательных учреждениях / А.Р. Шарафутдинова, В.С. Пядышева [Электронный ресурс]. URL: http://www.rusnauka.com/17_APSN_2013/Matemathics/2_140911.doc.htm (дата обращения: 23.05.2023).

60. Ярочкин, В.И. Информационная безопасность: учебник для вузов [Текст] / В.И. Ярочкин. — Москва: Академический Проект, 2020. — 544 с.

Приложение 1

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

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ПРОФИЛАКТИЧЕСКИХ МЕРОПРИЯТИЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГБПОУ «ЮУГК» КФ

Разработал:
Магистрант группы ЗФ-309/210-2-1
Рыбакова Юлия Максимовна

Челябинск
2025

СОДЕРЖАНИЕ

1 МЕТОДЫ ВЫЯВЛЕНИЯ И УСТРАНЕНИЯ НЕКОМПЕТЕНТНОСТИ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОЛЛЕДЖА

Важным требованием обеспечения деятельности образовательного учреждения является поддержание высокого уровня информационной безопасности. Информационная безопасность образовательного учреждения представляет собой комплекс мер различного характера, направленных на реализацию двух основных целей:

– защита персональных данных и информационного пространства от несанкционированных вмешательств, хищения информации и изменения конфигурации системы со стороны третьих лиц;

– защита учащихся от любых видов пропаганды, запрещенной законом.

Информационная безопасность в современной образовательной среде в соответствии с действующим законодательством предусматривает защиту сведений и данных, относящихся к следующим трем группам:

– персональные данные и сведения, которые имеют отношения к учащимся, преподавательскому составу, персоналу организации, оцифрованные архивные документы;

– обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения учебного процесса;

– защищенная законом интеллектуальная собственность.

Таким образом, основными задачами для выявления и устранения некомпетентности пользователей являются:

– определение действенных методов нахождения пробелов в знаниях информационной безопасности;

– оценка способов устранения этих пробелов;

– анализ результатов повышения грамотности в области информационной безопасности.

Наиболее распространенными угрозами безопасности, с которыми сталкиваются пользователи информационных систем образовательных организаций являются:

– общедоступность персональных паролей;

– не соблюдение разграничения прав доступа к информации;

– рассылки фишинговых писем, не умение пользоваться программными средствами защиты информации.

Первым этапом по определению пробелов пользователей в области информационной безопасности необходимо провести анкетирование персонала на знание основных принципов защиты информации, тест предлагается реализовать в следующем ключе – таблица 1.

Таблица 1 – Тестирование по основам информационной безопасности

№	Вопрос	№	Вопрос
1	*Сложность обеспечения информационной безопасности является следствием:* А) невнимания широкой общественности к данной проблематике Б) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним В) все большей зависимости общества от информационных систем	16	*В число архитектурных принципов, направленных на обеспечение высокой доступности информационных сервисов, входят:* А) автоматизация процессов Б) невозможность обхода защитных средств В) управляемость процессов, контроль состояния частей
2	*Сервисы безопасности подразделяются на:* А) буферизующие, сглаживающие злоумышленную активность Б) глобализующие, расширяющие зону поиска нарушителя В) локализующие, сужающие зону воздействия нарушений	17	*Согласно стандарту X.700, в число функций управления отказами входят:* А) изоляция отказов Б) предупреждение отказов В) выявление отказов

