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

Обеспечение информационной безопасности использования виртуальных сред для образовательных целей колледжа

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:
69 % авторского текста

Работа рекомендована к защите
«30» января 2024 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Винник Евгений Александрович

Научный руководитель:
к.п.н., доцент
Диденко Галина Александровна

Челябинск
2024

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Необходимостью использования контроля во всех сферах деятельности человека, общества и государства обуславливается огромное распространение виртуальных технологий. Приоритетный порядок представляется информатизации всех сфер профессионального образования.

В направленности на основные тренды экономики и процессы развития капитала человека заключается общемировой прогресс, в котором полноценными участниками прогресса будут в совершенстве владеющие цифровыми навыками.

Реализация программы «Цифровая экономика РФ» от 28 июля 2017 г. № 632-р, предъявляет существенные требования к СПО.

В соответствии с 68 статьей ФЗ РФ «Об образовании в Российской Федерации» от 29.12.2012 N 273-ФЗ, для удовлетворения потребностей государства, общества и личности при подготовке квалифицированных кадров в системе СПО реализуется интеллектуальное и профессиональное развитие.

Для создания условий развития в современных условиях необходимо создавать в образовательных учреждениях СПО безопасную виртуальную среду, которая при внедрении современных подходов и технологий, будет повышать цифровую грамотность обучающихся.

Понятие «виртуальной среды в профессиональной образовательной организации» определяет образовательную среду, в которой за счет интенсивного применения цифровых технологий подвержена процессам цифровизации, как виртуальную образовательную среду.

Президент Российской Федерации Путин В.В. в стратегии развития образования поставил задачу о необходимости внедрения современных цифровых образовательных технологий (далее ЦОС) и регламентацию их внедрения

в учебно-воспитательный процесс образовательных учреждений. Виртуальная образовательная среда является составной частью ЦОС.

На основании нормативно-правовой документации в сфере среднего профессионального образования обоснована актуальность данного исследования. При реализации в образовательных учреждениях СПО регионального проекта «Цифровая образовательная среда» выделяют реализацию мероприятий

- при реализации образовательного процесса необходимо учитывать особенности работы виртуальной образовательной среды в системе профессионального образования;

-проводить образовательный процесс с учетом профильной направленности по каждой профессии и специальности;

-использовать различные виртуальные технологии с учетом мнения обучающихся;

-проводить профессиональные пробы для абитуриентов и обучающихся для ознакомления с современными цифровыми компетенциями;

Чтобы организовать защиту от различных угроз виртуальную образовательную среду в профессиональном учреждении нужно проводить работу в соответствии с требованиями информационной безопасности.

Степень разработанности проблемы. В настоящее время в науке подробно разработана теоретическая основа процессов виртуальных образовательных сред и рассматривается в работах

Проблема информатизации и цифровизации образования представлена в работах Андреева А.А., Афониной Е.С., Богатыревой Ю.И., Ваграменко Я.А., Завьялова Н.Б., Ильина А.С., Курова Н.Н., Малюк А.А., Михалева Г.В., Моисеева В.Б., Петровой Н.П., Пимонова В.А., Сташкевич И.Р., ТайлаковаУ.Н., Чипига А.Ф., Ярочкина В.И.

Особенности организации виртуальной образовательной среды образовательногоучрежденияпредставлены вработахАксюхана А.А., Афониной Е.С., Богатыревой Ю.И., Ваграменко Я.А.,Завьялова Н.Б., Зубаирова А.Ф., Ильина

А.С., Лобачева С. Л., Малюк А.А., Михалева Г.В.,Моисеева В.Б., Петровой Н.П., Пимонова В.А., Привалова А.Н., Тайлакова У.Н..Чипига А.Ф. и др.

В трудах Аксюхана А.А., Андреева А.А., Блинова В.И., Вартановой Е.Л., Елжановой Р.К., Завьялова Н.Б., Курова Н.Н., Кязимова К.Г., Лобачева С. Л., Михалева Г.В., Моисеева В.Б., Петровой Н.П., Пимонова В.А., Самерхановой Э.К., Сташкевич И.Р. Тайлакова У.Н., Ярочкина В.И.освещены основы информационной безопасности.

Авторы в своих работах информационную безопасность в общих аспектах, а применение в системе СПО данный вопрос раскрыт не в полном объеме.

Актуальность исследования определена на научно-теоретическом уровне: необходимо системно обосновать проблему по реализации виртуальной информационной среды, провести выявление условий и разработку методических рекомендаций для обеспечения информационной безопасности в процессе создания и функционирования виртуальной среды профессионального образовательного учреждения.

Виртуальная среда профессионального образовательного учреждения должна при всей своей «открытости» направлена на защиту обучающихся от негативного влияния пропаганды.

В связи с отсутствием методических рекомендации необходимо разработать методические рекомендации в области виртуальной образовательной среды профессиональной образовательного учреждения для обеспечения информационной безопасности.

Научно-методический уровень решения данной проблемы делает ее более актуальной.

После проведения анализа теоретических и практических исследований в рассматриваемой области по внедрению виртуальной образовательной среды в организациях СПО можно обозначить следующие противоречия:

- на педагогическом уровне –для обеспечения безопасной работы в виртуальной образовательной среди и недостаточно сформированной общепрофессиональной компетенцией по использованию современных средства поиска, анализа и интерпретации информации и информационных технологий для выполнения задач профессиональной деятельности;

- на научно-теоретическом уровне - между требованием обеспечения безопасного функционирования виртуальной образовательной среды и не в полной мере разработанностью данного процесса в теории и методике педагогики;

- на научно-методическом уровне - между предъявляемыми требованиями по повышению уровня безопасности виртуальной образовательной среды и общего характера разработки методического инструмента.

Установленные противоречия позволяют утверждать, что на уровне среднего профессионального образования в теории и практике существует проблема: отсутствуют методические рекомендации по обеспечению информационной безопасности функционирования виртуальной образовательной среды.

Выявленная объективная данная проблема при реализации профессионального обучения студентов колледжа показывает необходимость ее научно обоснованного решения и доказывает актуальность данного исследования и позволяют сформулировать тему как «Обеспечение информационной безопасности использования виртуальных сред для образовательных целей колледжа».

Анализ состояния проблемы информационной безопасности в организациях среднего профессионального образования позволил выявить *противоречие* между целесообразностью применения комплексных мер в рамках реализации политики ИБ образовательного учреждения, а также недостаточной защитой виртуальной среды, используемой для образовательных целей колледжа.

Проблема исследования заключается в том, что необходимо выбрать средства защиты при использовании виртуальных сред для образовательных целей в организации профессионального образования.

Подводя итоги, можно сделать вывод, что тема исследования «Обеспечение информационной безопасности использования виртуальных сред для образовательных целей колледжа» является актуальной, а полученные результаты имеют важное практическое значение.

Целью исследования является разработка рекомендаций по выбору средств защиты информации при использовании виртуальных сред для образовательных целей колледжа с учетом комплексной оценки уровня защищенности и требований нормативно-правовой базы Российской Федерации.

Объект исследования: процесс обеспечения информационной безопасности в организации среднего профессионального образования.

Предмет исследования: организация защиты информации при использовании виртуальных сред для образовательных целей в колледже.

Гипотеза исследования: состоит в предположении о том, что повышение эффективности системы защиты информации при использовании виртуальных сред для образовательных целей в колледже возможно на основе оценки уязвимостей существующих средств защиты и обеспечения их оптимального обновления с учетом максимального соответствия организационно-распорядительной документации и техническим требованиям.

Чтобы достичь поставленную цель были сформулированы следующие задачи**:**

1) изучить теоретические аспекты обеспечения информационной безопасности использования виртуальных сред для образовательных целей колледжа;

2) проанализировать цифровую образовательную среду ГБПОУ «Миасский машиностроительный колледж» по реализации мер информационной безопасности;

3) разработать рекомендации по совершенствованию защиты информации при использовании виртуальных сред в ГБПОУ «МиМК»;

Чтобы решить поставленные задачи были использованы следующие **методы исследования:** изучение, анализ теоретико-методической литературы по теме исследования; документоведческий метод (анализ документации образовательной организации); анализ и сопоставление имеющихся средств для защиты данных; анализ и классификация собранных данных с последующим моделированием и проектированием системы защиты и выбора средств; метод апробации результатов; метод экспертной оценки качества разработанных мер защиты.

Научная новизна исследования*:* разработана модель функционирования виртуальной образовательной среды в организации среднего профессиональной образования для обеспечения информационной безопасности.

Теоретическая значимость исследования: рассмотрены основные компоненты виртуальной образовательной среды в организации среднего профессиональной образования для обеспечения информационной безопасности.

Практическая значимость работы заключается в разработке методических рекомендаций по совершенствованию защиты информации при использовании виртуальных сред в организации среднего профессиональной образования.

Апробация и внедрение результатов исследования осуществлялись при реализации процесса педагогической и экспериментальной деятельности в ГБПОУ «Миасский машиностроительный колледж».

База исследования: ГБПОУ «Миасский машиностроительный колледж».

Структура работы. Магистерская диссертация состоит из введения, трех глав, заключения, списка использованной литературы, приложений. Работа содержит 155 страниц, 22 рисунка, 33 источника литературы.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ ВИРТУАЛЬНЫХ СРЕД ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ЦЕЛЕЙ КОЛЛЕДЖА

1.1. Сущность, компоненты и функции виртуальной среды

В эпоху глобального цифрового мира живет и развивается современное человечество. Все самое современное создается при использовании современных технологий. Фактически в век новейших технологий формируются и закладываются самые основы информационного пространства для общения, работы и развития.

Виртуализация информационных систем привела к тому, что современная педагогика должна учитывать, что организация учебно-воспитательного процесса для современного подрастающего поколения осуществляется и с использованием различных виртуальных сред. Происходящие изменения протекают в различных сферах жизни и в том числе образовании настолько быстро, что и сам образовательный процесс необходимо изменять и внедрять новые информационно-образовательные технологии исключительно в том же темпе, в каком происходит развитие информатизации и цифровизации. Только при реализации такой траектории связь между различными возрастными поколениями будет сохранена.

Система среднего профессионального образования поставлена перед решением проблемы, в которой должна быть четко определена система подготовки квалифицированных кадров к применению различных виртуальных сред.

Виртуальная образовательная среда меняет не только реализуемые производственные задачи из-за влияния на образ мышления людей. Меняется

само представление решения и интерпретация поставленных перед обществом проблемы глобального масштаба

Именно поэтому система среднего профессионального образования должна решить проблемы и выстроить систему подготовки квалифицированных кадров к применению различных виртуальных сред в будущей профессиональной деятельности.

Довольно обычным явлением стала реализация обучения с использованием дистанционных образовательных ресурсов в системе СПО: реализуется основная профессиональная образовательная программа (учебные дисциплины, междисциплинарные курсы), мероприятия воспитательного содержания, профориентационной направленности. Также с использованием информационных технологий проводятся родительские собрания, реализуются программы популяризации профессий и специальностей, педагогические советы, общие собрания работников, методические советы, заседания предметно-цикловой комиссии.

Процесс организации виртуальной среды необходимо имеет свои особенности. В настоящее время реализация данного процесса имеет отсутствуют проявление инновационности в поведенческом мотиве участников образовательного процесса

Модель организации образовательного процесса с использованием дистанционных образовательных ресурсов в системе СПО напоминает линейную структуру организации, где педагогический работник с технических, программных и информационных ресурсов ставит обучающимся задачу для выполнения. При таком способе постановки задачи идет полный охват аудитории, но отсутствует индивидуальный подход, который бы полностью смог реализовать освоение федеральных государственных образовательных стандартов (далее ФГОС) по профессиям или специальностям.

Именно поэтому возникает необходимость в пересмотре подходов к реализации дистанционных образовательных ресурсов в системе СПО для реализации ФГОС СПО.

В данном случае применение психодидактического подхода с его постоянно изменяемыми видами деятельности при реализации образовательного процесса можно положить в основу для реализации поставленных задач. В последние десятилетия данный оптимальный образовательный процесс регулярно исследовался, в том числе проводились исследования в области возможностей для обучения в виртуальных образовательных средах.

В исследованиях представлены какие наиболее эффективные способы применяются для роста потенциального развития обучающихся, какие формы взаимодействия реализуются между преподавателями, мастерами производственного обучения и обучающимися. Исследования обращают внимание на то, что эффективные управленческие решения помогают реализовать все возможности информационных систем для организации высококачественного образовательного процесса.

В. А. Ясвин считает, что при формировании личности при точно заданных условиях и системах с учетом социума и развития происходит в образовательной среде.

Как систему образовательных условий можно принять определение образовательной среды. Условия содержат в себе требования к практике реализации применяемой образовательной технологии, межличностностые отношения участников образовательных отношений, виды деятельности с учетом возрастных и социальных особенностей групп.

Информационная образовательная среда профессиональных образовательных организаций реализуется с применением различных технологий: информационных и коммуникационных. Данная среда решает важные технологические задачи и занимается технической поддержкой мероприятий образовательного процесса в интернет-пространстве.

Для определения современных возможностей рассмотрены пути совершенствования информационно-образовательной среды в некоторых педагогических работах.

В определении Андреева А.А. к новейшей современной педагогической системе можно отнести информационно-образовательную среду, в которой в компьютерных учебно-методических комплексах соединены различные виды информации.

Розина И.Н. предлагает выделить принципы для классификации среды, которые делают ее гарантирующей реальные результат: обратная связь, мотивационная составляющая, интерактивность, критерии оценки

На открытость к применяемым программным, интеллектуальным, техническим ресурсам информационно-образовательной среды делает акцент в своих работах И.Г. [7].

Все вышеперечисленные факторы указывает в своих исследованиях Кречетников К. Г. Отдельно он выделяет оригинальность при работе с информационно-образовательной среды: аналитические, прогностические, новаторские способности.

Информационная безопасность в современном мире становится все более актуальной проблемой. С развитием технологий, особенно в области информационных технологий, возникают новые угрозы и риски для безопасности данных.

Одной из таких угроз является использование виртуальных сред для образовательных целей. Виртуальные среды для образовательных целей, такие как онлайн-курсы, платформы для дистанционного обучения и виртуальные классы, становятся все более популярными. Они предоставляют уникальные возможности для обучения и саморазвития, и часто злоумышленники получают несанкционированный доступ к конфиденциальной информации или для атак на системы и сети.

Одним из основных аспектов обеспечения информационной безопасности виртуальных сред для образовательных целей является защита персональных данных студентов и преподавателей. Виртуальные среды часто содержат большое количество конфиденциальной информации, такой как имена, адреса,

номера телефонов и электронных почтовых адресов студентов. Такая информация может быть использована для мошенничества или других незаконных целей. Поэтому необходимо обеспечить защиту персональных данных путем шифрования, доступа только для авторизованных пользователей и использования надежных механизмов аутентификаций.

Кроме того, виртуальные среды могут быть атакованы злоумышленниками для целенаправленного внедрения вредоносного программного обеспечения. Такой вредоносный софт может использоваться для кражи паролей и другой конфиденциальной информации, повреждения данных или нарушения работы системы. Для защиты от таких атак необходимо использовать современные антивирусные программы, брандмауэры и другие механизмы защиты информационной системы. Еще одним аспектом обеспечения информационной безопасности является обучение пользователей виртуальных сред различным аспектам безопасности информации. Все пользователи, включая студентов и преподавателей, должны быть осведомлены о возможных угрозах и методах защиты. Это может быть достигнуто путем проведения специальных тренингов и обучения, демонстрации примеров реальных атак и их последствий.

Однако, несмотря на все меры предосторожности, существуют неконтролируемые факторы, которые могут повлиять на безопасность виртуальных сред для образовательных целей. Например, ошибки в программном обеспечении или оборудовании, неявные уязвимости или социальная инженерия могут привести к компрометации безопасности. Поэтому необходимо иметь более гибкие механизмы обнаружения, отслеживания и реагирования над безопасностью инциденты. Информационная безопасность виртуальных сред для образовательных целей в колледже является крайне важной задачей. Учитывая возрастающие угрозы и риски, необходимо принимать соответствующие меры для защиты данных, обучения пользователей и реагирования на возможные

инциденты. Только так можно обеспечить безопасное и эффективное использование виртуальных сред для обучения студентов и поддержку их образовательного процесса.

Виртуальная среда — это программное окружение, которое позволяет создавать и использовать виртуальные машины (ВМ). Виртуальная машина является программным образом реализованной компьютерной системой, которая имитирует работу реальной физической машины.

Сущность виртуальной среды — это набор программных инструментов и ресурсов, которые позволяют создавать и управлять виртуальными машинами. Она предоставляет пользователю среду, в которой можно развернуть и запустить различные ВМ с различными операционными системами и приложениями. Виртуальная среда позволяет пользователю создавать несколько изолированных ВМ на одном физическом сервере.

Компоненты виртуальной среды включают в себя:

1. Гипервизор — это программное обеспечение, которое позволяет управлять и запускать виртуальные машины. Он обеспечивает взаимодействие между физическим сервером и виртуальными машинами, осуществляет разделение ресурсов и управление виртуальными машинами.

2. Виртуальные машины — это отдельные экземпляры операционных систем, которые работают на гипервизоре. Виртуальные машины могут быть развернуты на одном физическом сервере. Каждая ВМ может быть настроена под разные операционные системы и приложения.

3.Ресурсы — это вычислительная, сетевая и хранилища, которыми располагает виртуальная среда. Ресурсы могут быть распределены между различными виртуальными машинами в зависимости от их требований и приоритетов.

4.Менеджер виртуальной среды — это инструмент, который позволяет пользователю управлять виртуальными машинами и ресурсами. Он обеспечивает управление, мониторинг и настройку всех аспектов виртуальной среды,

включая создание и удаление виртуальных машин, настройку сетевых подключений, добавление и удаление ресурсов и т. д.

Функции виртуальной среды:

1. Консолидация ресурсов - виртуальная среда позволяет объединить физические серверы и ресурсы в одном месте, что позволяет более эффективно использовать вычислительные мощности и снизить затраты на оборудование и энергию.

2. Изоляция - каждая ВМ находится в своей изолированной среде и не может влиять на работу других ВМ. Это позволяет легко управлять и поддерживать ВМ, а также обеспечивать безопасность и защиту данных.

3. Поддержка различных операционных систем - виртуальная среда позволяет развернусь ВМ с различными операционными системами на одном физическом сервере. Это позволяет пользователям работать с различными приложениями, основанными на разных ОС, на одном сервере.

4. Быстрое развертывание и миграция - виртуальные машины могут быть быстро развернуты и запущены на новых физических серверах при необходимости. Они также могут быть легко перемещены с одного сервера на другой без прерывания работы или потери данных.

5. Масштабируемость - виртуальная среда позволяет легко добавлять и удалять ресурсы в зависимости от потребностей пользователей. Это позволяет эффективно использовать ресурсы и обеспечить высокую производительность ВМ.

6. Защита и восстановление данных - виртуальная среда позволяет создавать резервные копии и выполнять восстановление данных на уровне ВМ. Это обеспечивает надежность и безопасность данных, а также облегчает процесс резервного копирования и восстановления.

Кроме того, использование виртуальных сред позволяет студентам обмениваться опытом и знаниями с другими студентами и преподавателями. Они могут участвовать в форумах и обсуждениях, задавать вопросы и получать об-

ратную связь по своим работам. Это создает сотрудническую и интерактивную обучающую среду, которая способствует активному обучению и развитию навыков коммуникации. Однако, несмотря на все преимущества, использование виртуальных сред также имеет свои ограничения и проблемы. Одной из главных проблем является необходимость обеспечения доступности и надежности технологической инфраструктуры. При работе в интернете с образовательными ресурсами лишь у некоторой части обучающихся отсутствуют проблемы.

Кроме того, виртуальные среды не могут полностью заменить традиционные методы обучения, такие как лекции и практические занятия в классе. Они могут быть отличным дополнением к этим методам, но не могут полностью заменить их. Некоторые студенты могут испытывать затруднения при самостоятельном изучении материалов и требовать более плотной академической поддержки. В целом, использование виртуальных сред для образовательных целей колледжа предоставляет студентам широкие возможности для изучения, развития навыков и обмена знаниями. Однако, необходимо учитывать ограничения и проблемы, связанные с использованием таких сред, и сосредоточиться на обеспечении доступности образования.

Педагогическое сообщество, используя виртуальную образовательную среду, получило множество новых технических возможностей для решения проблем общения с участниками образовательного процесса

В наиболее перспективном направлении в современном образовательном пространстве при реализации дистанционного обучения все больше значимость занимает возможность работы преподавателя и его новые функции.

Образ мышления педагогического работника для работы в данной сфере должен измениться, адаптироваться и добавить ему новые профессиональные компетенции при организации он-лайн уроков, лекций и других мероприятий:

-новые формы составления диалогов в виртуальной среде: конкретизи-

рованная коммуникация с сокращенной однозначной осознанной формулировкой без ограничения во временных рамках и возможностью проанализировать и скорректировать - асинхронный «разговор»;

- внедрение основной современной педагогической технологии- методов проектов;

-реализация индивидуального пути развития в инновационных начинаниях, практической подготовки, практикоориентированность на протяжении всего процесса обучения с применением виртуальной образовательной среды;

-организация особой образовательной среды в виртуальных средах, в которых эффективно применяются технические, управленческие и экономические ресурсы;

-разработка современных методов обучения и концепций для работы в виртуальных средах, которые адаптированы к каждому обучающемуся индивидуально, подходят на различных этапах образовательного процесса;

-проведение обучающих мероприятий в рамках адаптации преподавателей в рамках педагогической деятельности в виртуальном образовательном пространстве

Поэтому в системе подготовке педагогических кадров необходимо реализовать мероприятия по обучению и применению в педагогической деятельности различных современных технологических процессов в рамках внедрения виртуальных образовательных сред.

Внедрение инноваций в образовательную область требует воплощение в жизнь различные усовершенствования в профессиональной среде педагогических кадров с учетом применения принципов непрерывности образования и применения новейших технологических достижений.

После проведения анализа терминологии «виртуальная образовательная среда» следует результат:

Отличие виртуальной образовательной среды заключается в том, что в ней применяется новый подход образовательного взаимодействия в образовании. Если в обыденной жизни мы используем личное общение, то при виртуальном – применяем различные способы и средства коммуникации.

Бурно развивающиеся средства для передачи информации в современном мире становятся очень доступными для студентов и педагогических работников для использования в процессе обучения

Широко распространенная организация использования дистанционных технологий в виртуальном пространстве трактуется как два различных направления: ознакомление с информацией и взаимодействие участников образовательного процесса

Создание индивидуального практикориентированного пути развития студента позволяет разработанная модель организации виртуальной образовательной среды. Модель может обеспечить непрерывность процесса образования, профессиональную поддержку преподавателям и мастерам производственного обучения, доступность различных новейших образовательных ресурсов из любой точки планеты и внедрение опыта взаимодействия.

Данную модель можно считать оптимальной, современной и открытой, так как все основные принципы современной педагогики нашли отражение в ней: непрерывность образования, использование различных коммуникативных функций, взаимодействия и удовлетворения всех потребностей участников образовательного процесса.