Продолжение таблицы 1

3	*В число основных принципов архитектурной безопасности входят:* А) укрепление наиболее вероятного объекта атаки Б) усиление самого слабого звена В) эшелонированность обороны	18	*К какой категории персональных данных относится отпечаток пальца в соответствии с ФЗ "О персональных данных"?* А) биометрические персональные данные Б) общедоступные персональные данные В) специальные персональные данные
4	*Средний ущерб от компьютерного преступления в США составляет примерно:* А) сотни тысяч долларов Б) копейки В) десятки долларов	19	*Согласно "Оранжевой книге", политика безопасности включает в себя следующие элементы:* А) логическое управление доступом Б) принудительное управление доступом В) произвольное управление доступом
5	*Эффективность информационного сервиса может измеряться как:* А) максимальное время обслуживания запроса Б) рентабельность работы сервиса В) количество одновременно обслуживаемых пользователей	20	*Обеспечение информационной безопасности зависит от:* А) системных и сетевых администраторов Б) руководства организаций В) пользователей
6	*В число целей политики безопасности верхнего уровня входят:* А) формулировка целей, которые преследует организация в области информационной безопасности Б) определение правил разграничения доступа В) определение общих направлений в достижении целей безопасности	21	*Доступность достигается за счет применения мер, направленных на повышение:* А) дисциплинированности Вариант 2 лояльности Вариант 3 безотказности
7	*Политика безопасности строится на основе:* А) изучения политик родственных организаций Б) анализа рисков В) общих представлений об ИС организации	22	*В рамках программы безопасности нижнего уровня осуществляются:* А) повседневное администрирование Б) отслеживание слабых мест защиты В) стратегическое планирование
8	*Окно опасности перестает существовать, когда:* А) заплата устанавливается в защищаемой ИС Б) администратор безопасности узнает об угрозе В) производитель ПО выпускает заплату	23	*Дублирование сообщений является угрозой:* А) целостности Б) доступности В) конфиденциальности

Продолжение таблицы 1

9	*Самыми опасными источниками угроз являются:* А) внешние Б) пограничные В) внутренние	24	*В число возможных стратегий нейтрализации рисков входят:* А) ликвидация риска Б) игнорирование риска В) принятие риска
10	*В число этапов жизненного цикла информационного сервиса входят:* А) спецификация прав человека Б) эксплуатация В) выведение из эксплуатации	25	*Экранирование может использоваться для:* А) обнаружения нарушений Б) локализации последствий нарушений В) предупреждения нарушений ИБ
11	*В число универсальных сервисов безопасности входят:* А) экранирование Б) средства построения виртуальных локальных сетей В) протоколирование и аудит	26	*Выявление неадекватного поведения выполняется системами управления путем применения методов, типичных для:* А) систем активного аудита Б) систем анализа защищенности В) систем идентификации
12	*Согласно Закону "О лицензировании отдельных видов деятельности", лицензия, это:* А) специальное разрешение на осуществление конкретного вида деятельности Б) удостоверение, подтверждающее высокое качество изделия В) документ, гарантирующий безопасность программного продукта	27	*Что из перечисленного не относится к числу основных аспектов информационной безопасности:* А) конфиденциальность Б) масштабируемость В) доступность Г) целостность
13	*Согласно рекомендациям X.800, выделяются следующие сервисы безопасности:* А) туннелирование Б) аутентификация В) идентификация	28	*На межсетевые экраны целесообразно возложить следующие функции:* А) верификация прикладного программного обеспечения Б) верификация базового программного обеспечения В) верификация Java-аплетов
14	*Как называется обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя в соответствии с Законом "Об информации, информационных технологиях и о защите информации"?* А) доступность информации Б) целостность информации В) конфиденциальность информации	29	*Какой вид подписи будет у подписи, ключ проверки которой указан в квалифицированном сертификате?* А) усиленная неквалифицированная электронная подпись Б) простая электронная подпись В) усиленная квалифицированная электронная подпись

Продолжение таблицы 1

15	*Уровень риска является функцией:* А) вероятности реализации угрозы Б) стоимости защитных средств В) числа уязвимостей в системе	30	В качестве аутентификатора в сетевой среде могут использоваться: А) кардиограмма субъекта Б) результат работы генератора одноразовых паролей В) номер карточки пенсионного страхования

Затем производится проверка данного теста и оглашение работникам результатов. Далее предлагается произвести проверку пользователей на практическое выполнение вопросов:

– рассылка проверочных фишинговых писем с дальнейшим выявлением «попавшихся»;

– просмотр журналов смены паролей в АСУ ProCollege;

– наблюдение за пользователями на предмет оставления рабочих компьютеров без присмотра, распространения личных паролей и т.п.;

– контроль использования рабочих электронных почтовых ящиков.

В завершении проверочных мероприятий проводится подробный инструктаж по информационной безопасности не прошедших проверку пользователей, после чего такие сотрудники направляются на прохождение онлайн курса на платформе «Интуит» - «Основы информационной безопасности».

Все подобные мероприятия рекомендуется проводить не реже одного раза в год, а также при появлении новых пользователей информационной системы, независимо от того штатный это сотрудник или совместитель.

Безопасность информационной системы организации один из ключевых показателей стабильности ее работы, об этом стоит помнить всем, начиная от руководства и заканчивая рядовыми пользователями. Основной задачей руководства является донесение важности этого показателя, своевременное обнаружение слабых звеньев и устранение пробелов знаний персонала в этой области.

2 РАЗГРАНИЧЕНИЕ ПРАВ ДОСТУПА К ОБРАБАТЫВАЕМЫМ ПЕРСОНАЛЬНЫМ ДАННЫМ В КОЛЛЕДЖЕ

Для повышения эффективности системы обеспечения информационной безопасности в первую очередь нужно обеспечить сохранность основных объектов защиты любой образовательной организации – персональных данных и информации для служебного пользования. Для выполнения данной задачи необходимо совершенствовать систему разграничения прав доступа к информации в направлении усиления защиты. Актуальность исследования обусловлена тем, что в случае, если работа системы разграничения прав доступа к данным образовательной организации недостаточно налажена, при использовании автоматизированных рабочих мест (АРМ) сотрудниками организации возможен несанкционированный доступ к информации (НСД) лиц, не допущенных к процессу обработки ПДн и информации для служебного пользования.

В первую очередь необходимо организовать список о разграничении прав доступа к обрабатываемым персональным данным в ГБПОУ «ЮУГК» КФ в соответствии с Федеральным законом от 27 июня 2006г. № 152-ФЗ «О персональных данных» и правилами внутреннего трудового распорядка колледжа, которые определяют уровень доступа должностных лиц к персональным данным работников и обучающихся.

Таблица 2 – Список лиц ответственных за автоматизированную и неавтоматизированную обработку персональных данных

Группа	Уровень доступа к ПДн	Разрешенные действия
Администрация колледжа (Руководитель филиала, заместители)	1) Обладает полной информацией о персональных данных обучающихся и их родителей, работников филиала 2) Имеет доступ к личным делам обучающихся и работников, информации на материальных носителях, содержащей персональные данные	1) Сбор и систематизация 2) Хранение и накопление 3) Обновление, изменение 4) Использование 5) Уничтожение 6) Распространение 7) Блокирование 8) Обезличивание

Продолжение таблицы 2

Группа	Уровень доступа к ПДн	Разрешенные действия
Специалист по кадрам	1) Обладает полной информацией о персональных данных работников филиала 2) Имеет доступ к личным делам работников, информации на материальных носителях, содержащей персональные данные	
Социальный педагог, педагог-психолог	Имеет доступ к личным делам обучающихся, информации на материальных носителях, содержащей персональные данные обучающихся и их представителей	1) Сбор и систематизация 2) Хранение и накопление 3) Обновление, изменение 4) Использование
Классный руководитель	Имеет доступ к личным делам обучающихся и информации на материальных носителях, содержащей персональные данные обучающихся **только своей группы** и их родителей	1) Сбор и систематизация 2) Хранение и накопление 3) Обновление, изменение 4) Использование 5) Уничтожение
Мастера производственного обучения	Имеет доступ к личным делам обучающихся и информации на материальных носителях (журнал учебной группы), содержащей персональные данные обучающихся и их родителей	
Преподаватель-организатор ОБЖ, допризывной подготовки	Имеет доступ к личным делам обучающихся и информации на материальных носителях, содержащей персональные данные обучающихся допризывного возраста	1) Сбор и систематизация 2) Хранение и накопление 3) Обновление, изменение 4) Использование 5) Уничтожение
Преподаватель	Имеет доступ к информации на материальных носителях (журнал учебной группы), содержащей персональные данные обучающихся и контактные данные родителей обучающихся групп	использование
Секретарь приемной комиссии, зам.председателя приемной комисии	1) Обладает полной информацией о персональных данных абитуриентов и их представителях 2) Имеет доступ к личным делам абитуриентов, обучающихся и информации на материальных носителях, содержащей персональные данные обучающихся, их представителей	1) Сбор и систематизация 2) Хранение и накопление 3) Обновление, изменение 4) Использование 5) Уничтожение 6) Распространение 7) Блокирование