Открытость данной модели обеспечивает процесс развития образования в целом и достигается за счет использования виртуальной образовательной среды в качестве основного средства коммуникации между преподавательской средой и студентам

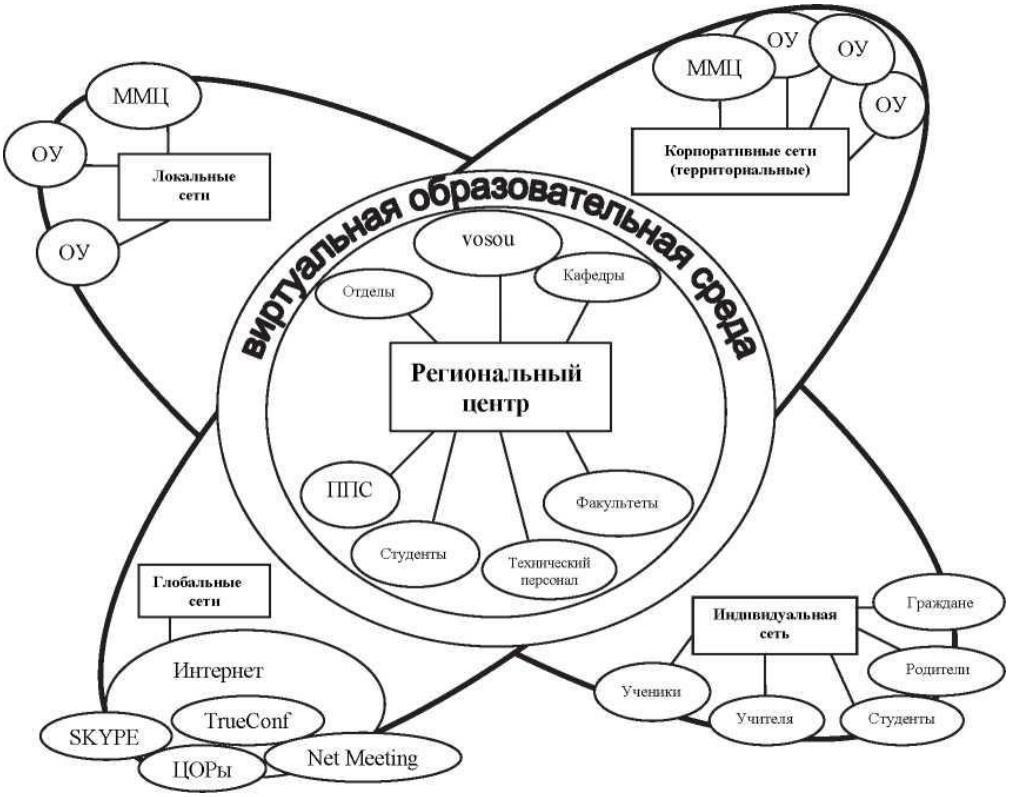

Рисунок 1. Модель организации виртуальной образовательной среды колледжа: К- колледж; МО–методическое объединение колледжа; ПР–педагогические работники; ЦР - цифровые ресурсы; ВСК- виртуальная образовательная среда колледжа

При глубочайшем проникновении информационных технологий в образовательный процесс виртуальная образовательная среда колледжа должна постоянно модернизироваться для обеспечения высококачественного образования.

При объединении множества факторов можно сформулировать понятие виртуальной образовательной среды.

Объединенные вместе в единое целое и направленные на взаимодействие участники процесса образования цифровое, технологическое и методологическое пространства О.А. Ильченко называет виртуальной образовательной средой.

Объединенные вместе учреждения СПО и управленческий аппарат, информационные источники, электронные источники, базовая документация, средства направленности информационных данных, протоколы взаимодей-

ствия –этим способом описывает Е.К. Марченко понятие виртуальной образовательной среды и указывает на значимость программно-методического обеспечения при организации данной среды.

По словам А.А. Андреева участие таких составляющих педагогики, как финансовая часть, управление, законодательная входит в понятие виртуальной образовательной среды.

Виртуальная образовательная среда, по мнению М.Е. Вайндорф-Сысоевой, является пространством для обмена информацией и осуществлением взаимодействия между всеми участниками образовательного процесса, возникающим при использовании информационно-коммуникационных технологий. В данной среде комплекс технологические средства предоставляют возможность управлять содержанием образования и обеспечивать связь.

Осуществление образовательной деятельности в виртуальной образовательной среде представляет собой систему, направленную на взаимодействие участников процесса образования в цифровом, технологическом и методологическом пространства. Среда требует индивидуальных настроек в зависимости от конкретного колледжа и функционирует на программных платформах с гибкими функциями и требует поддержки от разных банков данных и направлена на реализацию образовательной деятельности.

Для организации бесперебойной работы виртуальной образовательной среды в рамках образовательного процесса необходимо соблюдать следующие условия:

- восполнение–использование ресурсов с наименьшими затратами.
- оптимизация - создание условий и учет особенностей обучающихся для благоприятного протекания образовательного процесса
- информатизация–распространение информации в образовательных целях.
- комплексность - мульти применение средств информатизации и мультимедиа.

− направленность - учет видов профессиональных и общих компетенций при постановке задач.

Таким образом виртуальная образовательная среда помогает сформировать у студентов профессиональные и общие компетенции в колледже.

1.2 Модель виртуальной образовательной среды ГБПОУ «Миасский машиностроительный колледж»

Виртуальная образовательная среда в колледже представляет собой комплекс инструментов, платформ и ресурсов, которые обеспечивают эффективное и удобное обучение и взаимодействие студентов, преподавателей и администрации колледжа.

Модель такой среды может состоять из:

1. Электронная образовательная платформа или Learning Management System (LMS). Это центральный инструмент, на котором располагается весь учебный материал, задания, расписания занятий и другая информация, связанная с учебным процессом. Студенты могут получать доступ к этой платформе из любого устройства, в любое время. Она также может предоставлять инструменты для онлайн-тестирования и оценки успеваемости студентов.

2. Электронные учебники и материалы. Вместо традиционных бумажных учебников, студенты могут использовать цифровые версии, которые доступны на платформе колледжа. Кроме того, на платформе могут быть размещены другие материалы, такие как видео-уроки, интерактивные задания, лекции в записи и прочее.

3. Онлайн-курсы и массовые открытые онлайн-курсы. Помимо классических учебников, студентам могут быть доступны онлайн-курсы, которые можно пройти в свободное от основного расписания время. Массовые открытые онлайн-курсы также могут быть доступны для широкой общественности и позволять получить новые знания и навыки независимо от места жительства.

4.Виртуальные классы и вебинары. С использованием специальных программ и платформ, студенты и преподаватели могут проводить уроки и лекции

в режиме реального времени. Это особенно важно в случаях, когда студентам или преподавателям не удобно или невозможно присутствовать на занятиях по какой-либо причине.

5.Системы электронного портфолио. Для оценки успеваемости студентов и мониторинга их прогресса могут быть использованы системы электронного портфолио, на которых студенты собирают и представляют свои работы и достижения в течение учебного года.

6.Инструменты для коммуникации и обратной связи. Для более эффективного взаимодействия между преподавателями и студентами, а также для обратной связи по заданиям и работам, могут быть использованы инструменты для коммуникации, такие как электронная почта, форумы обсуждений, онлайн-чаты и т.д .

7.Индивидуализация обучения. Одним из преимуществ виртуальной образовательной среды является возможность индивидуального подхода к каждому студенту.

Платформа может предоставлять рекомендации и персонализированную поддержку в обучении на основе данных о прогрессе студента и его предпочтениях.

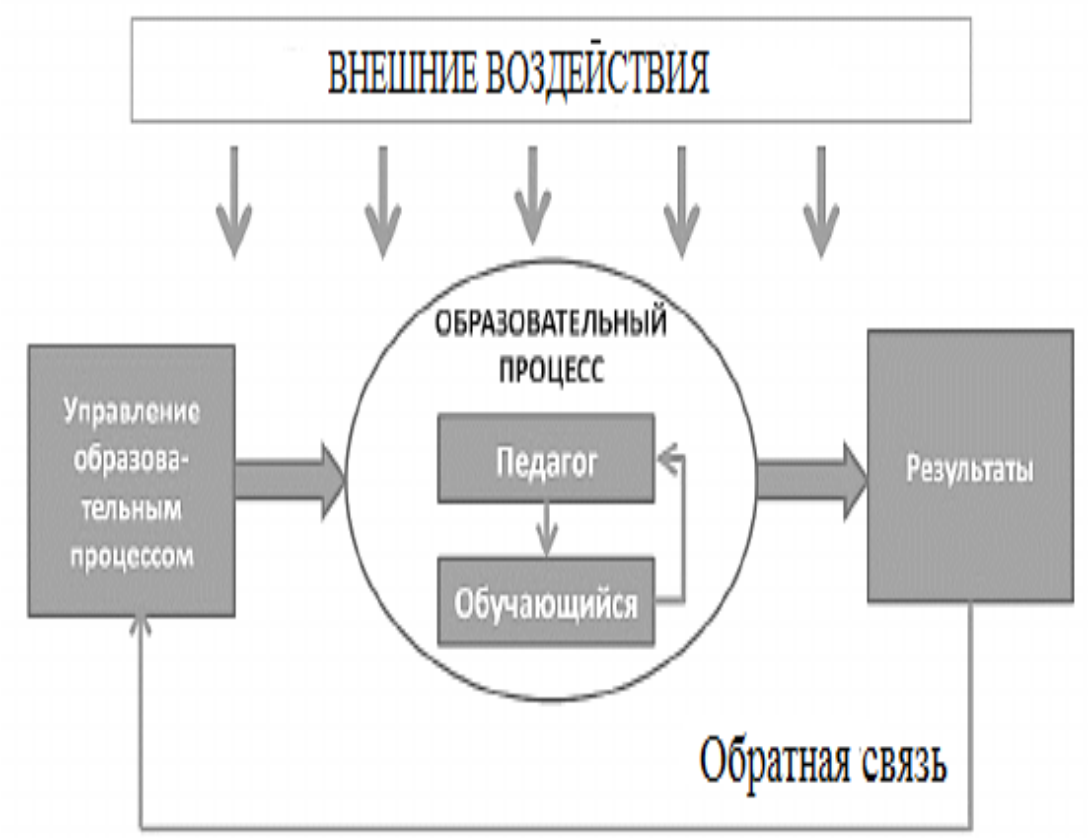

Рисунок 2 -Модель управления традиционным образовательным процессом

В целом, модель виртуальной образовательной среды в колледже направлена на повышение доступности, гибкости и эффективности обучения. Она обеспечивает возможность получить знания и навыки в любое время и из любого места, а также способствует активному взаимодействию студентов и преподавателей. Кроме того, такая среда позволяет использовать современные технологии и инструменты для более эффективного и интересного обучения.

Для создания информационной безопасности, была исследована основная нормативно-правовая документация и организация работы виртуальной образовательной среды ГБПОУ «Миасский машиностроительный колледж».

Описание виртуальной образовательной среды раскрыло особенности построения ее модели и требования к обеспечению информационной безопасности образовательных учреждениях СПО.

Рассмотрим работу виртуальной образовательной среды на примере ГБПОУ «Миасский машиностроительный колледж» и проведем анализ.

Национальные проекты РФ, направленные на развитие стратегических позиций в информатизации и цифровизации, регламентируют работу виртуальных образовательных сред образовательных учреждений СПО на отечественном программном обеспечение, которое находится в свободном доступе и не требует больших финансовых затрат.

Федеральные государственные образовательные стандарты по профессиям и специальностям требуют учета особенностей реализации при использовании виртуальных образовательных сред.

Таблица 1-Основные элементы виртуальной образовательной среды колледжа

№ п/п	Элементы ВОС колледжа	Реализация мероприятий
1.	Официальный сайт	Реализация мероприятий информационного сопровождения и открытости процессао бучения
2.	Электронная почта	Реализация мероприятий по управлению и взаимодействию с различными структурами
3.	Электронный журнал	Реализация мероприятий по входному, текущему и итоговому контролю.
4.	Электронный календарь	Реализация мероприятий по календарному учебному планированию
5.	Система электронного документооборота	Реализация мероприятий по ведению хранению, обработке и распространению информации
5.	Система дистанционного обучения для студентов	Реализация мероприятий по ФГОС с помощью дистанционных технологий
6.	Корпоративный портал	Проведения мероприятий, направленных на повышение мотивации в использовании виртуальных образовательных сред преподавателями и мастерами производственного обучения

После проведения подробного анализа виртуальной образовательной среды ГБПОУ «Миасский машиностроительный колледж» приходим к выводу, что в ней отражены лишь часть требуемого содержимого, а именно:

-официальный сайт ГБПОУ «МиМК» (http://miassmk.ru);

- электронная почта ГБПОУ «МиМК» (miassmk@mail.ru);

-электронный журнал ГБПОУ «МиМК» (Сетевой город «Электронный

журнал» Модуль ПОО: https://poo.edu-74.ru/).

Чтобы студенты колледжа смогли освоить учебный материал в соответствии с учебным планами по профессиям и специальностям в полном объеме в период дистанционного обучения образовательный процесс был организован с использованием информационно-коммуникационных образовательных платформ.

В эти периоды ГБПОУ «Миасский машиностроительный колледж» реализовывались лишь часть мероприятий:

- реализация мероприятий информационного сопровождения и открытости процесса обучения
- реализация мероприятий по управлению и взаимодействию с различными структурами
- реализация мероприятий по входному, текущему и итоговому контролю.

Однако данные мероприятия не проводились:

- реализация мероприятий по календарному учебному планированию;
- реализация мероприятий по ведению хранению, обработке и распространению информации;
- реализация мероприятий по ФГОС с помощью дистанционных технологий;
- проведения мероприятий, направленных на повышение мотивации в использовании виртуальных образовательных сред преподавателями и мастерами производственного обучения.

1.3. Анализ виртуальной образовательной среды ГБПОУ «Миасский машиностроительный колледж» по реализации мер информационной безопасности

Анализ виртуальной образовательной среды колледжа в отношении реализации мер информационной безопасности является важным шагом для

обеспечения защиты данных и сохранности информации. В современном мире, где цифровые технологии занимают все более прочные позиции, образовательные учреждения, включая колледжи, не являются исключением. Виртуальная образовательная среда предоставляет студентам и преподавателям доступ к обучающим материалам, курсам, онлайн-классам и другим ресурсам, улучшая процесс обучения и позволяя гибче работать с информацией. И это создает риск утечки данных и других нарушений информационной безопасности.

Для анализа виртуальной образовательной среды колледжа по реализации мер информационной безопасности следует рассмотреть несколько аспектов:

1. Инфраструктура: первым шагом является оценка инфраструктуры, используемой в виртуальной образовательной среде колледжа. Следует оценить сетевое оборудование, сервера, системы хранения данных и другие компоненты, которые могут быть уязвимыми для атак и взломов. Важно убедиться, что все системы обновлены и настроены должным образом для обеспечения безопасности данных.

2. Управление доступом: следующим шагом является анализ системы управления доступом в виртуальной образовательной среде колледжа. Это включает проверку систем аутентификации и авторизации, паролей и прочих механизмов, которые используются для проверки подлинности пользователей и предоставления им правильных разрешений доступа. Рекомендуется использовать механизмы двухфакторной аутентификации и проводить регулярную проверку паролей для поддержания высокого уровня безопасности.

3.Защита данных: важный аспект анализа виртуальной образовательной среды — это оценка механизмов защиты данных. Следует оценить наличие шифрования данных, архивации и резервного копирования, защиты от вредоносного программного обеспечения и других мер безопасности, которые используются для защиты важной информации. Также стоит обратить внимание

на соблюдение правил обработки персональных данных и соответствие местным законам и политикам в отношении конфиденциальности.

4.Обучение и осведомленность: еще одним важным аспектом является анализ обучения и осведомленности пользователей в отношении мер информационной безопасности. Колледж должен иметь программу обучения, которая обучает студентов и преподавателей правильным практикам по обеспечению безопасности данных и информации. Это может включать обучение по выбору сложных паролей, осведомленность о фишинговых атаках, осознание рисков социальной инженерии, а также обучение о том, как реагировать на инциденты информационной безопасности.

5.Мониторинг и реагирование: не менее важным является внедрение системы мониторинга и реагирования на возможные инциденты информационной безопасности. Колледж должен иметь процедуры и системы, которые позволяют быстро обнаруживать и реагировать на атаки, взломы или другие нарушения безопасности. Мониторинг активности позволяет выявлять подозрительное поведение и проблемы безопасности, а также предотвращать их в самом начале.

Осуществление анализа виртуальной образовательной среды колледжа по реализации мер информационной безопасности позволит выявить уязвимости и пробелы в системе и принять необходимые меры для их устранения. Это важно для обеспечения безопасности данных и сохранности информации, а также для предотвращения возможных негативных последствий, связанных с утечкой данных или взломом системы. Правильные меры информационной безопасности позволят колледжу обеспечить надежность и конфиденциальность пользовательской информации и создать безопасную и защищенную образовательную среду.

Анализ виртуальной образовательной среды ГБПОУ «Миасский машиностроительный колледж» проводился поэтапно:

1) Анализ защиты от угроз виртуальной образовательной среды колледжа в целом.

2) Анализ выполнения предостережений и правил при работе в виртуальной образовательной среде сотрудниками колледжа.

Для анализа мер защиты от угроз виртуальной образовательной среды проведены представленные «Лабораторией Касперского» работы.

Основываясь на анализе, получаем результаты:

1. Меры полностью выполнены на 41,2 % (7 из 17), частично на 23,6% (4 из 17) и не выполнены на 35,2% (6 из 17).

2. Регламент использования гаджетов педагогическими работниками и студентами не прописан.

3. Съемные устройства сотрудников и шифрование дисков выполнено частично или не реализовано совсем.

Таблица 2 - Анализ системы защиты виртуальной образовательной системы колледжа

№	Наименование элемента защиты информационной системы (Перечень «Лаборатории Касперского»)	Отметка о выполнении мер защиты
1.	Защита от вредоносного ПО	Выполнено
2.	Управление обновлением ПО	Выполнено
3.	Разграничение доступа к ИТ ресурсам	Выполнено
4.	Сетевая структура (выделение критически важных подсетей)	Выполнено
5.	Контроль использования внешних устройств	Выполнено частично
6.	Специальная политика безопасности для внешних устройств	Выполнено частично
7.	Специальная политика безопасности для съемных носителей	Выполнено частично
8.	Шифрование переписки	Выполнено
9.	Шифрование файлов и папок	Выполнено
10.	Контроль программ	Выполнено
11.	Антивирусное ПО для мобильных устройств	Не реализовано
12.	Специальная политика безопасности для ноутбуков	Не реализовано
13.	Полное шифрование диска	Не реализовано
14.	Шифрование данных на съемных носителях	Не реализовано
15.	Аудит ИТ безопасности независимыми компаниями	Выполнено частично
16.	Специальная политика безопасности для смартфонов / планшетов	Не реализовано
17.	Системы управления мобильными	Не реализовано

	устройствами	

Проведенный анализ информационной безопасности необходим в связи с тем, что в ГБПОУ «Миасский машиностроительный колледж» на первых курсах обучаются несовершеннолетние студенты, с учетом этих данных представлена модель обеспечения информационной безопасности студентов:

Рисунок 3 - Модель для создания информационной защищенности обучающихся

Для создания информационной защищенности необходимо выполнить условие, заключающееся в создании безопасности виртуальной образовательной среды у каждого обучающегося колледжа.

При создании безопасности виртуальной образовательной среды у каждого обучающегося колледжа нужно учитывать всесторонние риски, как внешние, так и внутренние. Таким рискам подвержены все возрастные группы обучающихся: и несовершеннолетние первокурсники и совершеннолетние старшекурсники.

Поэтому все возрастные группы студентов испытывают негативные воздействия виртуальной образовательной среды, и поэтому они должны научиться и применять способы защиты от разно факторных угроз виртуальных сред на всех уровнях участия в образовательном процессе.

Во время образовательного процесса за защиту от разно факторных угроз виртуальных сред несут ответственность все участники, указанные на рисунке 3: на государственном и общественном уровне, в информационном пространстве, преподаватели и мастера производственного обучения, родители (законные представители) и обучающиеся колледжа.

Очевидно, что в виртуальной среде информационное пространство заполнено различной информацией, за содержание и распространение которой не всегда можно осуществлять контроль

Родители (законные представители), испытывая колоссальную нагрузку на производстве в настоящее время, не всегда находят время и возможность проконтролировать информационные потоки у своих детей. А зачастую и сами подвергаются негативному воздействию и не имеют компетенций для фильтрации информации по возрастному и психофизическому принципам.

Чтобы оградить обучающихся колледжа он угроз необходимо создать контроль над всеми областями, оказывающими влияние на информационную безопасность: физиологическая область, нормативная документация, программное обеспечение, нравственно-этическая область, просветительская область.

По вышеперечисленным направлениям в ГБПОУ «МиМК» проводятся различные действия:

а) на федеральном и региональном законодательном уровне для защиты от угроз в виртуальной образовательной среде действует единая государственная политика и существует большое количество нормативной документации, которая предусматривает правовую защиту от негативной информации подрастающего поколения;

б) на сайте колледжа представлен раздел «Электронная информационно-образовательная среда» размещена нормативно-правовая документация, регламентирующая функционирования данного раздела:

- Положение ГБПОУ «МиМК» о порядке доступа педагогов к ИТ-сетям и базам данных»;
- Положение ГБПОУ «МиМК» о комиссии по обеспечению защиты персональных данных»;
- Положение ГБПОУ «МиМК» об информационной безопасности;
- Положение ГБПОУ «МиМК» о применении электронного обучения
- Методические рекомендации по защите персональных данных, угрозах, средствах и способах обеспечения информационной безопасности;

в) физиологическая особенность учитывается при рассмотрении возрастных особенностей при получении информации в виртуальных средах, в ней отражены поведенческие и этические аспекты;

г) отражение негативных воздействий виртуальной образовательной среды необходимо для обеспечения нормального психофизического здоровья не только у обучающихся, но и у педагогических работников, уменьшения вредных привычек таких как интернет – зависимость и игромания.

Реализации мероприятий по отражению негативных воздействий виртуальной образовательной среды необходимо для обеспечения нормального психофизического здоровья проводится не в полном объеме, их содержание отражено на сайте колледжа в разделе «Студенту» во вкладке «Информационная безопасность»:

- Методические рекомендации «Правовая основа ограничения доступа к информации, причиняющей вред здоровью и развитию студентов колледжа»;

- Памятка для обучающихся «Азбука безопасности студентов колледжа».

Несмотря на то, что размещенные на сайте вышеуказанные мероприятия находятся в свободном доступе на сайте колледжа, они не реализуются со всеми студентами в полном объеме и не применяются при воздействии угроз от различных информационных источников.

В плане учебно-воспитательной работы ГБПОУ «МиМК» мероприятия, направленные на отражение негативных воздействий виртуальной образовательной среды встречаются не часто, их реализация проводится не системно, реализация общих и профессиональных компетенций на формирование информационной культуры проводилось только 1 раз на предметной неделе по дисциплине «Информатика» среди студентов первого курса.

Требования современного ведения документооборота, дистанционного обучения, использования программ для деятельности колледжа должны выполняться для обеспечения всех запросов современной виртуальной среды. В ГБПОУ «МиМК» на всей компьютерной технике установлен контент-фильтр SkyDNS, который проводит сетевую фильтрацию интернета. Данный программный продукт не ограничивает трафик, но ограничивает доступ к вредоносным и запрещенным источникам информации и блокирует ее. Рассмотрим воздействие контент-фильтра SkyDNSв ГБПОУ «Миасский машиностроительный колледж»:

Таблица 3 - Воздействие контент-фильтра SkyDNS в ГБПОУ «МиМК»

Комплекс мероприятий		Внедрение в работу
Комплекс основных мероприятий	Установка классической DNS-фильтрации	Установлено на всех компьютерах- на учебном оборудовании лабораторий и мастерских
	Управление доступа к сайтам	Производится на различного типа шифрования

	Блокировка черных списков и сайтов, запрещенных в РФ	В соответствии с рекомендациями и нормативной документацией проведена блокировка (198 сайтов)
	Доступ только к разрешенным объектам и приложениям	выполнение
	Применение безопасного поиска, исключающего выходом на запрещенные и экстремистские сайты	Выполнение обязательной проверки
	Применение полного запрета на поиск, исключение выхода на запрещенные и экстремистские сайты	выполнение
	Применение полного запрета на всплывающую в окнах рекламу	выполнение
	Установка разных уровней защит у преподавателей, мастеров производственного обучения и студентов	выполнение
	Установка разных уровней защит у преподавателей, мастеров производственного обучения и студентов на одном и том же рабочем месте	выполнение
Обеспечение безопасности	Применение полного запрета на обход защиты от меняющихся IP-адресов	выполнение
	Применение полного запрета на установку вредоносных программ	выполнение
	Применение полного запрета от злоумышленников, которые пытаются внедрить вредоносные программы	выполнение

Применяемые в ГБПОУ «МиМК» отечественные программные продукты СкайДНС для обеспечения информационной безопасности позволят колледжу запрещать обходы защиты от меняющихся IP-адресов, установку вредоносных программ выполнены полностью.

В рамках реализации общеобразовательных дисциплин «Информатика», «Основы проектной деятельности, в том числе индивидуальный проект» и общепрофессиональных дисциплин «Информационные технологии в профессиональной деятельности, «Бережливые технологии», «Цифровая культура в области машиностроения» проводится обучение по оценке угроз со стороны виртуальных сред, ведется и работа с родителями (законными представителями об основах цифровой грамотности.

Проводимые мероприятия по учебным дисциплинам не в полном объеме рассказывают об особенностях угроз и в колледже они не отражены в плане учебно-методической работы, отсутствует централизованно организованные дополнительные общеразвивающие программы, которые бы могли сфокусировать внимание взрослого поколения к решению поставленных задач в данной области. Также с педагогическими работниками необходимо проводить занятия по современным средствам защиты, так как они являются прямыми участниками виртуального образовательного пространства.

Через учебно-воспитательную работу проводится основная организация мероприятий по изучению и использованию современных средств защиты в виртуальной образовательной среде, именно они способствуют формированию информационной культуры обучающихся профессиональных образовательных организаций для понимания самих базовых основ и понятий и применения этих компетенций не только в образовательном процессе, но и в повседневной жизни, а также проектировать их на остальных членов общества.

Мероприятия внеурочной деятельности в колледже задействованы для формирования информационной просвещенности студентов, в колледже размещены баннеры с информацией, предостерегающей от воздействия различной негативной и недостоверной информацией. Для погружения в это информационное поле необходимо делать акцент на данные баннеры и проводить разъяснительные работы.

В рамках двухлетнего периода с преподавателями и мастерами производственного обучения ГБПОУ «МиМК» проводилась работа по изучению базовых основ и понятий виртуальных образовательных сред и применения этих компетенций в образовательном процессе и получены следующие результаты: данная группа педагогических работников не в полной мере осознает принципы ответственного поведения при организации дистанционного образовательного процесса и допускает небрежное и попустительское отношение в следующих ситуациях:

– при окончании образовательного процесса не закрывают программы и не выключают компьютер;

– бездумно открывают неизвестные электронные письма от неизвестных пользователей, хранят свои персональные личные данные в открытом доступе, забывают выйти из личного почтового ящика, посещают разные сайты и переходит по ссылкам;

– открывают файлы с различными расширениями и не обращают внимание на те предупреждения об угрозах, которую несет виртуальная среда.

Подводя итоги работы по изучению базовых основ и понятий виртуальных образовательных сред и применения этих компетенций, студенты и педагогические работники колледжа, можно сделать вывод, что они не в полной мере осознают принципы ответственного поведения при организации дистанционного образовательного процесса и допускают небрежное и попустительское отношение. Именно поэтому необходимо разработать методические рекомендации по совершенствованию системы обеспечения информационной безопасности функционирования виртуальной образовательной среды ГБПОУ «МиМК».

Вывод по 1 главе

Изучив теоретические основы в первой главе магистерской диссертации, проведены исследования практического характера виртуальной образовательной среды ГБПОУ «Миасский машиностроительный колледж». Их реализация состояла из нескольких этапов.

После проведения анализа виртуальной образовательной среды ГБПОУ «Миасский машиностроительный колледж» приходим к выводу, что в ней отражены лишь часть требуемого содержимого: официальный сайт и почта ГБПОУ «МиМК» (электронный журнал ГБПОУ «МиМК». Для полной реализации возможностей виртуальной образовательной среды необходимо

применять система электронного документооборота и дистанционного обучения для студентов.

Чтобы оградить обучающихся колледжа он угроз необходимо создать контроль над всеми областями, оказывающими влияние на информационную безопасность: физиологическая область, нормативная документация, программное обеспечение, нравственно-этическая область, просветительская область.

Для анализа мер защиты от угроз виртуальной образовательной среды ГБПОУ «Миасский машиностроительный колледж» основаны на программном обеспечении «Лаборатории Касперского» работы. Меры полностью выполнены на 41,2 % (7 из 17), частично на 23,6% (4 из 17) и не выполнены на 35,2% (6 из 17). Регламент использования гаджетов педагогическими работниками и студентами не прописан. Съемные устройства сотрудников и шифрование дисков выполнено частично или не реализовано совсем.

Проводимые мероприятия по учебным дисциплинам не в полном объеме рассказывают об особенностях угроз и в колледже они не отражены в плане учебно-методической работы, отсутствует централизованно организованные дополнительные общеразвивающие программы, которые бы могли сфокусировать внимание взрослого поколения к решению поставленных задач в данной области. Также с педагогическими работниками необходимо проводить занятия по современным средствам защиты, так как они являются прямыми участниками виртуального образовательного пространства.

Требования современного ведения документооборота, дистанционного обучения, использования программ для деятельности колледжа должны выполняться для обеспечения всех запросов современной виртуальной среды. В ГБПОУ «МиМК» на всей компьютерной технике установлен контент-фильтр SkyDNS, который проводит сетевую фильтрацию интернета. Данный программный продукт не ограничивает трафик, но ограничивает доступ к вредоносным и запрещенным источникам информации и блокирует ее.

В рамках двухлетнего периода с преподавателями и мастерами производственного обучения ГБПОУ «МиМК» проводилась работа по изучению базовых основ и понятий виртуальных образовательных сред и применения этих компетенций в образовательном процессе и получены следующие результаты: данная группа педагогических работников не в полной мере осознает принципы ответственного поведения при организации дистанционного образовательного процесса и допускает небрежное и попустительское отношение.

После изучения теоретических основ и анализа виртуальных образовательных сред в ГБПОУ «Миасский машиностроительный колледж» позволяют перейти к выполнению второй группы практических задач работы, можно перейти к планированию мероприятий, которые будут способствовать усовершенствованию системы обеспечения информационной безопасности в условиях функционирования виртуальной образовательной среды колледжа.

ГЛАВА 2. АНАЛИЗ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ВИРТУАЛЬНЫХ СРЕД В ГБПОУ «МИАССКИЙ МАШИНОСТРОИТЕЛЬНЫЙ КОЛЛЕДЖ»

2.1 Общие сведения об образовательной организации

1. Общая характеристика профессиональной образовательной организации, краткая история учреждения, основные виды деятельности, структура управления, материальное обеспечение, расположение учреждения.

Базой практики является: Государственное бюджетное профессиональное образовательное учреждение «Миасский машиностроительный колледж», аббревиатура – ГБПОУ «МиМК».

Вначале второго десятилетия двухтысячных систему начального профессионального образования и среднего профессионального образования Российской Федерации захватила новая волна под названием «оптимизация». «Оптимизация – это процесс, в результате которого выбирается наилучший вариант из множества возможных, процесс, в результате которого система приводится в оптимальное (наилучшее) состояние». Этот процесс не прошел мимо и нашей профессиональной образовательной организации.

Дата образования ГБПОУ «Миасский машиностроительный колледж» - 29 декабря 2012 г.

Место нахождения: 456110, Челябинская область, город Миасс, ул. Октября, д.1

Образовательный процесс осуществляется по следующим адресам:

1. Комплекс «Электрорадиотехника и технологии» пр. Октября, д.1, д.4.каб. № 212. Тел. 53-38-86, 53-04-95, 8-902-614-33-49.

2. Комплекс «Автомобилестроение и металлообработка»Предзаводская площадь, д.1, каб. 113, Тел. 55-47-55

3. Центр подготовки квалифицированных рабочих и служащих ул. Гвардейская, 1а. каб. № 104. Тел. 55-00-71, 55-00-92

Формы обучения, нормативные сроки обучения.

На базе основного общего образования – 3 года 10 месяцев.

Режим работы колледжа.

08:00 до 17:00, обед с 12:00 до 13:00

Учебный год делится на семестры:

I- семестр: с 01 сентября по 31декабря.

II- семестр: с 01 января по 30 июня.

Предмет, цели и виды деятельности ГБПОУ «Миасский машиностроительный колледж»

Колледж осуществляет образовательную деятельность по основным профессиональным образовательным программам среднего профессионального образования - программам ППСЗ и, дополнительным общеразвивающим программам и программам профессионального обучения

Целями деятельности Учреждения являются:

3.1. Основной целью деятельности Колледжа является реализация образовательных программ среднего профессионального образования.

3.2. Исходя из поставленной цели, Колледж решает следующие вопросы:

– подготовка высококвалифицированных кадров;

– организация и проведение методических и творческих работ и исследований;

– сохранение и приумножение нравственных и культурных ценностей

– общества.

3.3. Основными направлениями деятельности Колледжа являются:

– организационно-управленческая деятельность;

– учебная и методическая деятельность;

– организация научно-исследовательской работы (в дальнейшем НИР) и научно-исследовательской работы студентов (далее НИРС);

– воспитательная работа среди обучающихся;

– совершенствование материальной базы Колледжа;

– обеспечение безопасности работников и обучающихся Колледжа.

Формы обучения: очная, заочная.

Перечень специальностей в ГБПОУ «Миасский машиностроительный колледж» по специальностям представлены в Таблицах

456318, г. Миасс, пр-т Октября, д.1, каб. 212, д.4, тел. 53-38-86, 8-902-614-33-49

од	**Наименование специальности**	**Основное общее образование (9 классов) Очная форма обучения**		**Среднее общее образование(11 классов)Заочная форма обучения**	
		Бюджет	Внебюджет	Бюджет	Внебюджет
09.02.07	Информационные системы и программирование	3 года 10 месяцев			
13.02.11	Техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям)	3 года 10 месяцев			
22.02.06	Сварочное производство	3 года 10 месяцев			
27.02.07	Управление качеством продукции, процессов и услуг (по отраслям)	2 года 10 месяцев			
13.01.10	Электромонтер по ремонту и обслуживанию электрооборудования (по отраслям)	2 года 10 месяцев			

Перечень специальностей по специальностям.456304, г. Миасс, Предзаводская площадь, д.1, каб. 113, тел. 55-47-55

Код	Наименование специальности	Основное общее образование (9 классов) Очная форма обучения		Среднее общее образование(11 классов)Заочная форма обучения	
		Бюджет	Внебюджет	Бюджет	Внебюджет
15.02.08	Технология машиностроения	3 года 10 месяцев			
22.02.03	Литейное производство черных и цветных металлов	3 года 10 месяцев			

23.02.02	Автомобиле- и тракторо-строение				3 года 10 месяцев
23.02.07	Техническое обслуживание и ремонт двигателей, систем и агрегатов автомобилей		3года 10 меся-цев		
8.02.01	Экономика и бухгалтерский учет (по отраслям)	2 года 10 меся-цев			
38.02.03	Операционная деятельность в логистике	2 года 10 меся-цев			

Перечень профессий по программам подготовки квалифицированных рабочих, служащих. 456304, г. Миасс, ул. Гвардейская, д.1А, каб. 104, тел. 55-00-71

Код	Наименование специальности	Основное общее образование(9 классов) Очная форма обучения		Среднее общее образование(11 классов)Заочная форма обучения	
		Бюджет	Внебюд-жет	Бюд-жет	Внебюд-жет
15.01.05	Сварщик (ручной и частично механизированной сварки (наплавки)	2 года 10 меся-цев			
15.01.33	Токарь на станках с числовым программным управлением	2 года 10 месяцев			
15.01.35	Мастер слесарных работ	2 года 10 меся-цев			
23.01.17	Мастер по ремонту и обслужи-ванию автомобилей	2 года 10 меся-цев			

Структура управления образовательной организацией.

Управление колледжа осуществляется в соответствии с законодательством РФ.

Управляет колледжем единолично директор. В ГБПОУ «МиМК» действуют следующие коллегиальные органы управления: Общее собрание работников и студентов колледжа, Совет колледжа, Педагогический совет, Попечительский совет, Совет родителей.

Общее собрание работников и студентов колледжа (далее общее собрание) проводится не реже 1 раза в год. В состав Общего собрания входят директор, категории работников (представители), представители родителей (законных представителей) несовершеннолетних студентов, представители студентов. Председатель, секретарь Общего собрания избираются Общим собранием на срок 3 года.

На общем собрании работников и студентов в количестве 7 человек сроком на 3 года избирается Совет колледжа. В его состав входит директор, представители всех категорий работников, представители родителей представители студентов, представители заинтересованных организаций в равных долях. Решения совета оформляются протоколами и вступают в силу с даты их подписания председателем Совета. Члены Совета Учреждения избираются Общим собранием открытым голосованием. Председатель, секретарь Совета колледжа избираются членами Совета на первом заседании. Решения Совета принимаются открытым голосованием.

В колледже действует Педагогический совет, состоящий категории педагогических работников. Решения педсовета принимаются открытым голосованием и оформляются протоколами. Решения педсовета являются рекомендательными для коллектива колледжа. Решения педсовета, утвержденные приказом техникума, являются обязательными для исполнения.

Студенческий совет формируется из представителей студентов – по одному представителю от группы. Избирается на общем собрании студентов в количестве одного человека от каждой группы сроком на 3 года. Решения студенческого совета принимаются открытым голосованием.

Попечительский совет колледжа действует в соответствии с действующим законодательством. В него входят представители администрации и работники колледжа, обучающиеся и их родители (законные представители), , представители работодателей, социальных партнеров, в количестве не менее 5 человек сроком на 3 года. Попечительский совет избирает из своего состава председателя и секретаря, определяет руководящие и контрольно-ревизионные органы совета. Права и обязанности участников указываются в положении о Попечительском совете. Решения принимаются открытым голосованием и оформляются протоколами.

Совет родителей является представительным органом родителей (законных представителей) несовершеннолетних студентов. В состав Совета родителей входят по одному представителю родителей от группы, которые избираются на родительских собраниях в группе на срок в соответствии с Положением о Совете родителей. Совет созывается по мере необходимости по решению председателя, по решению половины членов совета, по решению директора. Решения Совета принимаются открытым голосованием большинством голосов.

В ГБПОУ «МиМК» действуют коллегиальные органы управления:

- Общее собрание (конференция) работников и обучающихся ГБПОУ «МиМК»;
- Совет ГБПОУ «МиМК»;
- Совет родителей (законных представителей) обучающихся ГБПОУ «МиМК»;
- Студенческий совет ГБПОУ «МиМК»;
- Педагогический совет ГБПОУ «МИМК»;
- Попечительский совет ГБПОУ «МИМК».

Взаимосвязь между подразделениями ГБПОУ «Миасский машиностроительный колледж» представлена на Рисунке 4.

ОРГАНИЗАЦИОННАЯ СТРУКТУРА
государственное бюджетное профессиональное образовательное учреждение
«Миасский Машиностроительный колледж»

УТВЕРЖДЕНА
приказом ГБПОУ «МиМК»
от 20.10.2023 г. № 736

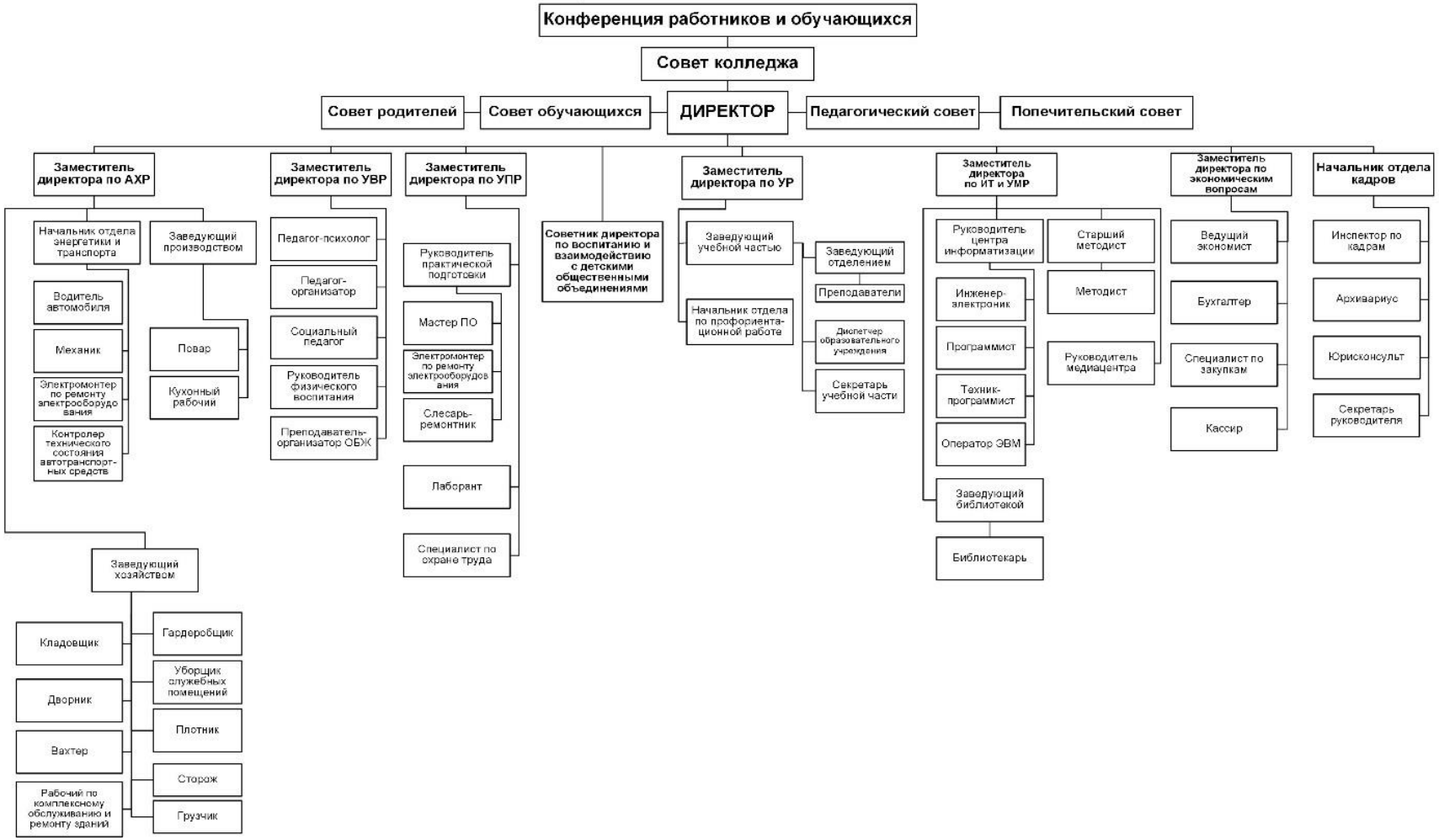

Рисунок 4– Взаимосвязь между подразделениями ГБПОУ «Миасский машиностроительный колледж»

Материально-техническое обеспечение и оснащенность образовательного процесса:

Учебно-материальная база колледжа по объему и содержанию отвечает лицензионным требованиям и условиям осуществления образовательной деятельности по образовательным программам, заявленным в лицензии. Образовательный процесс в колледже организован в зданиях и помещениях общей площадью – 29001,0 м². Существующие площади позволяют вести обучение в одну смену. Действующая структура функционирования Миасского машиностроительного колледжа обеспечивает возможность получения обучающимися профессионального образования на 4-х образовательных площадках:

Адрес площадки	**Площадь**
456318, Россия, Челябинская область, г. Миасс, пр. Октября, д.1	7690,2
456318, Россия, Челябинская область, г. Миасс, пр. Октября, д. 4	9594,3
456304, Россия, Челябинская область, г. Миасс, пл. Предзаводская, д.1	4187,0

Средства обучения и воспитания

Сведения об учебных, культурно-бытовых и административно-служебных помещениях образовательного учреждения

Наименование показателей Наличие в учебном заведении (ед.):	Количество
Учебных корпусов:	4
Кабинетов	63
Лабораторий	31
Учебно-производственных мастерских	13
Библиотек	3
Читальных зала	3
Актовых залов	3
Спортивных залов	4
Тренажерных залов	3
Спортивные площадки	3
Тиров	1
Столовых	3

Для изучения общеобразовательной программы в колледже имеются кабинеты общеобразовательных дисциплин. Наличие их представлено в следующей таблице 3.