Продолжение таблицы 2

Группа	Уровень доступа к ПДн	Разрешенные действия
Библиотекарь	Имеет доступ к информации на материальных носителях (формуляр читателя библиотеки), содержащей персональные данные обучающихся	1) Использование 2) Хранение
Начальник ХО	Имеет доступ к информации на материальных носителях, содержащие персональные данные работника о фактическом месте проживания и контактные телефоны	использование
Секретарь учебной части	Имеет доступ к информации на материальных носителях (журналы учебных групп), содержащей персональные данные обучающихся и контактной информации родителей обучающихся колледжа	использование
Инженер компьютерных систем и комплексов	1) Обладает полной информацией о персональных данных обучающихся и их родителей, работников филиала 2) Имеет доступ к личным делам обучающихся и работников, информации на материальных носителях, содержащей персональные данные	1) Сбор и систематизация 2) Хранение и накопление 3) Обновление, изменение 4) Использование 5) Уничтожение 6) Распространение 7) Блокирование

Также, для совершенствования системы обеспечения информационной безопасности образовательной организации в части разграничения прав доступа к ПДн возможны следующие варианты:

а) использование организационных мер защиты систем ПДн:

– АРМ, предназначенные для хранения и обработки ПДн, не общедоступны и расположены в физически защищенных помещениях (замок на двери, жалюзи), доступ в помещения имеют только лица, допущенные к обработке ПДн;

– доступ пользователей к системе осуществляется под собственными, известными только владельцу, идентификаторами (логином и паролем), смена паролей осуществляется **не реже одного раза в 3 месяца**;

– доступ АРМ, предназначенного для обработки ПДн, к сети Интернет отсутствует;

– существует возможность использования только рабочих (учтенных) носителей информации, прописанных администратором безопасности в данной системе, вынос носителей информации с территории образовательной организации осуществляется в случаях необходимости по разрешению лица, ответственного за обработку ПДн в организации.

б) комплекс программно-аппаратных и организационных мер совершенствования работы системы разграничения прав доступа к ПДн:

– доступ пользователей к системе осуществляется под собственными, известными только владельцу, идентификаторами (логином и паролем), смена паролей осуществляется **не реже одного раза в 3 месяца**;

– доступ пользователей к каталогам и ресурсам системы разграничен администратором безопасности (согласно таблице 2);

– настройка блокирования системы при отсутствии действий **в течение 15 минут**;

– использование лицензионного программного обеспечения (ПО);

– антивирусное ПО обновляется **не реже 1 раза в месяц**;

– доступ пользователей к сети Интернет ограничен (возможно использование только определенного набора разрешенных интернет сервисов);

– существует возможность использования только рабочих (учтенных) носителей информации, прописанных администратором безопасности в данной системе, вынос носителей информации с территории образовательной организации осуществляется в случаях необходимости по разрешению лица, ответственного за обработку ПДн в организации.

в) использование программных мер защиты ПДн (на примере Kaspersky Total Security Plus). Использование программного продукта, позволяет:

– обеспечить дискреционный принцип контроля доступа к ресурсам системы;

– создание замкнутой программной среды пользователя, позволяющей ему запуск только разрешенных приложений;

– производить регистрацию событий безопасности, в том числе и действий администратора;

– осуществлять маркировку выдаваемых на печать документов независимо от печатающего их приложения;

– обеспечивать гарантированную очистку освобождаемой оперативной памяти, содержимого защищаемых файлов при их удалении, файла(ов) подкачки при завершении работы системы;

– производить контроль целостности защищаемых ресурсов системы и компонентов системы защиты информации;

– управлять носителями информации;

– управлять устройствами;

– производить тестирование системы защиты информации.

В каждом из трех предложенных вариантов решения есть отрицательные моменты, основные из них рассмотрены в таблице 3.

Таблица 3 – Отрицательные стороны предложенных вариантов

№	Организационные меры	Комплекс программно-аппаратных и организационных мер	Программные меры
1	Необходимость использования (закупки) АРМ предназначенных исключительно для обработки ПДн	Необходимость привлечения администратора безопасности	Закупка ПО (336501р на 99 АРМ, лицензия на 1 год)
2	Невозможность работы АРМ в сети Интернет	Закупка носителей информации	Необходимость привлечения администратора безопасности
3	Организация отдельных помещений для работы с АРМ		
4	Необходимость привлечения администратора безопасности		
5	Закупка носителей информации		

3 РЕГЛАМЕНТ ОРГАНИЗАЦИИ ОБСЛУЖИВАНИЯ КОМПЬЮТЕРНОГО ОБОРУДОВАНИЯ ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Регламент технического обслуживания персонального компьютера помогает обеспечивать надлежащее техническое обслуживание и уменьшает риски возникновения неисправностей, а также обеспечивает безопасность и сохранность данных.