Таблица 4- Перечень кабинетов общеобразовательных дисциплин

№№	Наименование кабинетов (ед.)	АСиМО	ЦПКРС	ЭРТиТ	ИТОГО
1.	Географии и экологии	1	1	2	4
2.	Иностранного языка	2	2	3	7
3.	Информатики	1	1	2	4
4.	Истории и обществознания	1	1	2	4
5.	Математики	1	1	2	4
6.	Основ безопасности жизнедеятельности	1	1	1	3
7.	Русского языка и литературы	1	1	1	3
8.	Физики	1	1	1	3
9.	Физической культуры	1	1	2	4
10.	Химии и биологии	1	1	2	4

Информация о материально-техническом обеспечении учебного процесса в ГБПОУ «Миасский машиностроительный колледж»

Реализуемая образовательная программа среднего профессионального образования

09.02.07 Информационные системы и программирование

11.01.01 Монтажник радиоэлектронной аппаратуры и приборов

13.01.10 Электромонтер по ремонту и обслуживанию электрооборудования (по отраслям)

13.02.11 Техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям)

15.01.05 Сварщик (ручной и частично механизированной сварки (наплавки)

15.01.30 Слесарь

15.01.33 Токарь на станках с числовым программным управлением

15.01.35 Мастер слесарных работ

15.02.08 Технология машиностроения

15.02.15 Технология металлообрабатывающего производства

19.02.10 Технология продукции общественного питания

22.02.03 Литейное производство черных и цветных металлов

22.02.06 Сварочное производство

23.01.17 Мастер по ремонту и обслуживанию автомобилей

23.02.02 Автомобиле- и тракторостроение

23.03.03 Техническое обслуживание и ремонт автомобильного транспорта

27.02.04 Автоматические системы управления

27.02.07 Управление качеством продукции, процессов и услуг (по отраслям)

38.02.01 Экономика и бухгалтерский учет (по отраслям)

38.02.03 Операционная деятельность в логистике

43.02.15 Поварское и кондитерское дело

Специально оборудованные учебные кабинеты для инвалидов и лиц с ОВЗ

В состав учебно-производственных мастерских входят слесарные, механические, электромонтажные и сварочные мастерские, учебно-производственный участок на базе столовой по адресу пр. Октября, 4. Они обеспечивают возможность проведения учебных практик для получения первичных профессиональных навыков по следующим рабочим профессиям: слесарь механосборочных работ, токарь, слесарь по ремонту автомобилей, монтажник радиоэлектронной аппаратуры и приборов, электромонтер по ремонту и обслуживанию электрооборудования, сварщик, повар, кондитер.

1. Наличие спортивных объектов

В колледже имеются:

- 4 спортивных зала,
- 3 тренажерных зала,

- 4 лыжные базы,
- 3 спортивные площадки,
- 1 тир.

Для проведения лыжной подготовки имеются беговые лыжи в достаточном количестве для проведения учебных занятий. Кроме того, есть 7 велосипедов; для проведения занятий и тренировок имеется 12 теннисных столов.

Объекты спорта, приспособленные для пользования инвалидами и лицами с ОВЗ

Библиотека колледжа имеет в своей структуре 3 библиотеки, с 3 абонементами, книгохранилищами и читальными залами на 76 посадочных мест.

Учебная литература (учебники, учебные пособия) соответствует нормативным требованиям (наличие грифа, количество экземпляров на одного обучающегося, доступность учебников для студентов). Ежегодно фонд библиотеки пополняется новой учебной, учебно-методической и справочной литературой.

В читальных залах библиотеки оборудованы автоматизированные рабочие места читателей с выходом в сеть Интернет для работы обучающихся и педагогов во внеурочное время. Доступ к сети Интернет открыт на бесплатной основе в период рабочего времени библиотеки.

Таблица 5– Библиотеки

	Учебная литература		**Учебно-методическая литература**	**Справочная литература**	**Дополнительная и худ. литература**	**Общий фонд**
	По общеобр. дисциплинам	**По спец. дисциплинам**				
Состояние библиотечного фонда (экз.)	15373	57746	16049	5460	23802	118430
ЭБС «Знаниум» (экз.) по СПО	117	1887	978	566	2340	36686
ИТОГО:	***15490***	***59633***	***17027***	***6026***	***26142***	***155116***

Состояние библиотечного фонда (экз.)	15373	57746	16049	5460	23802	118430
ЭБС «Знаниум» (экз.) по СПО	117	1887	978	566	2340	36686
ИТОГО:	***15490***	***59633***	***17027***	***6026***	***26142***	***155116***

Между колледжем и ООО «Знаниум» заключен договор о предоставлении доступа к электронной библиотечной системе «Знаниум» на 1300 точек доступа. Обучающиеся и педагоги имеют возможность пользоваться учебной литературой и периодическими изданиями ЭБС «Знаниум» с любого автоматизированного места в колледже, а также с домашних компьютеров и смартфонов, в том числе инвалиды.

Ежегодно фонд библиотеки пополняется новой учебной, учебно-методической и справочной литературой, в том числе и через ЭБС. С целью качественного пополнения книжного фонда новой литературой библиотека работает с различными книготорговыми фирмами и издательствами: «Академия», «ИНФРА-М», «Машиностроение», «Феникс» и другими. В мае 2020 года для преподавателей и студентов предоставлен тестовый доступ к ЭБС «Университетская библиотека online». Фонд библиотеки колледжа соответствует требованиям ФГОС СПО и рабочим учебным планам по специальностям и профессиям.

Электронные образовательные ресурсы разработаны и размещены в автоматизированной системе управления «ProCollege» (на основе Moodle). Для доступа к этой системе у всех обучающихся колледжа имеются логины и пароли.

Все компьютеры в колледже объединены в единую локальную сеть, со всех компьютеров, задействованных в образовательном процессе, имеется доступ к сети Интернет, скорость доступа 50 Мб/сек.

Для входа в данную систему у всех обучающихся, в том числе и у лиц с ограниченными возможностями, имеется логин и пароль.

В колледже разработан и поддерживается сайт по адресу: miassmk.ru. Основным информационно-ресурсными компонентам Сайта является первая (главная) страница сайта, которая содержит: − полное название колледжа; − логотип или фотографию; − меню, отображающее разделы сайта; − ленту новостей (или ссылку на страницу, содержащую ленту новостей); − контактную информацию (адрес, телефон, электронная почта). Работает электронная почта miassmk@mail.ru.

Главная страница сайта ГБПОУ «Миасский машиностроительный колледж» показана на Рисунке 5

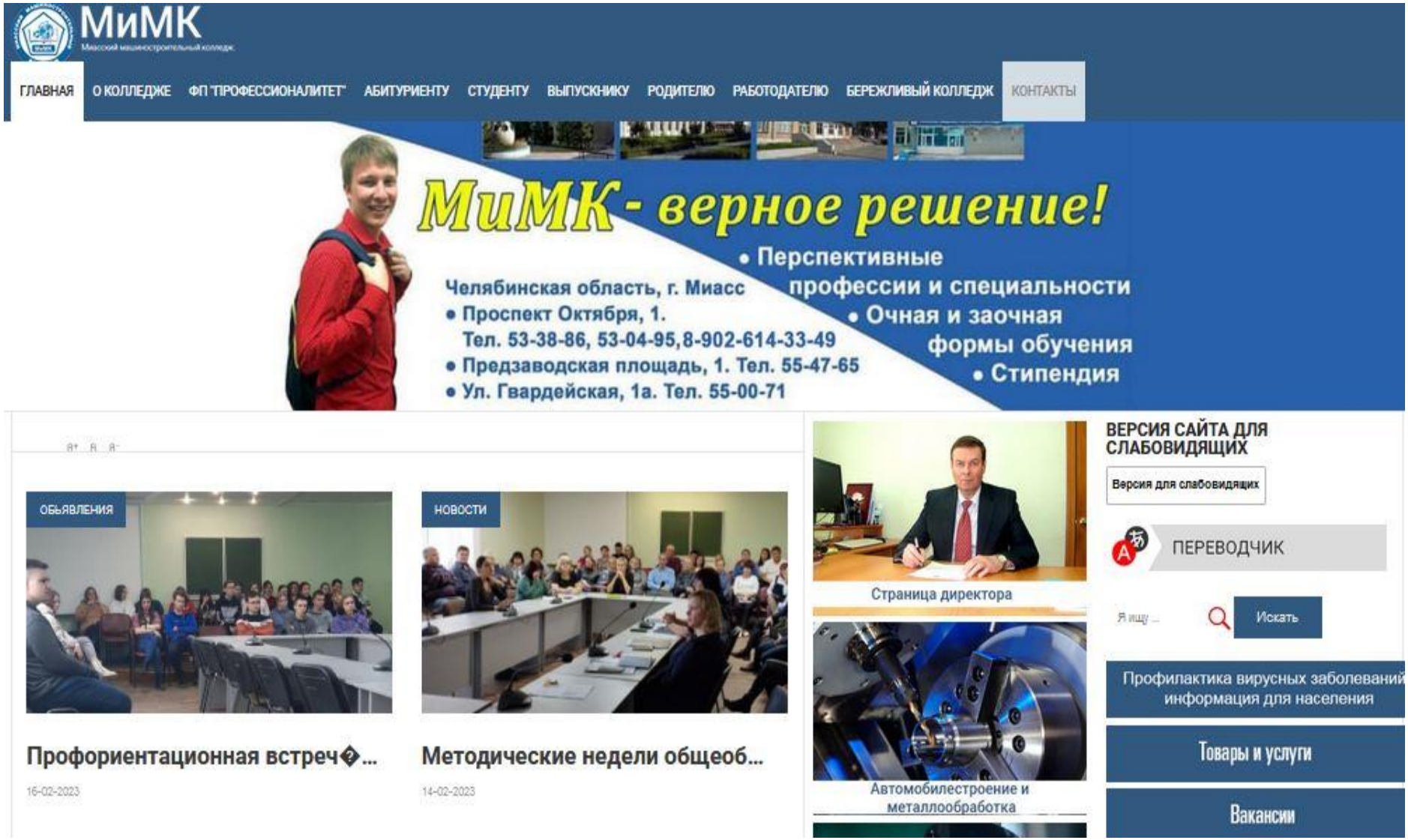

Рисунок 5- Сайт колледжа МиМК

Сайт предназначен для представления интересов в глобальной сети Интернет, получения доступа пользователей Интернет к информационным и научным ресурсам, развития связей с другими организациями, установления персональных контактов, а также для получения оперативной информации всеми участниками образовательного процесса, и призван способствовать:

– созданию целостного позитивного образа в стране, как учебного заведения с многолетними традициями в области образования и большим научным потенциалом;

– оперативному и объективному информированию всех заинтересованных лиц о наиболее значимых событиях, происходящих в колледже;

– осуществлению обмена информацией между всеми участниками образовательного процесса;

– повышению качества обучения на основе использования Интернет-технологий.

На сайте размещается официальная информация об основных сферах деятельности колледжа: образовательной, научной и общественной деятельности, традициях и истории, общественных организациях, функционирующих в колледже, структурных подразделениях, сотрудниках и основных событиях.

Задачи Сайта:

− информационное обеспечение участников образовательного процесса о деятельности колледжа, повышение открытости и доступности образовательного процесса;

− презентация колледжа, достижений, обучающихся и педагогического коллектива, его особенностей, истории развития, реализуемых образовательных программ;

− формирование позитивного имиджа колледжа, формирование комплексной информационной среды;

− демонстрация опыта деятельности и достижений педагогов и обучающихся, распространение инновационного опыта;

– стимулирование творческой активности педагогов и обучающихся;

– осуществление обратной связи с участниками образовательного процесса и социальными партнерами.

Сайт создаётся под руководством заместителя директора по информационным технологиям.

Создание, содержание и обслуживание сайта осуществляется техником вычислительного центра и администратором сайта. Директор колледжа несёт ответственность за информацию, размещённую на сайте.

Информационный ресурс Сайта формируется в соответствии с деятельностью всех структурных подразделений колледжа, его преподавателей, работников, обучающихся, родителей и прочих заинтересованных лиц.

Сайт колледжа содержит несколько разделов:

– Сведения об организации (включает в себя общие сведения об образовательной организации, структуру и органы управления образовательной организации, сведения об учредителях, историю организации, о педагогическом и руководящем составе ит.п.).

– Студенту (подразделы: очное отделение, заочное отделение, трудоустройство, советы психолога, перспективы обучения в высших учебных заведениях и т.д.).

– Абитуриенту (подразделы: объявление о приеме, приемная компания, специальности, правила приема обучающихся, перечень документов для поступления в К-ИИТ, заявление абитуриента и т.д.).

– Новости (раздел, в котором публикуется информация о всех предстоящих событиях в колледже).

В целом, на сайте можно получить доступ ко всей необходимой, в рамках учебного процесса, информации.

Во время прохождения педагогической практики основная работа проходила с группой студентов 261 (2 курс), обучающихся по специальности: «Технология машиностроения», основные сведения о специальности: обучение производится на базе основного общего образования – 3 года 10 месяцев.

2.2. Требования законодательных актов к системе защиты информации при использовании виртуальных сред в колледже ГБПОУ «МиМК»

Цифровизация всего населения является стратегической задачей государственной политики. Для достижения результатов в этой области на законодательном уровне государства разрабатываются, рассматриваются и внедряются различные меры, вводятся в действие различные федеральные проекты.

Указ Президента РФ от 09.05.2017 №203 «О Стратегии развития информационного общества в РФ на 2017–2030 годы» ставит приоритетные задачи для достижения показателей цифровизации населения различных категорий. В ней года показаны объемы, сроки перехода оказания государственных услуг на цифровой вид и можно наблюдать систему государственных услуг в динамике.

Реализованы в 2023 году следующие задачи Стратегии:

Министерство просвещения Российской Федерации провело модернизацию правил применения организации электронного обучения в профессиональных образовательных организациях. В них установлен регламент, перечислены основные отличия и преимущества использования не только полного объема, но и частичного применения технологий дистанционного образования в учебном процессе.

Реализуемые в настоящее время федеральные проекты «Создание современной образовательной среды для школьников», «Цифровая школа», «Современная цифровая образовательная среда в Российской Федерации» решают проблемы доступности образования в школах, повышают уровень технологической оснащенности, программного обеспечения и обеспечивают доступность качественного образования. Они обеспечивают колоссальный прорыв и гарантируют равные шансы развития для обучающихся из разных населенных пунктов.

В нормативно-правовой документации защита от угроз в виртуальных образовательных пространствах представлена в документах:

– Доктрина информационной безопасности Российской Федерации,

утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646.

– Концепция информационной безопасности детей, утвержденная распоряжением Правительства РФ от 2.12.2015 г. № 2471-р.

– Федеральный закон РФ от 27.07. 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»

– Федеральный закон Российской Федерации от 29 декабря 2010 г. № 436- ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

– Федеральный закон РФ от 27.07. 2006 г. № 152-ФЗ «О персональных данных»

– Постановление Правительства Российской Федерации от 17.11.2007 г. №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

– Приказ Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 г. № 5/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».

- Федеральный закон Российской Федерации от 24 июля1998 г. № 124-ФЗ «Об основных гарантиях прав ребёнка в Российской Федерации»;

- ст. 4 Закона Российской Федерации от 27 декабря1991 №2124 -1 «О средствах массовой информации»;

- ст.5 Федерального закона Российской Федерации от 13.03.2006 № 38-ФЗ «О рекламе»;

- Постановление Государственной Думы Федерального собрания РФ от 24.11.2000г. № 843-IIIГД «О государственной политике в области телевизионного вещания и радиовещания»;

- Письмо Роспотребнадзора от 17.09.2008г. № 01/10237-8–32 «О ме-

рах, направленных на нераспространение информации, наносящей вред здоровью, нравственному и духовному развитию детей и подростков».

Систему мер по защите от угроз в информационной среде описывает Доктрина. В ней дана оценка информационной защиты, способы обеспечения нацбезопасности страны от информационных угроз, раскрыта тактика реализация мероприятий по внедрению защитных мер.

Реализация мер по защите должна реализоваться параллельно с внедрением информационных технологий и действовать на опережение и гарантировать снижение различных угроз в информационных пространствах. Так как цифровизация внедряется во все сферы жизни и становится все более популярна у различных слоев населения, то у различных незаконопослушных граждан возникает возможность ввести в заблуждение добропорядочного гражданина и навязать ему взгляды экстремистского содержания или обмануть.

Прописываются в Доктрине стратегии информационной безопасности в оборонной промышленности, экономической, технологической и научной среде, госбезопасности, образовательной области, равноправия и стратегического партнерства.

В экономической, технологической и научной среде сделаны акценты на:

-обеспечение и потенциал кадрового состава, который благодаря использованию образовательных мероприятий будет участвовать в организации информационной безопасности

-цифровизация граждан с дошкольного возраста приведет к росту цифровой грамотности и тем самым обеспечит высокий уровень защиты населения от угроз в информационных средах.

В ответственном подходе к защите от угроз подрастающего поколения заключаются формулировки Концепции информационной безопасности детей. В ней учитываются возрастные, психологические, индивидуальные осо-

бенности детей и подростков. Указаны способы защиты и мероприятия по организации защиты по сохранению позитивного мышления, адаптации при использовании виртуальных сред.

Стратегия государственной политики в организации информационной безопасности в отношении детей, семьи и образовательных организаций сформулирована и представлена по следующим направлениям:

- цифровизация и информатизация подрастающего поколения, повышение навыков ответственного подхода использования электронных ресурсов;
- повышение культа семьи, традиционных ценностей, социализация и расширение совместной деятельности, доверительных отношений и общения различных возрастных групп;
- воспитание ответственной личности по отношению к окружающему миру, людям и обществу, формирование нравственной личности, ответственного гражданина своей страны со здоровыми моральными принципами;
- традиционное половое воспитание, толерантность к культурным ценностям различных многонациональных направлений и конфессий, формирование навыков познавательной, нравственной активности обучающихся по различным направлениям;
- формирование навыков самовыражения, мотивация на творческое развитие личности, повышения уверенности в собственных силах, способствование прогрессу различных явлений.

Концепция призывает к консолидации всех пользователей информационных пространств организовать деятельность с минимальными рисками проявления недопустимого поведения подростков, агрессии, экстремизма, разжигания межнациональной розни, пропаганды вредных привычек.

Для организации регулирования информационных сред на государственном уровне проводятся профилактические мероприятия и разрабатывается нормативная документация.

Чтобы защитить подростков от угроз информационных пространств, обеспечить их психофизическое здоровье нужно систематически проводить мероприятия, которые способствуют формированию информационной культуры обучающихся профессиональных образовательных организаций для понимания самих базовых основ и понятий и применения этих компетенций не только в образовательном процессе, но и в повседневной жизни, а также проектировать их на остальных членов общества[9].

Повышение культа семьи, традиционных ценностей, социализация и расширение совместной деятельности, доверительных отношений и общения различных возрастных групп на государственном уровне стимулирует возникновение защиты по сохранению позитивного мышления, адаптации при использовании виртуальных сред у подростков.

Законом РФ «О защите детей от информации, причиняющей вред их здоровью и развитию», «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию», и законодательными актами по ограничению доступа к противоправной информации в сети Интернет» определено понятие информационной безопасности.

Для определения информационной безопасности, использовано следующие формулировки состояние, при котором дети гарантированно на законодательном уровне защищены от угроз от информационных источников, и они не оказывают негативного воздействия на психологическое состояние и здоровье детей и подростков.

И четко указаны те виды информации, которые составляют угрозы для детей:

- призывы к нанесению вреда психическому и физическому здоровью, склонение к суицидальным действиям;
- призывы к распространению или употреблению наркотиков, психотропных препаратов, табакосодержащие изделия, алкоголь, пиво и содержащиеся в них напитки;

- призывы к участию в азартных играх, склонение к половой жизни, насилию и жестокости к окружающим людям, животным;
- отрицание традиционных ценностей, уход от отношений и общения различных возрастных групп.

При передаче информации посредством информационно-телекоммуникационных сетей законодательство обязывает операторов сотовых связи ограничивать доступ к вредоносным и запрещенным источникам информации и блокировать путем установкой специализированного программного обеспечения и ограждать от причинения вреда психологическому состоянию и здоровью детей и подростков.

Операторам сетей регламентированы законом «Об информации, информационных технологиях и о защите информации» способы поиска, передача, распространение информации и обеспечение ее защиты.

Законодательством осуществляется контроль информационных сред, технологий и мер по защите от угроз в информационных пространствах на основании:

- способы поиска, передача, распространение информации и обеспечение ее защиты можно только на основании разрешенных законных методов;
- на сайтах федеральных, региональных и муниципальных организаций должна быть размещена вся актуальная информация и находиться в свободном доступе;
- содержание информации, размещенной на сайтах федеральных, региональных и муниципальных организаций может быть ограничено только на законодательном уровне;
- размещенная и находящаяся в свободном доступе информация должна своевременно обновляться и быть достоверной;
- представление информации должно быть на государственном языке и обеспечивать доступность для всех языковых групп;
- информационное пространство сайтов гарантирует надежность и

безопасность в применении у пользователей;

− размещенная и находящаяся в свободном доступе информация не распространяет и не собирает персональные данные, не использует для распространения без личного согласия;

− обеспечивает равноправный доступ на территории все страны.

Правовой регламент выделяет четыре типа информации:

1.общедоступную – информация, которая распространяется без ограничений;

2.ограниченную – содержит информацию, которую законодательство РФ ограничивает к распространению.

Также можно выделить категорию информации, которая может быть распространена по согласию участников, которые находятся во взаимодействии и информацию, которая в соответствии с действующей нормативно-правовой базой обязательна к представлению.

В законе РФ «Об информации, информационных технологиях и о защите информации» перечислены требования к страницам сайтов, их адресам, доменным именам, указаны реестры, которые содержат запрещенную информацию и подлежат блокировке [14].

Блокируются в интернет-пространстве включенные в запрещенный реестр сайты:

- информация с порнографическим содержанием и пропагандой сексуальной распущенности
- информации о способах, методах разработки, изготовления и использования к распространению или употреблению наркотиков, психотропных препаратов, табакосодержащие изделия, алкоголь, пиво и содержащиеся в них напитки;
- информация с призывом к нанесению вреда психическому и физическому здоровью, склонение к суицидальным действиям;
- информации об отрицании традиционных ценностей, уход от отношений и общения различных возрастных групп;

- информации, направленной на склонение или иное вовлечение несовершеннолетних к участию в азартных играх, склонение к половой жизни, насилию и жестокости к окружающим людям, животным.

При поступлении сигнала о том, что запрещенная информация содержится на том или ином сайте, его включают в запрещающий реестр. Оператор обязан ознакомить владельца сайта с новыми сведениями, заблокировать и удалить все сведения данного сайта для нераспространения запрещенной к распространению информации.

Владелец сайта обязан после уведомления оператором связи экстренно заблокировать и удалить все сведения данного сайта для нераспространения запрещенной к распространению информации.

Информационная защищенность представлена в законе «Об информации, информационных технологиях и о защите информации».

Технические сбои в программном обеспечении при незаконном доступе, проведении действий по распространению, копированию, блокировке и уничтожению операторы связи и владельцы сайтов должны своевременно обнаруживать и предупреждать все сбои. Обеспечение восстановления данных при применении неправомерных действий также лежат в зоне ответственности операторов информационных сетей.

Закон «О персональных данных» прописывает основные принципы защиты информации персональных данных, которые относятся к конфиденциальным [13].

Законом гарантировано, что личная информация и персональные данные не могут быть информацией, которая может быть в свободном доступе, она носит конфиденциальный характер и не подлежит распространению без личного согласия. Так же установлено, что существует информация, которая составляет государственную тайну.

Созданная в рамках правового поля система отправки персональных данных четко определяет угрозы конфиденциальности информации и определяет концепцию по преодолению опасности распространения:

- персональные данные необходимо обеспечить мероприятиями по защите при проведении работ по их обработке;
- работники организаций, которые в рамках своих должностных инструкций работают с конфиденциальной информацией, несут персональную ответственность при проведении действий, связанных с их обработкой, этот факт необходимо учесть в их работе;
- разработанный локальный нормативный акт, регламентирующий способы и порядок нераспространения данных, и безопасные сервисы по их передаче.

Работников организации, которые в рамках своих должностных инструкций работают с конфиденциальной информацией, включают в перечень сотрудников, которые могут это делать. Они несут за это персональную ответственность.

Учитывая результаты анализа нормативно-правовой документации в области организации защиты в информационной среде, можно прийти к выводу, что в данной сфере существуют недоработки.

Отсутствие конкретных мероприятий, механизмов решения и показателей при реализации федеральных проектов, которые только показывают направления цифровизации и информатизации и не показывают масштабы данных задач.

Выявленные недоработки при внедрении национальных проектов показывают многозадачность разносторонних сред, не в полном объеме решающие проблемы развития образования и прогресса информатизации.

Процесс цифровизации различных уровней образования не имеет равного обеспечения техническими средствами обучения и программным обеспечением.

Конкретные механизмы решения и показатели реализации в сере образования на различных уровнях представлены не пропорционально.

Также проведение цифровизации образования при реализации федеральных проектах рассчитано провести в условиях традиционной организации и не в условиях трансформации и модернизации.

Существующая реальность требует современных и модернизированных, действующих на опережающее развитие способов цифровизации и информатизации всех уровней образования на равной основе.

Выявленные проблемы необходимо решать путем уточнения целевых показателей и подойти системно к выполнению мероприятий.

2.3. Методика оценки угроз безопасности информации при использовании виртуальных сред в колледже

В основу разработки методики оценки угроз безопасности информации при использовании виртуальных сред в колледже легла утвержденная Федеральной службой по техническому и экспортному контролю 05.02.2021 г «Методика оценки угроз безопасности информации».

1. Общие положения

1.1. Методика оценки угроз безопасности информации при использовании виртуальных сред в колледже (далее - Методика) разработана в соответствии с федеральной **Методикой оценки угроз безопасности информации»**.

1.2. Методика определяет порядок и содержание работ по определению угроз безопасности информации, реализация (возникновение) которых возможна в информационных системах колледжа, автоматизированных системах управления, информационно-телекоммуникационных сетях, облачных инфраструктурах (далее - системы и сети), а также по разработке моделей угроз безопасности информации систем и сетей.

1.3. Методика применяется для определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях, отнесенных к информационным системам колледжа, информационным системам персональных данных.

1.4. В документе не рассматриваются методические подходы по оценке угроз безопасности информации, связанных с нарушением безопасности шифровальных (криптографических) средств защиты информации, а также угроз, связанных с техническими каналами утечки информации.

1.5. Методика ориентирована на оценку угроз безопасности информации, возникновение которых обусловлено действиями нарушителей.

1.6. В Методике используются термины и определения, установленные законодательством Российской Федерации и национальными стандартами в области защиты информации и обеспечения информационной безопасности.

1.7. Положения настоящей Методики применяются для оценки угроз безопасности информации в системах и сетях колледжа, решение о создании или модернизации (развитии) которых принято после даты ее утверждения, а также в эксплуатируемых системах и сетях.

Модели угроз безопасности информации систем и сетей, разработанные и утвержденные до утверждения настоящей Методики, продолжают действовать и подлежат изменению в соответствии с настоящей Методикой при развитии (модернизации) соответствующих систем и сетей.

2. Порядок проведения оценки угроз безопасности информации

Чтобы определить угрозы информационной безопасности необходимо определить системы и архитектурные сети, в которых потенциально могут создаваться условия для возникновения и распространения различных угроз информационных систем.

При изучении условий для возникновения и распространения различных угроз информационных систем необходимо решать следующие задачи:

− спрогнозировать последствия, возникающие при наступлении момента нарушения безопасности информационной среды колледжа;

− выяснить, какие объекты могут быть наиболее уязвимые и провести обследование операционных систем колледжа;

− оценить потенциальных нарушителей, которые заинтересованы и мотивированы в создании угроз колледжу;

− провести «тренировку» решения проблем, возникших при возникновении условных угроз.

Произвести оценку потенциала возможных угроз информационной безопасности можно по следующим признакам:

− списки угроз информационной безопасности размещены в базе данных ФСТЭК России (bdu.fstec.ru);

− вероятность предполагаемых негативных последствий воплощения угрозы в жизнь;

− пути вероятных атак на информационные системы размещены в интернет – пространстве (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

− отсутствие информации о системах в соответствии с требованиями в данной области;

− пользовательские соглашения не заключены, инфраструктурное содержание не соответствует действующему законодательству;

− сети не соответствуют описанию и назначению не соответствуют правовым актам РФ;

− не соответствие полномочий, которые взяли на себя операторы сети, технологическим процессам;

− при получении услуг пользователь получает ущерб.

Мероприятия по внедрению защитных мер от угроз информационной безопасности рекомендуется проводиться на принципах системности и реализовываться на каждом этапе использования виртуальных сред. При реализации защитных мер на таких условиях можно гарантировать обеспечение высокой степени защиты. Использование своевременных мер формирует эффективность противодействия постоянно модернизирующихся угроз.

Проведение тщательного анализа сетей по архитектуре, оценка потенциальных угроз формируют пути реализации предполагаемых способов защиты. Уточняются, какие объекты становятся наиболее уязвимыми и провести обследование операционных систем колледжа и оцениваются потенциальные

нарушители, которые заинтересованы и мотивированы в создании угроз колледжу. Система подвергается проверке в тестовом режиме работы.

Реализованные в соответствии с Методикой мероприятия способствуют спрогнозировать последствия, возникающие при наступлении момента нарушения безопасности информационной среды колледжа, выяснить, какие объекты могут быть наиболее уязвимые и провести обследование операционных систем колледжа, оценить потенциальных нарушителей, которые заинтересованы и мотивированы в создании угроз колледжу и провести «тренировку» решения проблем, возникших при возникновении условных угроз.

При принятии решений о применении тех или иных технологических мер для предотвращения угроз нужно делать осознанный выбор в пользу самых передовых способов, которые проверены и зарекомендовали себя в данной области на этапе планирования систем.

И тогда уже в процессе эксплуатации проделанная на подготовительном этапе работы по предотвращению проявлению угроз даст результаты и позволить оценить, насколько они позволили обеспечить функционирование безопасной информационной среды.

Внедрение цифровизации и безопасность среды в колледже обеспечивается сотрудниками Центра информатизации. В его состав входят руководитель Центра информатизации, инженер-электроник, техник –программист. Каждый сотрудник на своем уровне проводит мероприятия по внедрению защитных мер от угроз информационной безопасности на принципах системности и реализуют их на каждом этапе использования виртуальных сред. При реализации защитных мер обеспечивают высокую степень защиты и предпринимают своевременные по противодействию постоянно модернизирующихся угроз.

При необходимости проводятся консультации с операторами информационных систем.

Сотрудники Центра информатизации колледжа имеют знания и умения:

- ознакомлены с угрозами информационной безопасности, размещенными в базе данных ФСТЭК России;
- могут определить негативные последствия угроз;
- проводят оценку путей вероятных атак на информационные системы, размещённых в интернет;
- контролируют информацию о системах в соответствии с требованиями в данной области;
- способствуют заключению пользовательских соглашений и соответствию инфраструктурного содержания действующему законодательству;
- приводят в соответствие сетей описанию и назначению к правовым актам РФ;
- предотвращают получение ущерба от услуг пользователей.

Региональные операторы различных систем на постоянной основе проводят проверку защитных мер от угроз информационной безопасности, и дают рекомендации, тем самым обеспечивая внешнюю экспертную оценку эффективности работы Центра информатизации. При этом эксперты рекомендуют внедрять программные средства, которые работают в автоматическом режиме.

На каждом этапе реализации защитных мер в колледже от угроз информационной безопасности рекомендуется использование программных средств, которые работают в автоматическом режиме, тем самым проверка и тестирование систем проводится более детально и обнаружение угроз будет более эффективным.

При организации работы в колледже с использованием облачных технологий необходимо проводить оценку угроз не только для сетей, но и самих облачных технологий, так как информация, содержащаяся в них, должна быть подвержена проверке и оценке рисков. На рисунке 6 представлена схема проведения оценки угроз сетей и облачных технологий.

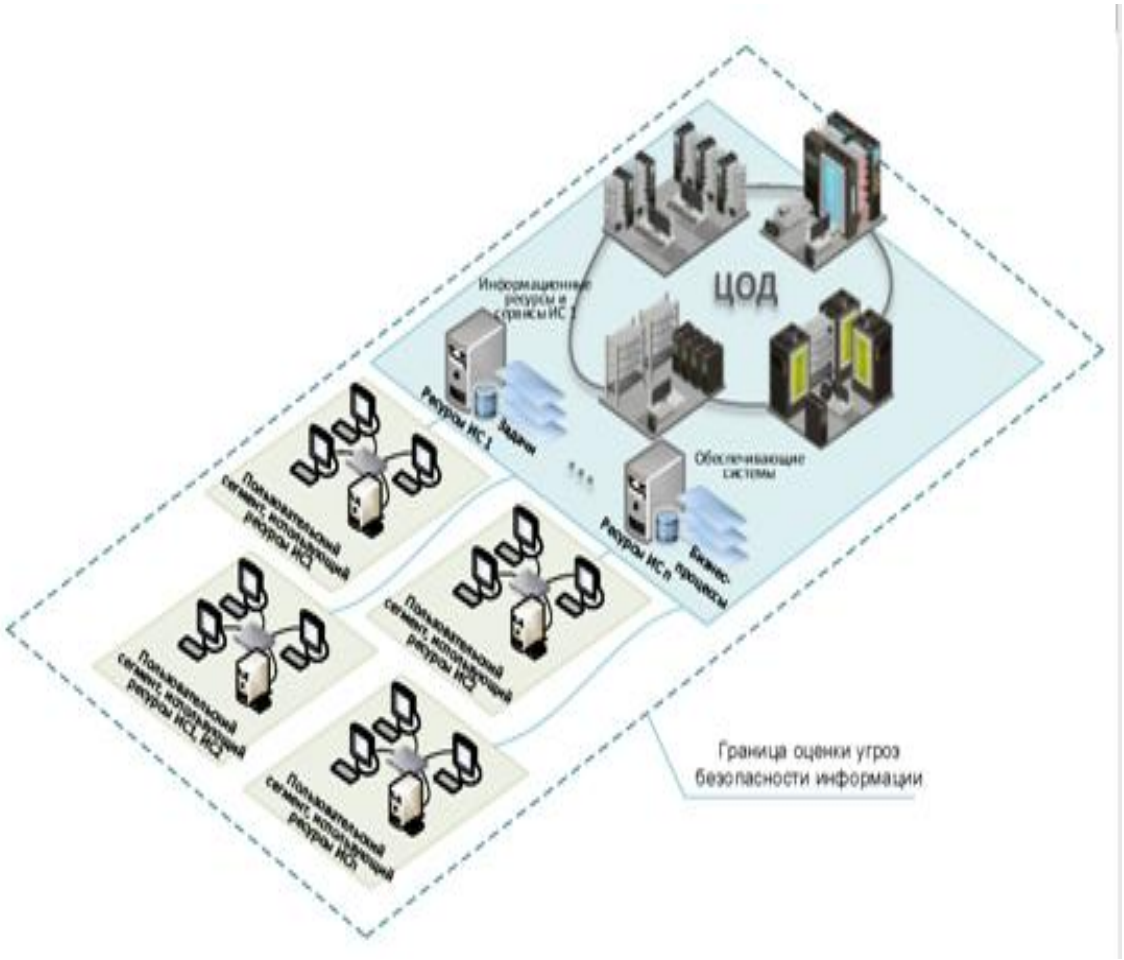

Рисунок 6 - Схема проведения оценки угроз сетей и облачных технологий

При организации работы в колледже на условии размещения сетей у поставщиков услуг необходимо проводить оценку угроз не только колледжных сетей, но и сетей, принадлежащей поставщикам. Данные работы необходимо проводить колледжу совместно с поставщиками услуг.

Поставщику услуг необходимо ответственно подойти к обеспечению безопасности, так как игнорирование потенциальных угроз может привести к нарушениям законодательства и скомпрометирует колледж.

Рассмотренная нами Методика предлагает структурную модель, содержащую анализ угроз безопасности информации, описывает сети, систему мер по предупреждению угроз.

Если оператор или владелец информации проводит работы в колледже, то оценку угроз не только колледжных сетей, но и сетей, принадлежащих операторам или владельцам информации. Данные работы необходимо проводить колледжу совместно с оператором или владельцем информации.

Модель должна обеспечивать стабильную защиту от угроз, как у подобных, так и разнообразных владельцев информации. Она должна реализовываться и давать эффективный результат и своевременно реагировать на современные вызовы. Для этого электронная версия Модели будет внедряться намного эффективней

Гибкость Модели обеспечивает постоянно меняющиеся потенциалы угроз и реализуется при:

- меняющейся нормативной документации;
- изменении способов обработки информационных потоков, архитектурных способов сборки;
- возникновении новых угроз при тестировании и выявлении несанкционированного доступа;

г) обновления банка данных угроз безопасности информации ФСТЭК России.

Для проведения мероприятий по предотвращению угроз безопасности информации необходимо:

1) обозначить опасности при возможном наступлении угроз безопасности информации;

2) выяснить, какие объекты могут быть наиболее уязвимые и провести обследование операционных систем колледжа;

3) оценить потенциальных нарушителей, которые заинтересованы и мотивированы в создании угроз колледжу.

Представим на рисунке 7 схему процесса оценивания безопасности информации колледжа.

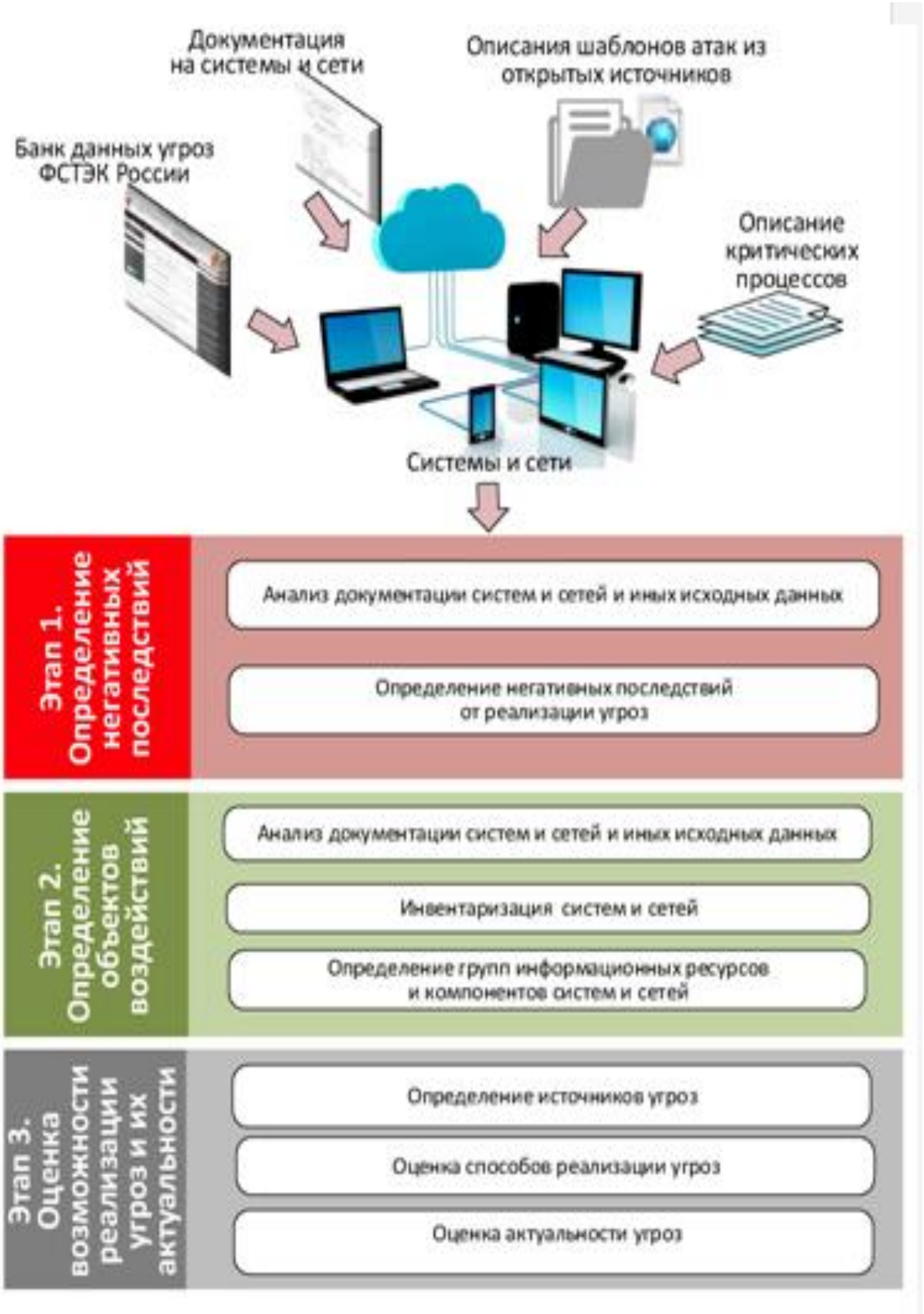

Рисунок 7- Схема процесса оценивания безопасности информации колледжа

3. Объекты групп информационных ресурсов

К ним можно отнести:

- личные данные пользователей, информация о системах, сетях, безопасности;
- техническое оборудование, хранилища информации;
- программное обеспечение;
- виртуализацию серверов;
- приложения;
- базы данных;
- веб-приложения;
- съемные носители информации;
- внешние жесткие диски;
- карты памяти;
- средства аутентификации;
- компьютерные сети;
- средства для защиты информации;
- средства управления и контроля;
- обеспечивающие системы.

Потенциал возможного отражения угроз необходимо оценивать по различным видам воздействий на информационные ресурсы, которые выражаются в:

- утечке персональных данных в полном или частичном объеме и нарушении конфиденциальности;
- доступ к персональным данным и защищенным данным;
- прерывание доступности к компонентам программы;
- изменение целостности, проникновение в служебные данные;
- нестабильное или не свойственное проведение операций для компонентов;
- нарушение способов передачи и функциональности.

На рисунке 8 представлена организация сетевого взаимодействия на различных уровнях.

Рисунок 8 - Организация сетевого взаимодействия

При организации воздействия на различных этапах происходит сетевое взаимодействие, которое трансформируется в зависимости от видов воздействия в процессе эксплуатации сетей. Оценка угроз безопасности при этом производится при изменяющихся условиях эксплуатационных условий.

Содержание услуг от поставщиков и их воздействие на объекты воздействия необходимо подвергать уценке оценке на содержание угроз безопасности в телекоммуникационной инфраструктуре, так как сервисное и программное обеспечение могут содержать потенциальные риски для пользователей.

Программное обеспечение, виртуальные серверы, каналы связи, которые могут использоваться колледжем, например, в рамках сетевого взаимодействия между различными профессиональными образовательными организациями, определяют границы потенциальных угроз и определяют как объекты взаимодействия.

Благонадежность поставщиков услуг в телекоммуникационной инфраструктуре влияет на выбор при принятии решений в определении и заключении сотрудничества.

Способ разграничения границ ответственности при выявлении угроз безопасности информации между оператором и поставщиком услуг показан на рисунке 9.

Рисунок 9- Способ разграничения границ ответственности при о выявлении угроз безопасности информации между оператором и поставщиком услуг.

4. Определение источников угроз безопасности информации

Угрозы безопасности создаются реальными объектами, которые заинтересованы в нанесении ущерба информационным системам путем получения незаконного доступа к программному обеспечению, сетям, персональным данным.

В создании потенциальных угроз заинтересованы данные группы:

- представители служб разведки недружественных государств;
- радикально - ориентированные группы;
- нарушители законодательства;
- хакеры;
- конкуренты;
- программисты;
- менеджеры программного обеспечения;
- провайдеры;
- менеджеры услуг;
- системные администраторы сторонних организаций;
- уволившиеся работники, имевшие доступ к системам.

Перечень объектов, которые заинтересованы в нанесении ущерба информационным системам колледжа можно расширить, некоторые нарушители могут одновременно попадать в различные группы.

Негативное воздействие на информационные системы колледжа создают реальные угрозы и приносят ущерб. Для того, чтобы обеспечить надежную защиту от вышеперечисленных источников угроз необходимо строго следовать Методике, учитывать возможности современных средств защиты и организовывать мероприятия на системной основе.

Каждая группа нарушителей заинтересована в достижении своих целей, которые перечислены в Методике. Оценка рисков проводится на основании этих соответствий.

Учитывая разный уровень мотивации, ресурсного обеспечения объектов, создающих угрозы, можно выделить разные возможности причинения ущерба от нарушителей:

1. базовые;
2. базовые повышенные;
3. средние;
4. высокие.

Возможности причинения ущерба нарушителей могут быть различными к тому или иному информационному пространству. Методика позволяет оценить уровень возможностей при реализации угроз безопасности.

Категории нарушителей можно представить по тем признакам, которые они получают при несанкционированном доступе к системам, данным:

1. сторонние – объекты, которым необходимо обойти систему авторизации и проникнуть в систему, к которой у них нет доступа и получить информацию или нанести ущерб программному обеспечению;
2. внутренние – объекты, которым не нужно обходить систему авторизации и проникать в систему, к которой у них есть доступ и они получают информацию для нанесения ущерба программному обеспечению.

Сторонние нарушители применяют агрессивное программное обеспечение, которое в специально созданных условиях для реализации сценариев по угрозам, наносят невосполнимый урон безопасности информационной среды.

Внутренние нарушители не применяют агрессивное программное обеспечение, которое в специально созданных условиях для реализации сценариев по угрозам, в отличие от сторонних, но также наносят ущерб безопасности информационной среды при не санкционном проникновении в среду.

На рисунке 10 показан процесс проникновения в систему сторонних нарушителей в систему, к которой у них нет доступа для получения информацию.