3.1 Общие положения.

3.1.1 Регламент организации сервисного обслуживания компьютерного оборудования государственного образовательного учреждения, разработан в соответствии с целевой программой развития системы образования.

3.1.2 Сервисное обслуживание средств вычислительной техники находящихся на балансе образовательного учреждения, осуществляется систематически в соответствии с настоящим регламентом.

3.1.3 Аварийные и ремонтно-восстановительные работы осуществляются немедленно по возникновению потребности в проведении указанных работ.

3.1.4 Сервисное обслуживание программных и технических средств осуществляется строго в соответствии с настоящим регламентом;

3.1.5 Настоящий регламент принимается органом самоуправления образовательного учреждения и утверждается руководителем этой организации.

3.1.6 Настоящий регламент является локальным нормативным актом, регламентирующим деятельность образовательного учреждения.

3.1.7 Настоящий регламент принимается на неопределенный срок. Изменения и дополнения к регламенту принимаются в составе новой редакции органом самоуправления образовательного учреждения и утверждается директором организации. После принятия новой редакции регламента предыдущая редакция утрачивает силу.

3.2 Организация сервисного обслуживания. Сопровождение технических и программных компонентов.

3.2.1 Формами сервисного обслуживания технических компонентов и сопровождения программных компонентов являются:

– профилактическое техническое обслуживание;

– гарантийное обслуживание оборудования, осуществляемое поставщиком или производителем;

– пост гарантийное фирменное обслуживание оборудования;

– модернизация, диагностика неисправностей, плановый ремонт;

– замена расходных материалов (краска, картриджи, тонеры);

– обследование и экспертная оценка оборудования для подготовки к списанию;

– обновление и замена версий;

– выполнение мероприятий антивирусной защиты;

– резервное копирование и восстановление файлов;

– техническое консультирование.

3.2.2 Субъектами сервисного обслуживания технических компонентов и сопровождения программных компонентов являются:

– должностные лица образовательного учреждения;

– работники ремонтных предприятий на основании договоров;

– работники организаций, осуществляющих гарантийное и пост гарантийное фирменное обслуживание на основании договоров.

3.2.3 Должностные лица образовательного учреждения, прошедшие в установленном порядке обучение и проверку знаний в области информационно-коммуникационных технологии (ИКТ) и профилактического обслуживания компьютерного оборудования, а также инструктаж по нормам охраны труда и информационной безопасности, могут самостоятельно осуществлять профилактическое техническое обслуживание и сопровождение программных компонентов в соответствии с настоящим регламентом.

3.2.4 Для учета технических и программных компонентов введется единая информационная система оказания услуг (ЕИС ОУ), подлежащих сервисному обслуживанию, используется специальный «Реестр».

3.2.5 Регламент сервисного обслуживания включает следующие виды и периодичность проведения работ:

– продувка внутренних полостей системного блока, блока питания, радиаторов охлаждения компьютера **1 раз в полгода**;

– чистка экрана монитора, поверхностей системного блока **1 раз в месяц**;

– проверка параметров монитора, восстановление характеристик изображения **1 раз в месяц**;

– проверка работоспособности интерфейсных устройств и носителей информации (CD, FDD - приводы) **1 раз в месяц**;

– - проверка и чистка клавиатуры, манипулятора – «мышь» **1 раз в месяц**;

– проверка работоспособности принтера. Продувка внутренних полостей. Протирка роликов и протяжного механизма **1 раз в полгода**;

– проверка состояния картриджа, тонера, замена картриджа при необходимости;

– проверка работоспособности коммутационного оборудования - систематически.

3.2.6 Регламент профилактического обслуживания включает следующие виды и периодичность проведения работ:

– обновление антивирусного программного обеспечения, проверка устройств постоянного хранения информации **1 раз в неделю**;

– инсталляция программного обеспечения (кроме продуктов, инсталлируемых специалистами производителя или поставщика) по мере поступления программных продуктов;

– проверка и установка критических обновлений безопасности операционной системы **1 раз в месяц** или по мере поступления обновлений;

– установка обновлений программного обеспечения **1 раз в месяц**;

– архивирование и резервное копирование файлов баз данных в соответствии с порядком использования автоматизированным информационными системами управления (АИСУ) и системой управления базами данных(СУБД);

– проверка и дефрагментация жестких дисков **1 раз в месяц**;

– приведение в стандартное состояние профиля пользователей **1 раз в месяц**;

– администрирование сети (регистрация и редактирование пользовательских учетных записей, сетевых прав и ограничений доступа) по мере необходимости;

– структурирование и оптимизация данных **1 раз в неделю**.