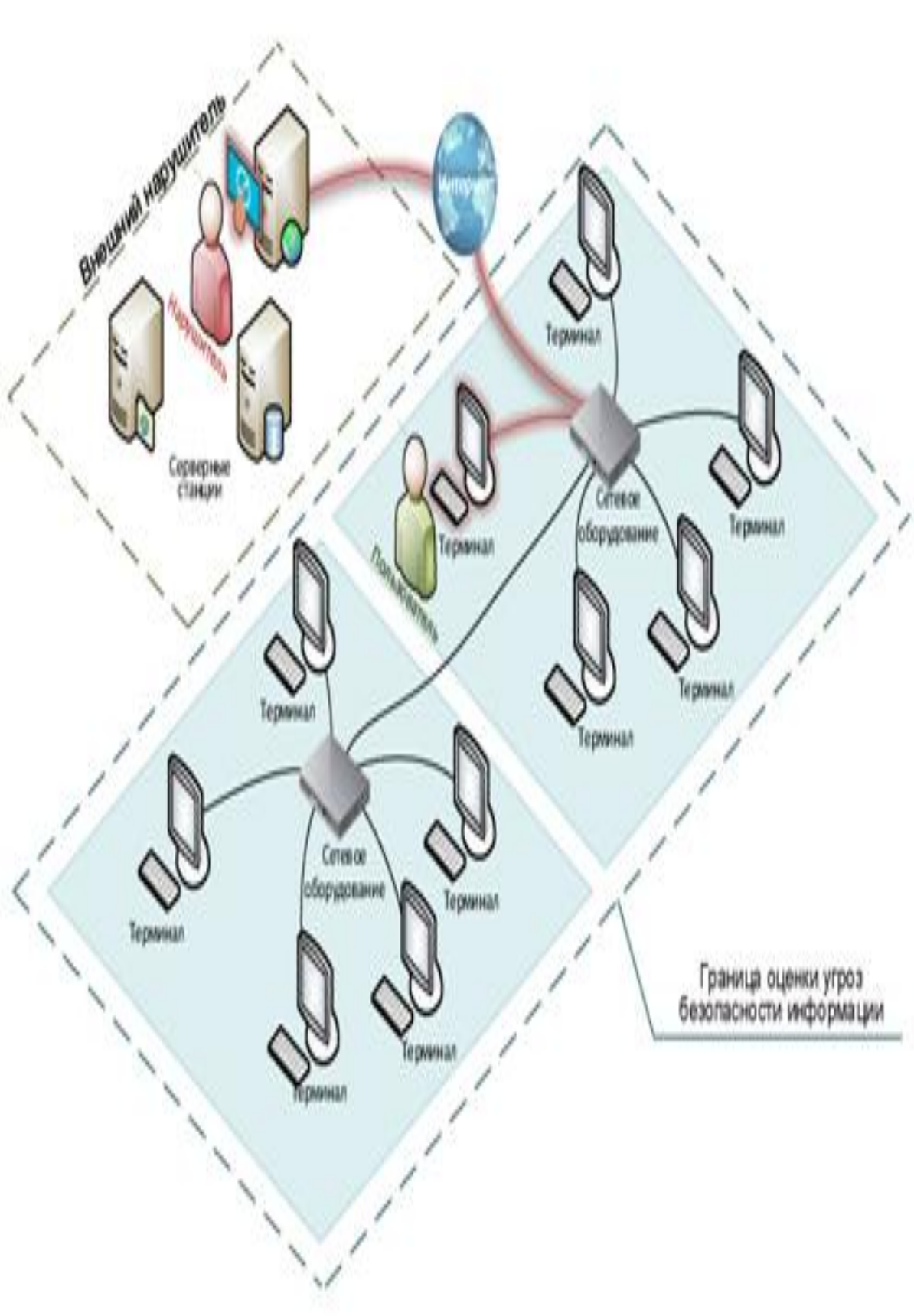

Рисунок 10 - Процесс проникновения в систему сторонних

В зависимости от тех условий доступа, какие имеют внутренние нарушители, процесс авторизации для входа в систему и проникновения в систему,

к которой у них есть доступ для получения информацию с целью нанесения ущерба программному обеспечению, может быть наименее или наиболее сложным. Он зависит от того, какую должность и роль они занимают и насколько широк их уровень доступа, как часто они пользуются этой системой.

Проникновение в систему сторонних нарушителей зависит от уровня профессионализма и тех корыстных целях, которые они планируют при нарушении безопасности.

Рассмотрим угрозы безопасности, которые возникают без каких-то случайных сценариев. Такие угрозы приводят к нарушению функционирования систем и баз данных, когда случайным образом вносятся данные, превышающие лимит объема, или к сбою работы сайтов при загрузке сотрудниками ошибочной конфигурации файла.

Необходимостью в стабильной работе обосновывается требование к системам, которое заключается в устойчивости и надежности функционирования в различных условиях, таких как внешние факторы воздействия и условия эксплуатации.

Нужно предусмотреть все случаи чрезвычайных ситуаций, в которых должна обеспечиться безопасность информации и функционирование системы с исключением создания угроз.

Чрезвычайные ситуации, в которых должна обеспечиться безопасность информации, могут быть вызваны следующими факторами:

- некачественное или нелицензионное программное обеспечение, которое не обеспечивает надежное хранение баз данных и их передачу;
- обслуживание системы проводятся не качественно;
- высокое ценообразование лицензионных программ и комплектующих при работе с внешними поставщиками услуг.

Регулярность воздействий внешних угрожающих факторов можно установить на данных наблюдений за прошедшие периоды. Если данные наблюдений за прошедшие периоды о воздействии внешних угрожающих факторов отсутствуют, то их можно получить при экспертном оценивании.

Своевременное обнаружение случаев чрезвычайных ситуаций, в которых должна обеспечиться безопасность информации и функционирование системы с исключением создания угроз, необходимо проводить при строгом соблюдении норм и требований федерального законодательства.

После проведения процедуры оценки источников угроз безопасности информации необходимо выявить, какие виды нарушителей могут совершить действия по преодолению средств защиты, и с какой целью они проводят эти преступления, а также исключить возможность для создания условий для совершения непреднамеренных угроз безопасности.

Для своевременного обнаружения ситуаций, в которых должна обеспечиться безопасность информации и функционирование системы с исключением создания угроз необходимо анализировать предполагаемые мотивы сторонних и внутренних нарушителей, которые заинтересованы в нарушении безопасности конкретной системы.

Ответственный подход при работе с сотрудниками организации, которые не поддаются провокациям и не вступают в сговор со сторонними нарушителями, исключает возможные сценарии для совершения непреднамеренных угроз безопасности, и представители служб разведки недружественных государств, радикально - ориентированные группы, нарушители законодательства, хакеры и конкуренты не смогут с помощью внутренних специалистов совершить противоправные действия и разрушить безопасность.

5. Оценка способов осуществления угроз безопасности информации

Оценка действий осуществления опасных действий для информационных систем проводится для исключения рисков возможных сценариев при совершении преднамеренных угроз безопасности объектами, которые реально могут ее разрушить.

Сценарии для осуществления опасных действий для информационных систем, которые реально могут разрушить безопасность, могут быть следующими:

- произошла утечка персональных данных в полном или частичном объеме и нарушении конфиденциальности;
- получен доступ к персональным данным и защищенным данным;
- отказано в доступе к компонентам программы;
- изменилась целостность, похитили служебные данные;
- наблюдается нестабильность или не свойственное проведение операций для компонентов;
- нарушились способы передачи и функциональности.

Перечень возможных путей для осуществления опасных действий для информационных систем, которые реально могут разрушить безопасность, может быть расширен.

Оценка действий осуществления опасных действий для сетей также проводится с целью исключения рисков возможных сценариев при совершении преднамеренных угроз безопасности объектами, которые реально могут ее разрушить.

Сценарии для осуществления опасных действий для сетей, которые реально могут разрушить безопасность, могут быть следующими:

- поиск уязвимостей программного обеспечения, которые можно использовать для нанесения сетям повреждений;
- использование программного обеспечения, которое преднамеренно наносит вред;
- использование нелицензионного программного обеспечения или некачественных технических средств;
- встраивание в систему программы или изменение фрагмента программы путем скрытого внедрения;
- распространение конфиденциальной информации в случаях осуществления атак по скрытым каналам;

- перехват средством измерений побочных электромагнитных излучений, наводок различных средств вычислительной техники, используемой для распространения конфиденциальной информации;
- преодоление всех уровней защиты различных средств вычислительной техники, используемой для распространения конфиденциальной информации;
- преднамеренные технические нарушения при проведении настройки всех уровней защиты различных средств вычислительной техники, используемой для распространения конфиденциальной информации;
- не преднамеренные технические нарушения при проведении настройки всех уровней защиты различных средств вычислительной техники, используемой для распространения конфиденциальной информации.

Перечень возможных путей для осуществления опасных действий для сетей, которые реально могут разрушить безопасность, может быть расширен.

Оценка способов осуществления угроз безопасности информации перечислена в Методике. Оценка способов осуществления угроз безопасности информации проводится на основании этих соответствий.

Оценка способов осуществления угроз безопасности информации является актуальной и проводится для исключения рисков возможных сценариев при совершении преднамеренных комплексных угроз безопасности объектами, которые реально могут ее разрушить.

Нарушители могут использовать следующие способы осуществления угроз безопасности информации при получении доступа интерфейсам:

- внешние сетевые, которые осуществляют передачу данных между программами через интернет;
- внутренние сетевые, которые обеспечивают взаимодействие между компонентами программам и сети через интернет с внешними интерфейсами;
- пользовательские, которые служат для удовлетворения запросов пользователей;

− бесконтактные, которые обеспечивают взаимодействие между бесконтактными носителями и компонентами программам;

− функциональные, которые обеспечивают управление и администрирование над компонентами программам при нахождении техники на ремонте или техническом обслуживании.

Перечень элементов, которые осуществляют передачу данных между программами через интернет, обеспечивают взаимодействие между компонентами программам и сети через интернет с внешними интерфейсами, между бесконтактными носителями и компонентами программам, управление и администрирование над компонентами программам при нахождении техники на ремонте или техническом обслуживании являются объектами, на которые нарушители для создания угроз могут оказывать воздействие.

Угрозы безопасности могут оказывать воздействие на интерфейсы всех систем технического оборудования. Использование интерфейсов нарушителями зависит от уровня профессионализма и тех корыстных целях, которые они планируют при нарушении безопасности.

На этапе определения интерфейсов, которые осуществляют передачу данных между программами через интернет, обеспечивают взаимодействие между компонентами программам и сети через интернет с внешними интерфейсами, между бесконтактными носителями и компонентами программам, управление и администрирование над компонентами программам при нахождении техники на ремонте или техническом обслуживании, необходимо оценить предполагаемые элементы, на которые нарушители для создания угроз могут оказывать воздействие.

Данные работы рекомендуется проводить в автоматическом режиме.

После проведения оценки способов осуществления угроз безопасности информации необходимо определить:

−направленность групп нарушителей, применяющих возможность осуществления угроз безопасности информации;

−перечень возможных путей для осуществления опасных действий для сетей, которые реально могут разрушить безопасность.

6. Определение последствий от создания угроз

Определение последствий от создания угроз проводится для исключения рисков возможных сценариев при совершении преднамеренных угроз, которые реально могут ее разрушить.

Модели угроз безопасности и возможности причинения ущерба нарушителей могут быть различными к тому или иному информационному пространству. С помощью Методики можно оценить уровень возможностей при реализации угроз безопасности.

Реализованные в соответствии с Методикой мероприятия способствуют спрогнозировать последствия, возникающие при наступлении момента нарушения безопасности информационной среды колледжа, выяснить, какие объекты могут быть наиболее уязвимые и провести обследование операционных систем колледжа, оценить потенциальных нарушителей, которые заинтересованы и мотивированы в создании угроз колледжу и провести «тренировку» решения проблем, возникших при возникновении условных угроз.

Оценка возможных сценариев осуществления угроз перечислена в Методике. Оценка способов осуществления угроз безопасности информации проводится на основании этих соответствий.

Для предотвращения совершения процессов, которые перечислены в Методике, необходимо разработать дорожную карту по мониторингу угроз. В план мероприятий необходимо включить:

- блокировку утечки персональных данных в полном или частичном объеме и нарушения конфиденциальности;
- запрет на доступ к персональным данным и защищенным данным;
- организацию прерывания доступности к компонентам программы;
- мониторинг изменения целостности, проникновения в служебные данные;

- отслеживание нестабильного или не свойственного проведение операций для компонентов;
- блокировка нарушения способов передачи и функциональности.

Дорожная карта по мониторингу угроз данной Методики служит для предотвращения совершения процессов реализации угроз.

Объекты, которые заинтересованы в нанесении ущерба информационным системам колледжа, тщательно прорабатывают методы и возможные способы реализации по созданию угроз.

Негативное воздействие на информационные системы колледжа создают реальные угрозы и приносят ущерб. Для того чтобы обеспечить надежную защиту от вышеперечисленных источников угроз необходимо строго следовать Методике, применять современные средства защиты и организовывать мероприятия на системной основе (рисунок 11).

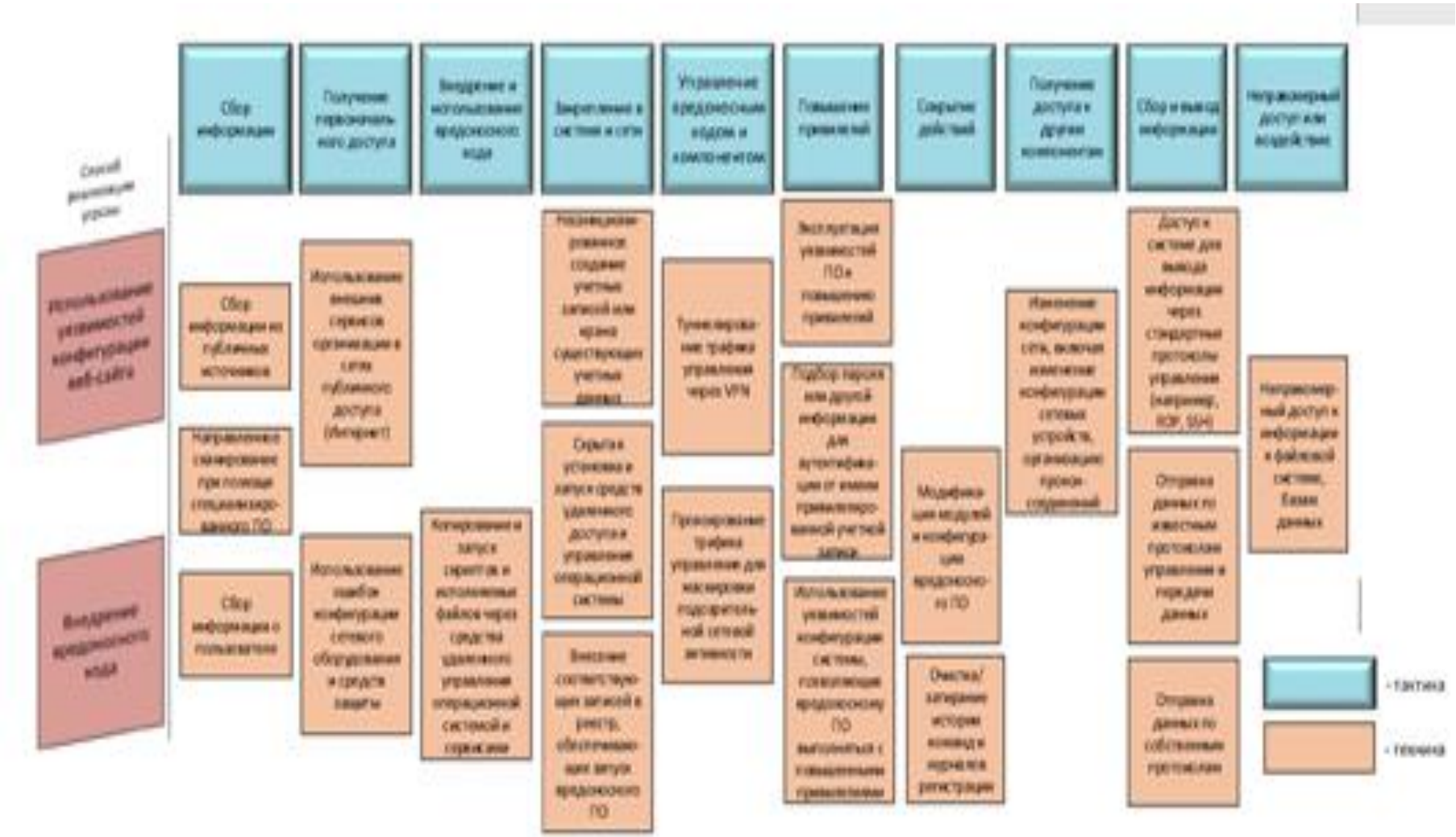

Рисунок 11- Негативное воздействие на информационные системы колледжа.

Оценка действий осуществления опасных действий для сетей также проводится с целью принятия эффективных технических решений и средств защиты при совершении преднамеренных угроз безопасности объектами, которые реально могут ее разрушить.

При изучении работы системы в тестовом режиме необходимо провести прогнозирование вероятных угроз, для этого проводится:

- контроль внешних сетевых интерфейсов, которые осуществляют передачу данных между программами через интернет;
- контроль внутренних сетевых интерфейсов, которые обеспечивают взаимодействие между компонентами программам и сети через интернет с внешними интерфейсами;
- анализ запросов пользователей;
- контроль бесконтактных интерфейсов, которые обеспечивают взаимодействие между бесконтактными носителями и компонентами программам;
- обеспечение управления и администрирования над компонентами программам при нахождении техники на ремонте или техническом обслуживании.

Возможный сценарий при совершении преднамеренных угроз показан на рисунке 12.

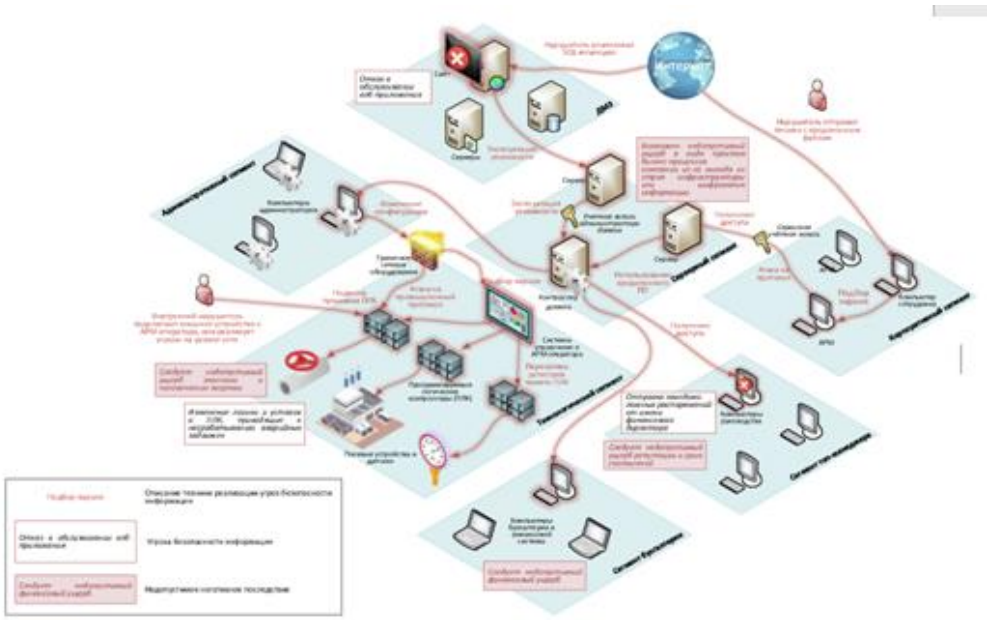

Рисунок 12- Сценарий при совершении преднамеренных угроз

Архитектура систем и сетей: совокупность основных структурно-функциональных характеристик, свойств, компонентов систем и сетей, содержащие основные правила взаимодействия, способы обработки информации.

Взаимодействующая система: сеть, которая функционально осуществляет взаимодействия сетевых интерфейсов с системой и сетью оператора и не погружена в состав процесса оценки угроз безопасности информации.

Компетентность нарушителя: ресурсные и мотивационные возможности нарушителя для реализации угрозы безопасности информации.

Граница оценки угроз: совокупность ресурсов и компонентов систем и сетей, в рамках которой организуется защита информации (безопасность) с учетом процедурам контроля и проводится мониторинг за проводимыми мероприятиями по обеспечению защиты информации (обеспечения безопасности).

Выводы по главе 2

Конкретные механизмы решения и показатели реализации в сере образования на различных уровнях представлены не пропорционально. Также проведение цифровизации образования при реализации федеральных проектах рассчитано провести в условиях традиционной организации и не в условиях трансформации и модернизации.

Существующая реальность требует современных и модернизированных, действующих на опережающее развитие способов цифровизации и информатизации всех уровней образования на равной основе. Выявленные проблемы необходимо решать путем уточнения целевых показателей и подойти системно к выполнению мероприятий. Негативное воздействие на информационные системы колледжа создают реальные угрозы и приносят ущерб. Для того, чтобы обеспечить надежную защиту от вышеперечисленных источников угроз необходимо строго следовать Методике, учитывать возможности современных средств защиты и организовывать мероприятия на системной основе.

Данные результаты анализа защиты информации при использовании виртуальных сред в ГБПОУ «Миасский машиностроительный колледж» позволяют перейти к разработке рекомендаций по совершенствованию защиты информации при использовании виртуальных сред.

ГЛАВА 3. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО СОВЕРШЕНСТВОВАНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ВИРТУАЛЬНЫХ СРЕД В ГБПОУ «МИМК»

3.1. Разработка и апробация рекомендаций по совершенствованию защиты информации при использовании виртуальных сред в колледже

Выбор оптимальных методов защиты облачных ресурсов, сравнения облачных технологий. К выбору поставщиков различного программного обеспечения при предоставлении услуг удаленных, который соответствует предъявляемым требованиям заказчиков, нужно подходить ответственно и интересоваться репутацией поставщиков услуг.

Существует огромный выбор между облачными технологиями, они могут быть бесплатными, а могут быть и на коммерческих основах.

Потребности, предъявляемые к облачным технологиям, определяют подходы к выбору данной инфраструктуры.

Подобранные облачные технологии предполагают учреждениям выбрать модель обслуживания, наиболее удовлетворяющие их запросы: модели IaaS, PaaS и SaaS.

Наиболее подходящий моделью для профессиональных образовательных организаций можно считать IaaS модель в том случае, если существует потребность в вычислительных мощностях и дополнительный сервис не представляется возможным приобрести.

Популярные иностранные провайдеры IBM Smart Cloud Enterprise, VMWare, Amazon EC2, Windows Azure, Google Cloud Storage, которые предоставляют такие услуги, расположены в недружественных странах и их использование не рекомендовано.

В Челябинской области популярностью пользуются провайдеры Теле2, Ростелеком, Дом.ру, МТС.

Благодаря высокой доступности при предоставлении услуг клиентам в любой момент времени, поддержке систем и реализации сопряжения собственной виртуальной инфраструктуры и функциональности SRM лидирующие позиции удерживает VMware.

Проведенные сравнения провайдеров, которые подходят под вышеуказанные условия, рассмотрим в таблице 6

Таблица 6 - Характеристика российских провайдеров

№	Провайдер IaaS	Системы хранения	Стоимость HDDпри статической модели,	Стоимость HDDпри динами-
1	IT-GRAD	NetApp FAS 6240	30	44
2	Dataline	NetApp FAS 6210, HP MSA P2000	20	40
3	Cloudone	NetApp FAS 2040, NetApp FAS 3240	14	нет
4	ONLANTA	HDS HUS	32	нет
5	SafeData	NetApp FAS 3250	24	30
6	Cloud4Y	NetApp FAS 3250	38	нет
7	Croc	EMC VNX 5700	26	40
8	I-Teco	3PAR 10400, IBM Storewize 7000, IBM	30	нет
9	MegaFon	HP EVA 8400	28	нет
10	RTComm-	EMC VNX	30	нет
11	SoftLine	NetApp FAS 2240	30	44
12	DEPO	NetApp E- series	26	нет

У каждой представленной в таблице компании есть свои выгодные позиции, которые учитывают индивидуальный подход и могут удовлетворить конкретного потребителя с определенными потребностями.

Разработчики современного программного обеспечения используют колоссальные ресурсы для вычислительных операций, их участие в администрировании баз данных и операционных систем ограничен. Использование модели PaaS находит свое применение в таких ситуациях.

Чтобы профессиональная образовательная организация в полной мере могла реализовать свои потребности, необходимо учитывать реализацию:

- поддержка протоколов SSL (HTTPS);

- типы разрешения приложений;
- типы баз данных.

В таблице 7 рассмотрим отличия между PaaS платформами

Таблица 7- Сравнение языков программирования и баз данных PaaS платформ

Платформа	Поддерживаемые языки програмирования	Поддерживаемые базы данных	Стоимость, $
Beanstalk	Java, .NET, PHP, Node.js, Python, Ruby, Go иDocker	Amazon Relational Database Service (Amazon RDS), Amazon DynamoDB илиMicrosoft SQL	от 0.05 до 4.10 за час
Force.com	HTML, CSS, and JavaScript	Oracle Database	75 за пользователя в месяц
Heroku	Ruby, Java, Node.js, Scala, Clojure, Python, Go иPHP	Cloudant(англ.), Membase(англ.), MongoDB иRedis, помимоосновной— PostgreSQL	от 0.05 до $0.10 за час
Microsoft Azure	Java, PHP, Ruby, Node.js, C	SQL Server	от 0.02 до 0.64 за час
OpenShift	.NET Core 1.0 .NET Core 1.1 Node.js 0.10 Node.js 4 PHP 5.5 PHP 5.6 Python 2.7 Python 3.3 Python 3.4 Python 3.5 Ruby 2.0 Ruby 2.2 Ruby 2.3 Perl 5.16 Perl 5.20 Tomcat 7 Tomcat 8	MariaDB 10.1 MongoDB 2.4 MongoDB 2.6 MongoDB 3.2 MySQL 5.5 MySQL 5.6 PostgreSQL 9.2 PostgreSQL 9.4 PostgreSQL 9.5	от 0.02 до 0.10 за час
App Engine	Python, Java, Go, PHP	-	от 0.05 за час
Engine Yard	Ruby, JRuby, REE, Rubiniu, Node.js, PHP	MySQL и PostgreSQL	от 0.05 до 2.19 за час

Модель SaaS реализует режим работы удаленного доступа для своих пользователей, которые принимают решение работать с определенным приложением в связи с отсутствием возможности установки данных приложений на их технических средствах.

Модели SaaS представлены в:

- Gmail,

- Netflix,
- Photoshop.
- Acrobat.

Глобальный захват ранка потребителей мобильных приложений также использует модель SaaS.

Вышеперечисленные приложения с моделью SaaS предоставляют широкий выбор различного функционала при фактически одинаковых возможностях облачных хранилищ, который пользователь выбирает, основываясь на запросах, объемах хранилищ и ценовой политики поставщиков услуг.

Поставщики услуг, предоставляющие широкий выбор различного функционала при фактически одинаковых возможностях облачных хранилищ, имеют низкую мотивацию к организации безопасного хранения конфиденциальной информации, поэтому нарушители чаще всего создают угрозы безопасности в модель SaaS.

Обеспечение ответственного хранения и передачи конфиденциальной информации пользователей производится путем безопасной установки соединений с облачными хранилищами.

Поставщики услуг, предоставляющие широкий выбор различного функционала при фактически одинаковых возможностях облачных хранилищ, не учитывают возникновения угроз сетям и маршрутизаторам и не включают в стандартные опции дополнительные инструменты по защите от атак.

Так как дополнительные услуги по защите от атак затрагивают дополнительные финансовые затраты, то не все категории потребителей имеют возможность заблокировать и устранить вероятные угрозы нарушителей. Внешние облака серверов наиболее подвержены данной угрозе.

Потребители имеют возможность заблокировать и устранить вероятные угрозы нарушителей путем установки межсетевого экрана, шифрования каналов передачи, а также обязательной авторизацией.

Шифрование каналов передачи и авторизация пользователей позволяет осуществлять контроль и порядок доступа, дает возможность своевременно

заблокировать и устранить вероятные угрозы нарушителей.

Чтобы хранение и передача конфиденциальной информации пользователей осуществлялась безопасно, необходимо привести в соответствие регламент работы облачных хранилищ с шифрованием каналов передачи и авторизацией пользователей. Подробное описание типов подключения перечислены в Приложении 1.

Выбор поставщиков услуг, предоставляющих дополнительные инструменты по защите от атак и возникновения угроз сетям и маршрутизаторам, делается персонально клиентами.

Предложенные дополнительные меры по защите от атак и возникновения угроз сетям могут помочь осуществить передачу данных на безопасном уровне, но гарантировать полную защиту при применении предложенных мер не представляется возможным. В этой ситуации возникает необходимость дополнительного шифрования данных.

Внешние нарушители создают угрозы сетям, поэтому необходимо выстраивать систему по отражению угроз, они также пытаются негативно воздействовать на сотрудников провайдера. Данная ситуация особенно важна, если пользователь хранит данные в мобильных приложениях.

Шифрование, которое применяется в облачных сервисах, должно соответствовать следующим условиям:

- пользователь имеет доступ по модели частного облака;
- облачный сервис обработки можно назвать наиболее удобным для пользователя;
- приложение общедоступно.

Рассмотрим достоинства одного из предлагаемых поставщиками сервиса ownCloud.

Веб-приложение ownCloud бесплатно корпоративным пользователям осуществляет синхронизацию данных и организует совместную работу с файлами под управлением Windows, OSX или Linux, устройствами мобильной

связи на IOS и Android, и предоставляет возможность редактирования текстовых файлов и других необходимым в повседневной жизни функциям (калькулятор, звукозапись, календарь, список контактов) [10].

В ГБПОУ «МиМК» установлен облачный сервис ОС UbuntuServer14.04 и проложено VPN соединение типа Remoteaccess (Рисунок 13).

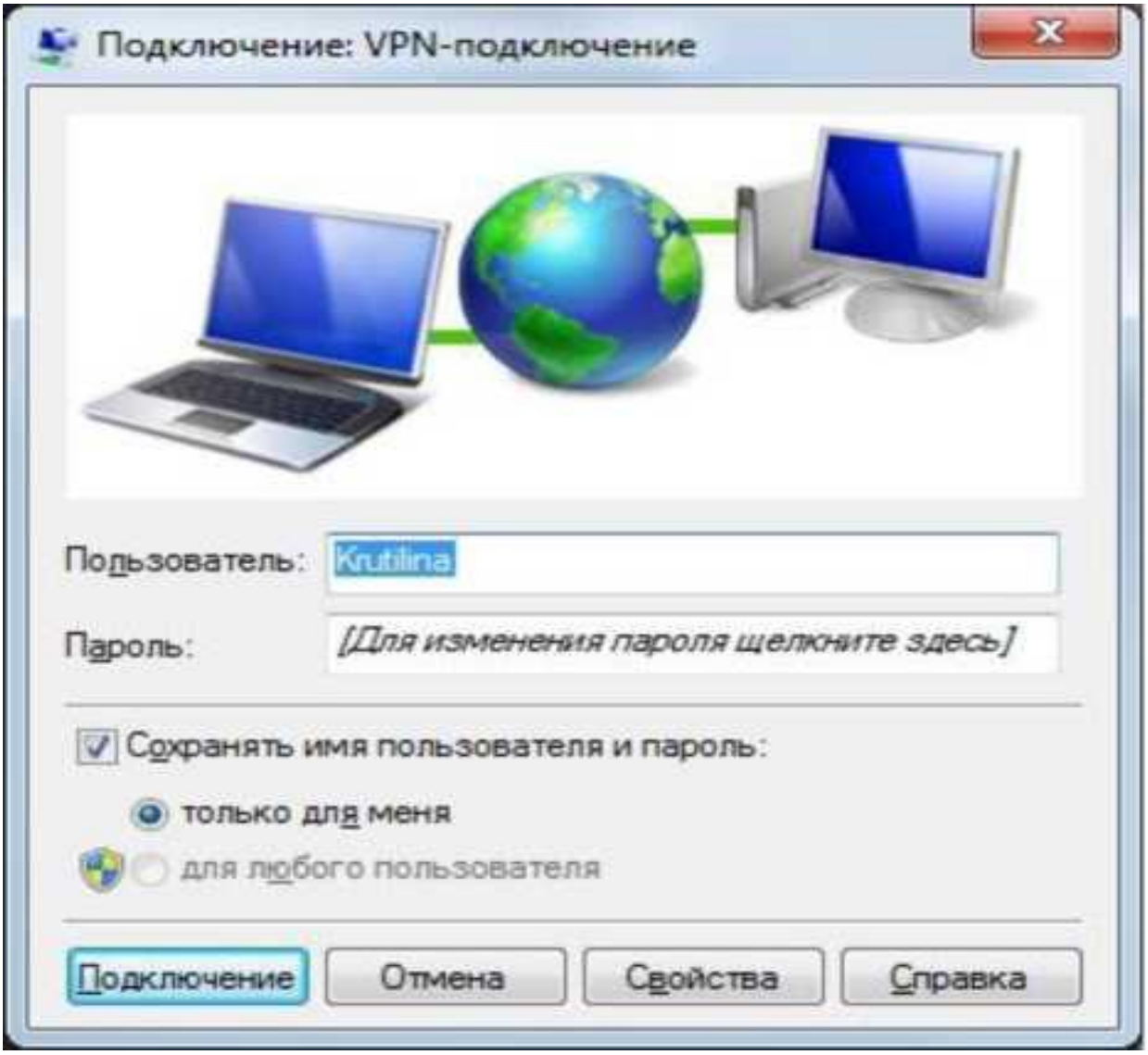

Рисунок 13 - VPN соединение в ГБПОУ «МиМК»

На рисунке 14 показано подключение сеанса PuTTY для организации удаленного доступа к серверу

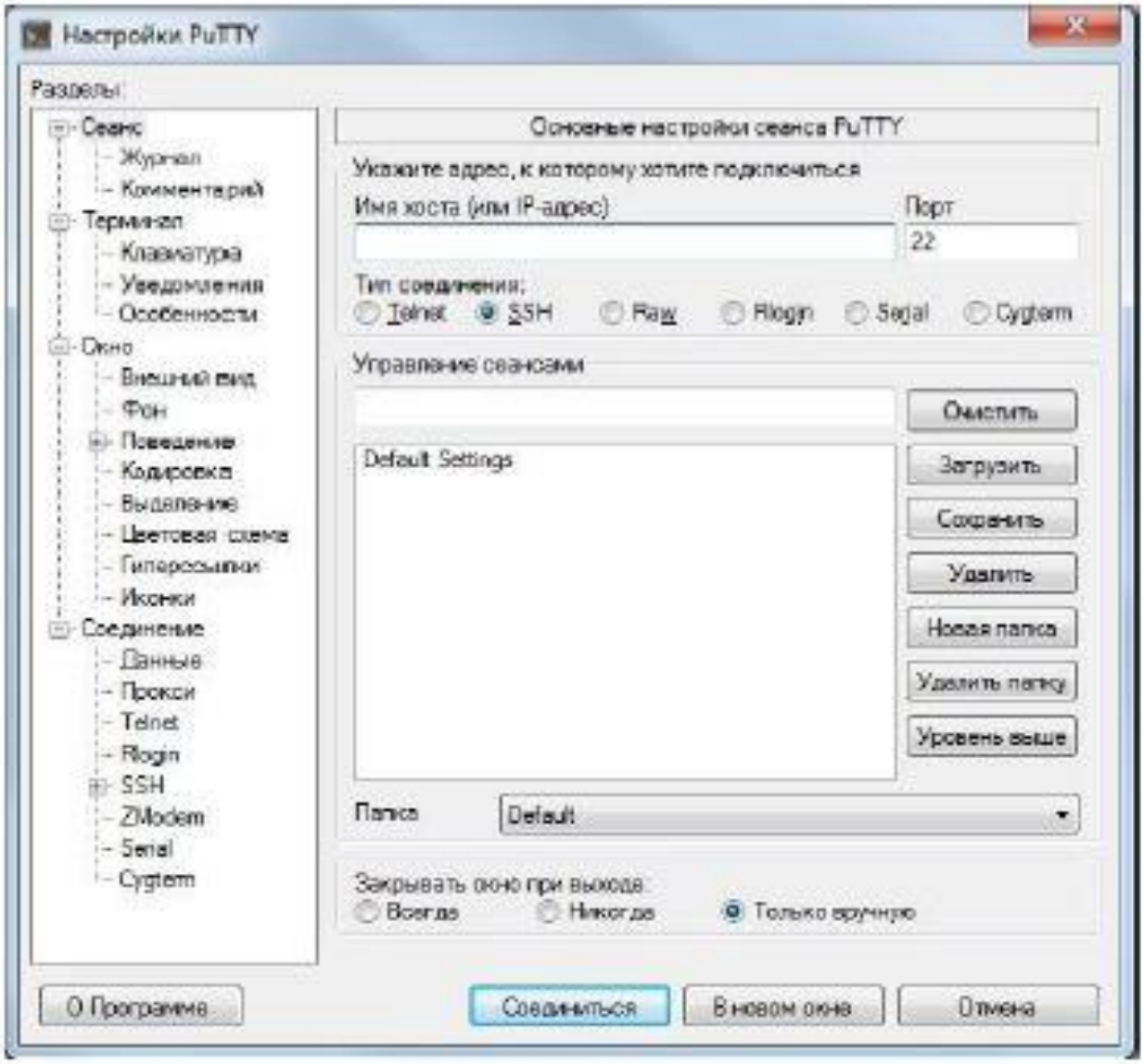

Рисунок 14 – Настройки подключения сеанса PuTTY

Управление удаленным сервером при использовании данного приложения дает возможность подключения и управления с помощью протоколов SSH, Telnet, rlogin (Рисунок 15)

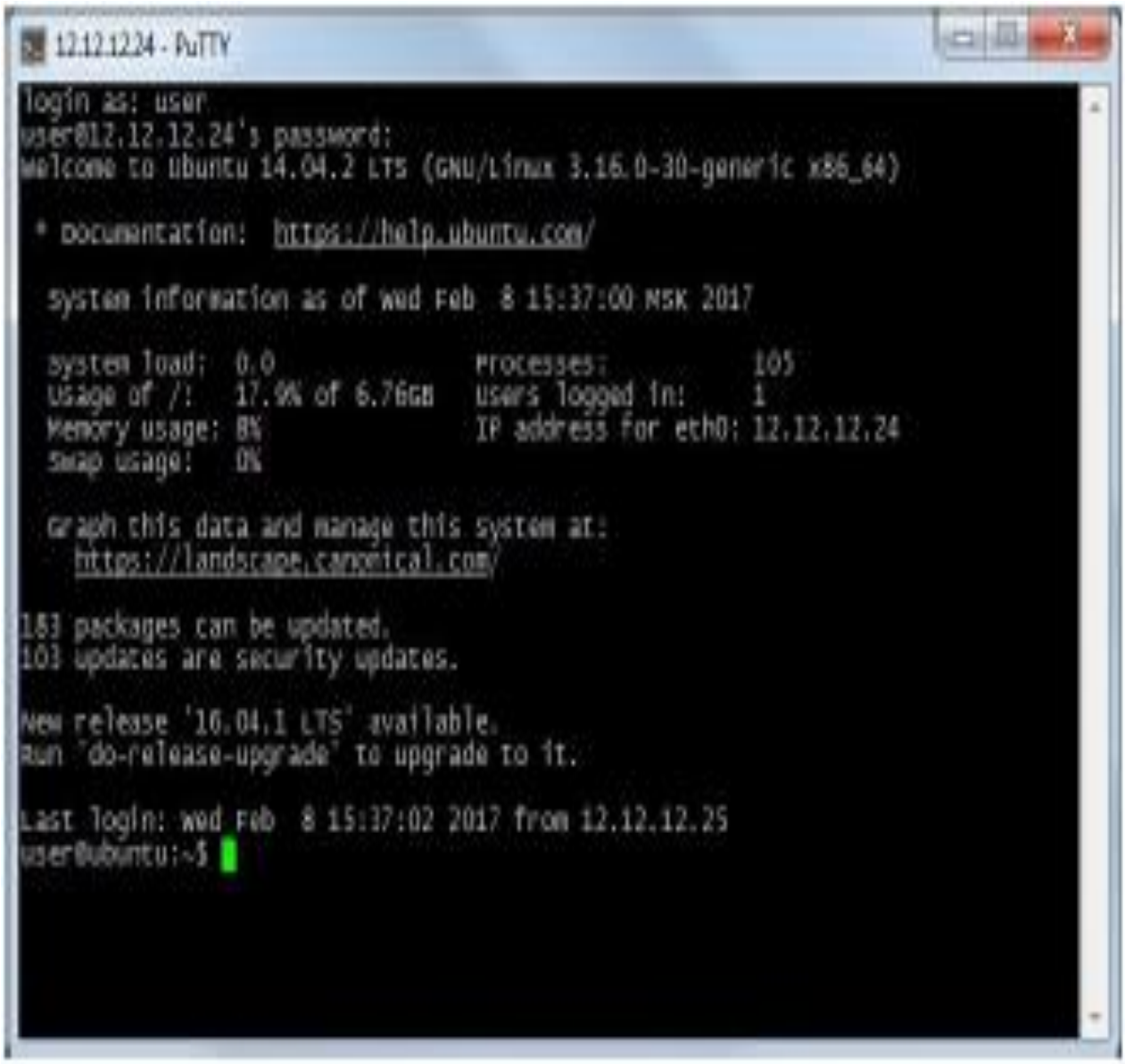

Рисунок 15 – Вид сервера

Установка реляционной базы, представленной в виде связанной информации и описываемой как набор связей была выполнена перед установкой ownCloud, после нее сервер был запущен.

Для осуществлении процесса загрузки файлов в облачное хранилище вводим адрес http://ip_адрес_пользователя/owncloud в строке браузера, вид облачного хранилища на сервере представлен на рисунке 16:

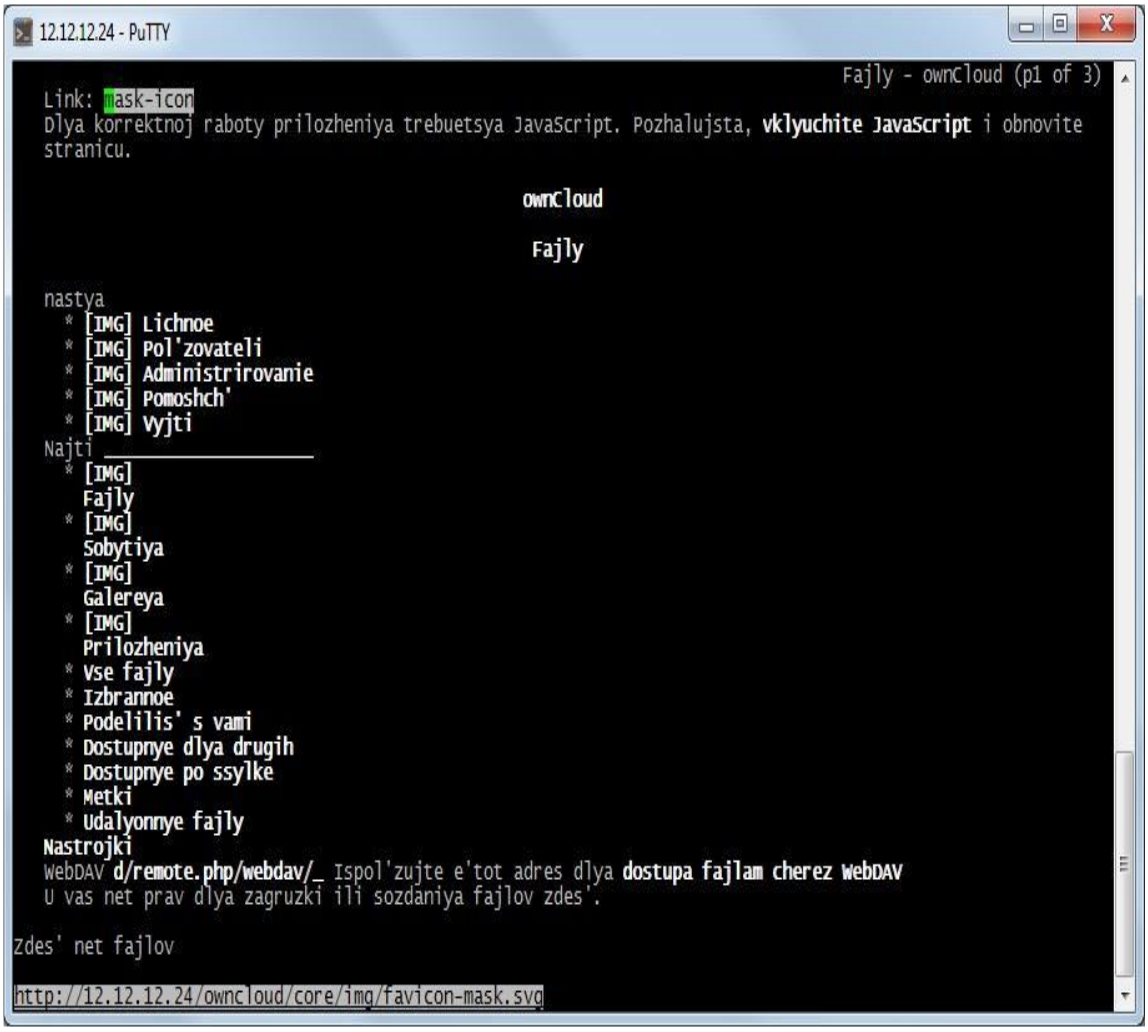

Рисунок 16 – Вид облачного хранилища на сервере

На рисунке 17 представлено окно браузера с видом на облачное хранилище:

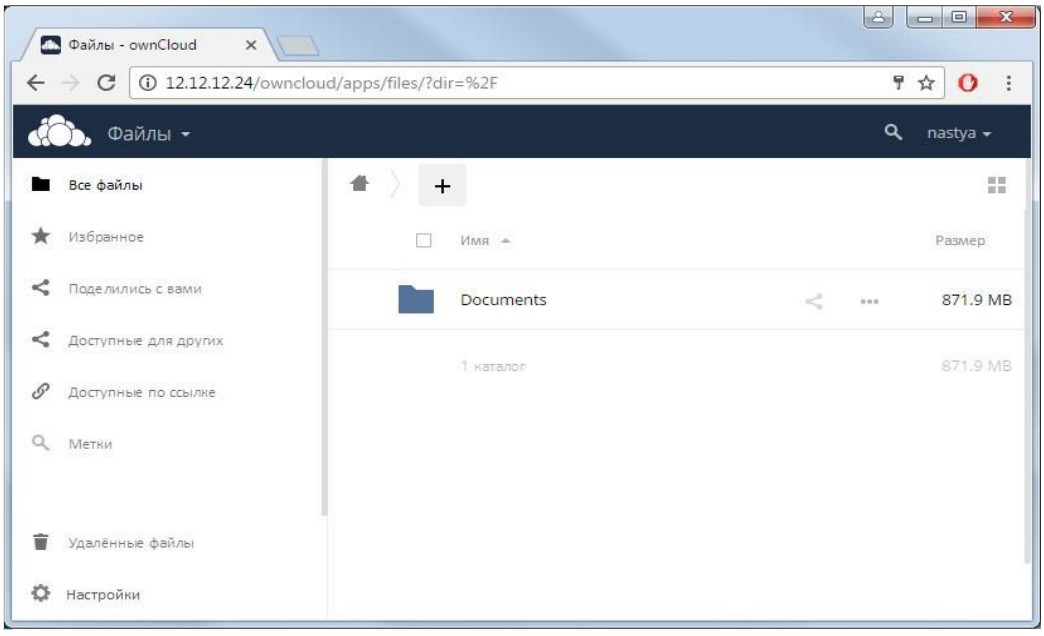

Рисунок 17 – Окно браузера с видом на облачное хранилище

Безопасность передачи и хранения файлов сейчас имеет очень большое значение для любого пользователя сети Интернет. Именно поэтому важно обеспечивать дополнительную защиту данных. Одним из наиболее распространенных методов защиты является шифрование.