3.3 Организация аварийных и ремонтно-восстановительных работ.

3.3.1 Формами аварийных и ремонтно-восстановительных работ с техническими и программными компонентами, выполняемых в образовательном учреждении, являются:

– восстановление работоспособности компьютера;

– замена вышедшего из строя или утратившего номинальные параметры периферийного оборудования;

– восстановление работы локальной вычислительной сети (ЛВС);

– замена коммутационного оборудования;

– восстановление операционной системы, или программного обеспечения.

3.3.2 Субъектами проведения аварийных и ремонтно-восстановительных работ с техническими и программными компонентами единой информационная системой оказания услуг (ЕИС ОУ) в образовательном учреждении являются:

– заместитель директора по учебно-воспитательных работ (УВР) с функциональными обязанностями в области информационно-коммуникационных технологий (ИКТ);

– должностные лица, исполняющие обязанности инженера.

3.3.3 Должностные лица, прошедшие в установленном порядке обучение и проверку знаний в области информационно-коммуникационных технологий (ИКТ) и профилактического обслуживания компьютерного оборудования, а также инструктаж по нормам охраны труда и информационной безопасности, могут самостоятельно осуществлять аварийные и ремонтно-восстановительные работы в соответствии с настоящим регламентом.

3.3.4 Неисправности технических компонентов и нарушение функций программных компонентов единой информационная системой оказания услуг (ЕИС ОУ) учитываются в журнале учета неисправностей.

3.3.5 Регламент аварийных и ремонтно-восстановительных работ, проводимых в образовательном учреждении включает следующие виды работ:

– восстановление работоспособности компьютера после выхода из строя блока питания, жесткого диска, приводов оптических дисков, сетевых, звуковых и видеокарт – **в течение недели** после выявления неисправности;

– замена монитора – **немедленно** с использованием резервного оборудования;

– замена клавиатуры или манипулятора «мышь» - **немедленно** с использованием резервных комплектующих;

– восстановление кабельного соединения рабочей станции и коммутационного устройства – **в течение рабочего дня** после диагностики неисправности;

– восстановление соединения коммутационных устройств с выделенными серверами – **в течение рабочего дня** после диагностики неисправности;

– замена вышедших из строя концентраторов, коммутаторов - **немедленно** с использованием резервного оборудования;

– замена роутера – **немедленно** после закупки и настройки оборудования **в течение недели** после выявления неисправности;

– замена источников бесперебойного питания – **немедленно** с использованием резервного оборудования;

– восстановление настроек выделенных серверов – **в течение недели** после выявления неисправности;

– восстановление или замена операционной системы компьютера – **в течение 3 рабочих дней**;

– восстановление вышедшего из строя программного обеспечения - **немедленно** после выявления неисправности.

3.3.6 Модернизация оборудования, связанная с установкой дополнительных жестких дисков или жестких дисков большего объема, приводов оптических дисков, сетевых или видеокарт, а также с заменой операционных систем также выполняется в образовательном учреждении должностными лицами, перечисленными в п. 3.3.2. Иные виды ремонтно-восстановительных работ выполняются с привлечением специалистов обслуживающих организаций в сроки, определяемые временем приема заказа, проведения платежа и выполнения работ.

3.4 Обеспечение замены комплектующих и расходных материалов.

3.4.1 Постоянно потребляемые комплектующие (картриджи, клавиатуры, манипуляторы «мышь»), а также расходные материалы (бумага, кабели, разъемы, записываемые CD и DVD диски) приобретаются в количествах, необходимых для поддержания работоспособности оборудования с учетом среднестатистических данных за учебный год.

3.4.2 Комплектующие, необходимые для проведения аварийных или ремонтно-восстановительных работ в образовательном учреждении (блоки питания, жесткие диски, приводы оптических дисков, сетевые карты, видеокарты) приобретаются по мере возникновения потребности, связанной с проведением аварийных или ремонтно-восстановительных работ, а также с модернизацией оборудования по плану развития единой информационной системой оказания услуг (ЕИС ОУ).

3.4.3 Учет поступления и использования расходных материалов осуществляется в специальном журнале.

3.4.4 Учет комплектующих осуществляется бухгалтерской службой в порядке учета нефинансовых активов.

3.4.5 Списание потребленных без остатка расходных материалов и комплектующих проводится в установленном порядке в соответствии с учетной политикой образовательного учреждения. В настоящем регламенте излагаются порядок и правила выполнения работ по техническому обслуживанию ПК. При выполнении технического обслуживания должны дополнительно использоваться эксплуатационные документы на изделия, входящие в состав ПК. Техническое обслуживание проводится в отношении оборудования, состоящих на балансе хозяйственного управления, так же направлено на обеспечение постоянной готовности оборудования к использованию по прямому назначению и предотвращение преждевременного выхода его из строя. Изменение состава обслуживаемого оборудования или его перемещение производится по заявке специалистов отделов информатизации с занесением информации в формуляр изделия. В случае выявления дефектов, которые не могут быть устранены на площадке пользователя, оборудование (с согласия материально-ответственного лица, пользователя) изымается сотрудником отдела технических средств для ремонта в лабораторных условиях. При возникновении необходимости изъятия средства вычислительной техники с рабочего места для ремонта или настройки больше чем на четыре часа, должна быть составлена ремонтная карта об изъятии данного оборудования с описанием работ, с указанием даты, времени изъятия, за подписью пользователя или лица ответственного за его эксплуатацию и лица, производящего изъятие. Взамен изъятого средства вычислительной техники на рабочее место, если имеется возможность, выставляется оборудование из обменного фонда средств вычислительной техники, с занесением соответствующих записей в формуляр изделия. Если в процессе проведения технического обслуживания выявляются факты нарушения правил технической эксплуатации оборудования или правил техники безопасности пользователем, специалист, производящий техническое

обслуживание, должен принять соответствующие меры к их немедленному устранению и недопущению впредь, и в установленном порядке проинформировать об этом руководителя соответствующего структурного подразделения.

3.4.6 Состав работ, входящих в техническое обслуживание по видам оборудования. Подробное описание состава работ, в соответствии с видом оборудования, фиксируется исполнителем данных работ в соответствующей графе ремонтной карты:

- очистка от пыли и грязи внутренних объемов с разборкой;
- проверка работоспособности устройств на тестах в ускоренном режиме;
- проведение дефрагментации накопителей на жестких магнитных дисках;
- полное тестирование всех устройств ПК;
- полная проверка дисковой памяти на наличие вирусов.

Таблица 4 – Пример ремонтной карты

Дата и время поступления	13.07.2024, 10:30
Кабинет оборудования	304
Вид оборудования Серийный номер Инвентарный номер	Системный блок Серийный NASJ405112 Инвентарный N 1101041193
Характер и подробное описание заявки	Постоянно требует синхронизации
Неисправность	
Состав работы (подробное описание)	Тестирование системы
Израсходованные материалы	
Исполнитель	Копылов Александр Юрьевич
Дата и время выдачи заявки	13.07.2024, 11:00
Дата приема оборудования	
Дата исполнения (возврата оборудования)	
Подпись ответственного за эксплуатацию оборудования (ФИО, должность, тел.)	

Приведенные в таблице 4 данные указывают на факт выполнения технического обслуживания. Услуги должны оказываться в соответствии с законодательством Российской Федерации, в том числе в соответствии с:

– «ГОСТ12.1.030-81. Система стандартов безопасности труда. Электробезопасность. Защитное заземление. Зануление»;

– «ГОСТ 12.2.007.0-75. Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности»;

– «ГОСТР 50571.3-2009 (МЭК 60364-4-41:2005). Национальный стандарт Российской Федерации. Электроустановки низковольтные. Часть 4-41. Требования для обеспечения безопасности. Защита от поражения электрическим током»;

– «ГОСТ Р 53245-2008. Информационные технологии. Системы кабельные структурированные. Монтаж основных узлов системы. Методы испытания».

Исполнитель должен оказывать услуги таким образом, чтобы исключить возможность нанесения вреда оборудованию, обеспечивать соответствие качества оказанных услуг требованиям, предъявляемым к качеству услуг такого рода, а также рекомендациям и требованиям производителя оборудования. Все услуги должны оказываться своевременно, качественно.