Для выбора метода шифрования применялись такие начальные критерии, как:

— Осуществляемо для Windows ОС;

— Облачный клиент не умеет синхронизировать файлы поблочно;

— Метод шифрования должен обеспечить возможность быстрого доступа к любому файлу на облаке для его обновления или дешифровки без необходимости передачи больших объемов паразитных данных.

Исходя из этих, условий было выделено несколько возможных методов шифрования:

1) Проприетарные программы, позиционируемые как средство для шифрования данных в облаке.

Особенность работы данных программ в том, что они шифруют отдельные файлы, представленные на диске, а потом с помощью библиотек Dokanили EldosCBFScоздают их виртуальное расшифрованное представление. При локальной работе файлы прозрачно расшифровываются, а при синхронизации папки пользователя с облачным хранилищем передаются в зашифрованном виде. Данные программы идеально подходят для пользователей, не имеющих опыта в шифровании данных.

Из существующих на данный момент программ была выбрана бесплатно распространяемая программа Box Cryptor (Рисунок 18). Box Cryptor является кросс-платформенной программой для персональных компьютеров и телефонов и поддерживает все наиболее популярные облачные хранилища данных. С ее помощью можно осуществить шифрование документов с помощью RSAи симметричного алгоритма блочного шифрования AESс длинной ключа 256 бит.

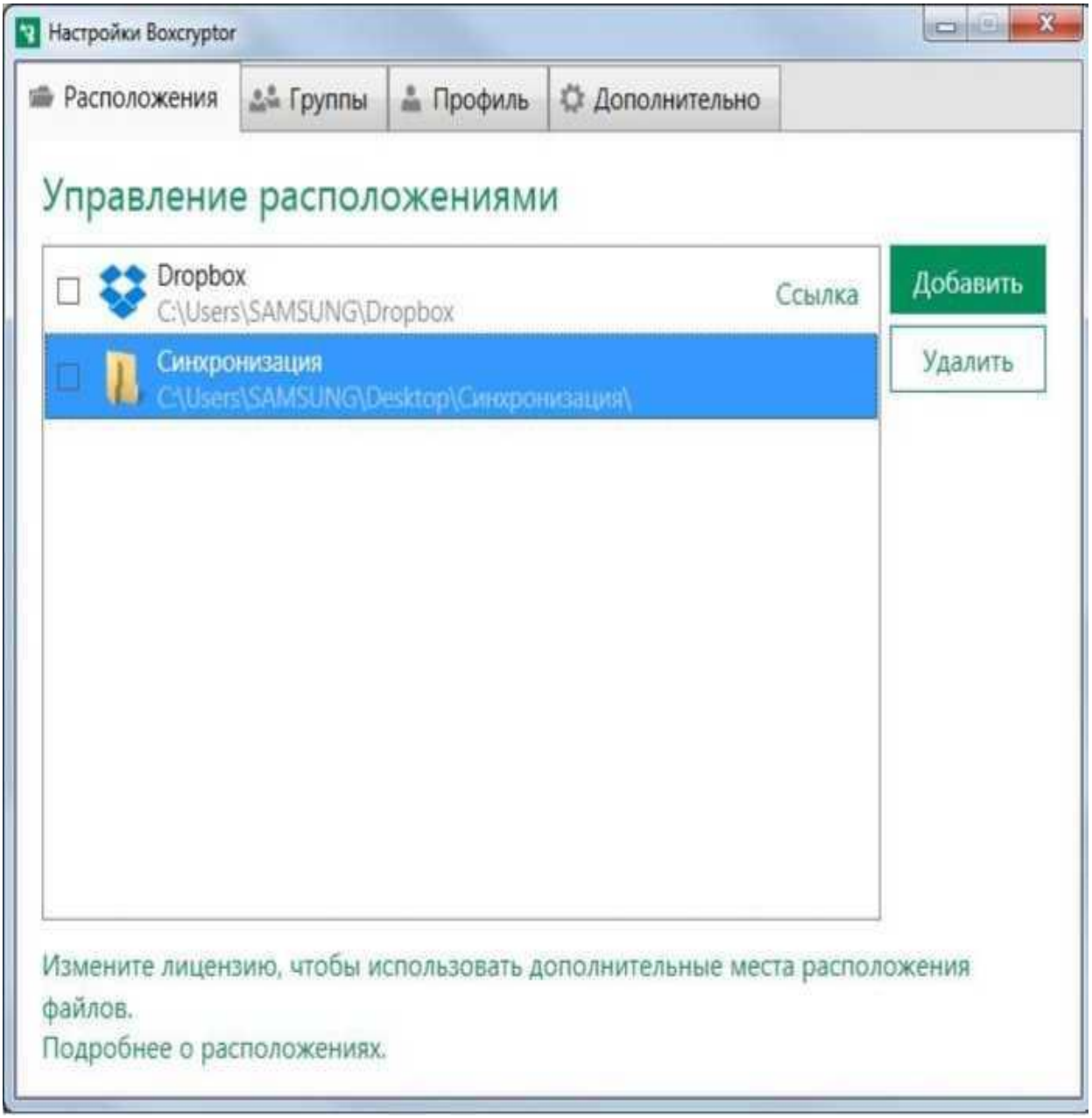

Рисунок 18 - Выбор синхронизированной папки для защиты Недостатки данного подхода:

— Ограниченное количество функций в бесплатной версии программы;

— При утере пароля доступ к зашифрованным файлам становится невозможен и необходимо обратиться к администратору;

— Зашифрованные файлы можно просматривать только через интерфейс программы;

— В бесплатной версии можно загружать только один файл за раз;

— Субъективное мнение: недостаточная производительность, особенно при редактировании видео.

2) Порт EncFCдля Windows

EncFL- это криптографическая файловая система, прозрачно шифрующая файлы, используя произвольную директорию в качестве места для хранения файлов. EncFSвзаимодействует непосредственно с libfuse(интерфейс FUSE), библиотекой логирования иOpenSSL(библиотека шифрования). Основная реализация системы поддерживается операционными системами Linux, MacOS X, FreeBSD, но в последнее время получили активное развитие несколько реализаций под Windows [20]EncFS имеет ряд преимуществ над другими системами шифрования разделов жёсткого диска, потому что каждый файл отдельно шифруется и сохраняется как обычный файл:

Занимаемое EncFSдисковое пространство может расти и уменьшается в зависимости от изменений количества и размера зашифрованных файлов;

— Некоторые директории в директории-точке монтирования могут физически находиться на различных устройствах;

— Средства резервного копирования могут обновлять только те файлы, которые изменились в исходной директории, а не всю директорию;

— Это свободная система, с открытым исходным кодом;

— encf4winподдерживает ключ -reverse (Рисунок 19). В reverse-режиме локальные данные остаются нетронутыми, а шифруется только их отображение на виртуальном диске. Для работы encfs4wintребуется установка библиотеки Dokan0.6.0 (программного интерфейса для Windows, позволяющего создавать виртуальную файловую систему).

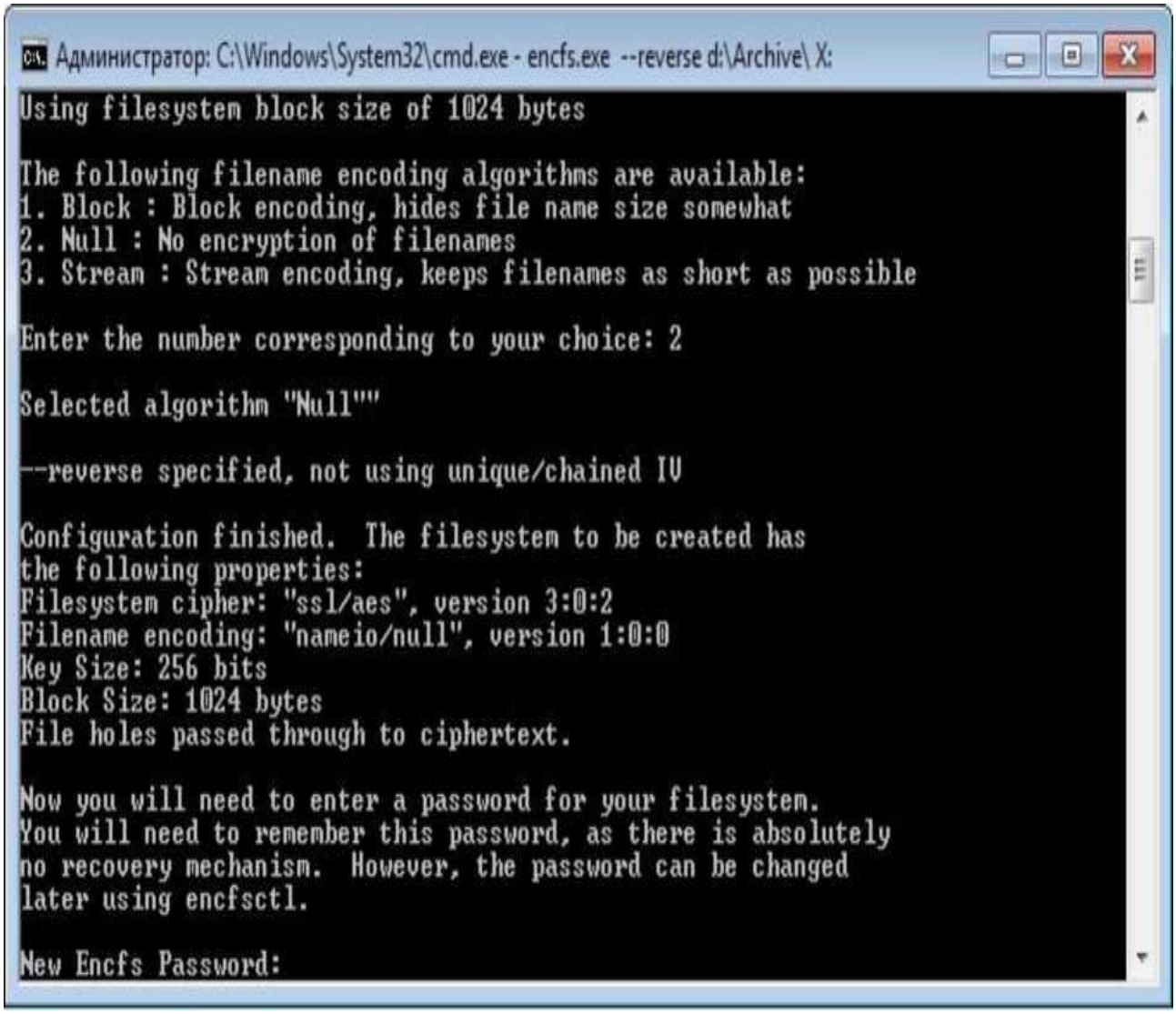

Рисунок 19 - Описание Reserveключа

Недостатки подхода:

— Тома EncFSne могут быть отформатированы под произвольную файловую систему. Они сохраняют особенности и ограничения файловой системы, содержащей директорию-источник;

— Фрагментация зашифрованного тома вызывает фрагментацию файловой системы, содержащей директорию-источник;

— Каждый пользователь, имеющий доступ к директории-источнику, способен видеть количество файлов в зашифрованной файловой системе, какие права они имеют, их приблизительный размер, приблизительную длину имени и дату последнего доступа или изменения.

3) Локальное шифрование файлов в архивы, защищенные паролем, и их последующая синхронизация с облаком. Утилита CryptSync.

CryptSync— это программа, которая синхронизирует две папки и шифрует одну из них, поэтому в распоряжении пользователя оказываются как непосредственно файлы, с которыми предстоит работать, так и их безопасная резервная копия. Открытая исходная программа шифрует папки с использованием формата 7-Zip, поэтому пользователь получает не только зашифрованные, но и уменьшенные в объеме данные (Рисунок 20). Данная программа не только индивидуально шифрует каждый файл, и его название.

С помощью CryptSyncтакже возможно шифрование и копирование файлов с компьютера на ноутбук или же с компьютера на внешний источник

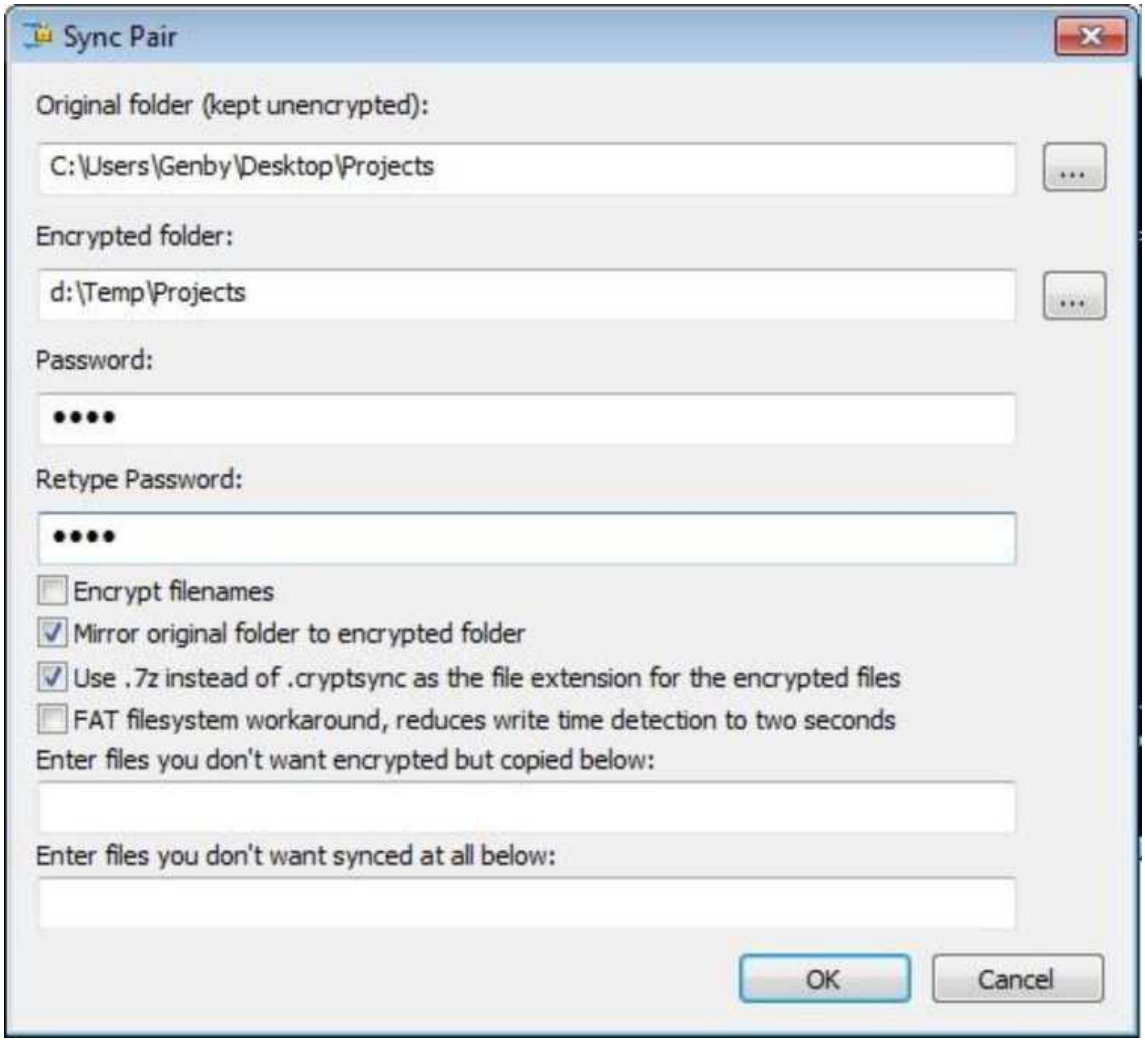

Рисунок 20 - Выбор шифруемой папки

Недостатки:

— Единственная поддерживаемая платформа — Windows;

— Необходимо хранить две копии файлов на локальном диске;

— Имеет недостаточный уровень защищенности, по сравнению с другими мерами.

Приведенные выше решения предоставляют только зашифрованное представление данных в локальной папке пользователя. Дальнейшая синхронизация может осуществляться любимым webdav-клиентом, либо официальным клиентом облака.

Представленные же ниже варианты имеют автоматическую интеграцию с облачными сервисами.

4) Duplicati— это программа с открытым исходном кодом, предназначенная для резервного копирования и созданная на основе одноименной утилиты с платформы Linux. Основной особенностью этой программы является возможность создания полноценного пошагового резервного копирования данных непосредственно в облако (Рисунок 10). Данной функцией поддерживаются такие облачные сервисы как, GoogleDrive, Skydrive, AmazonS3, Rackspace, Webdav, SFTP, FTP. На выбор предлагается шифрование встроенной библиотекой SharpAESCrypt(алгоритм шифрования AES-256) или средствами GnuPG(приложение для защиты сообщений и файлов, использующее шифрование и электронную цифровую подпись). Среди многочисленных функций Duplicatiособенный интерес также вызывает возможность быстрого восстановления отдельного файла из облака. Резервные копии при создании автоматически разбиваются на блоки размером 10 Мбайт. Поэтому при восстановлении одиночного файла будет задействовано ограниченное количество блоков. Помимо этого, данная программа полностью конфигурируема через командную строку и поддерживает портативный режим [21].

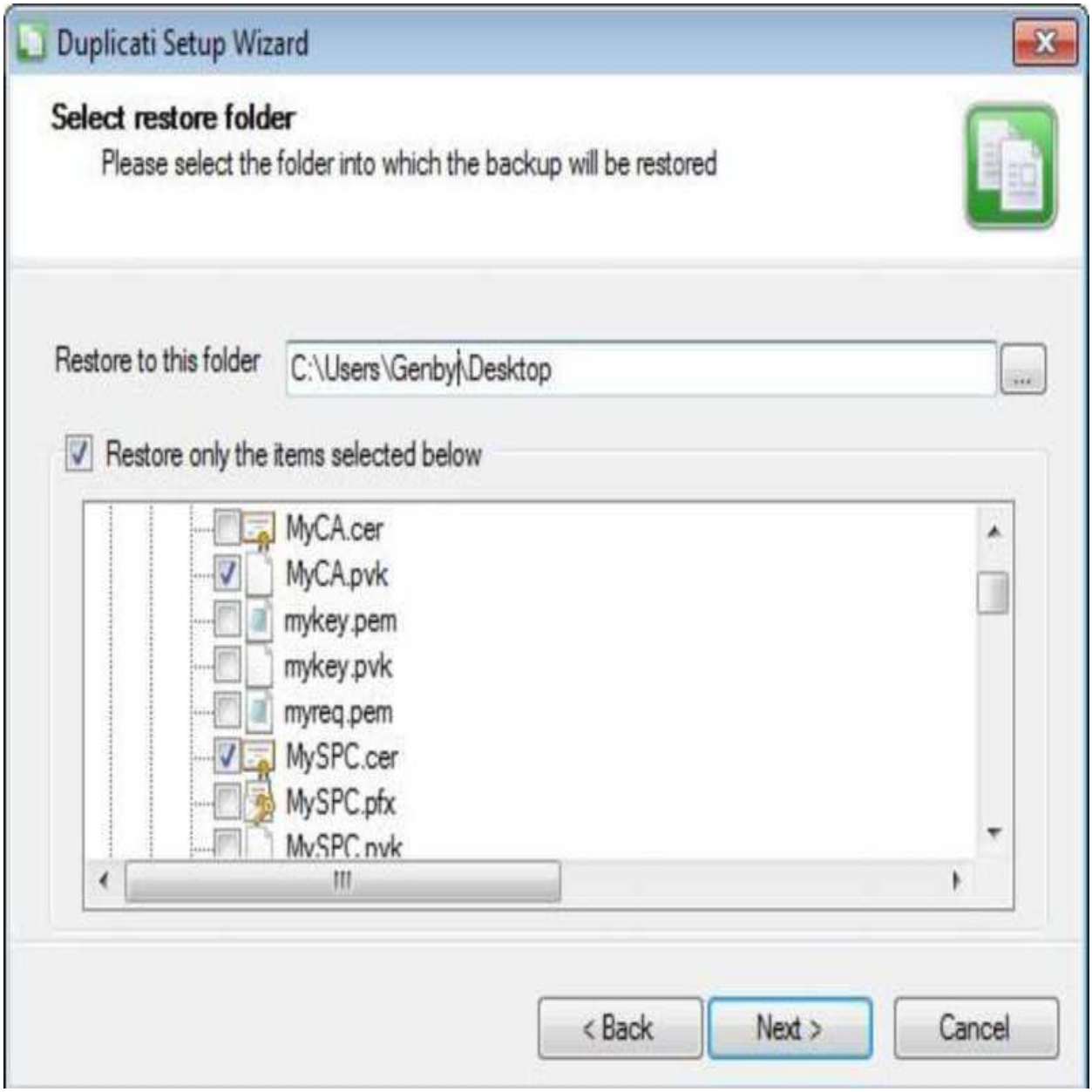

Рисунок 21 - Выбор папки для резервного копирования

Недостатки использования Duplicati:

— Невозможность обновления отдельного файла на облаке, кроме как путём создания новой инкрементальной итерации всего архива;

— Неудобно и долго восстанавливать одиночные файлы посредством использования графического интерфейса пользователя, особенно после нескольких инкрементальных итераций и при большом размере блока;

— Все данные о подключениях к облачным сервисам сохраняются в базе данных Sqllite, зашифрованной стандартным паролем.

5) Клиент CarotDav.

CarotDAV- это программа, которая помогает организовать удобный доступ, загрузку и управление файлами в нескольких облачных сервисах одновременно (Рисунок 11). Данный клиент не предоставляет всех функций, которые поддерживают фирменные клиенты облачных хранилищ данных, но может быть удобен в случае необходимости единовременного использования нескольких сервисов, например во время передачи файлов между ними. Кроме webdav-облаков CarotDAVосуществляется поддержка таких облачных платформ, как SkyDrive, Dropbox, GoogleDrive, Box, SugarSyncи FTP(S). Данная программа написана на объектно-ориентированном языке программирования VB.NETи является полностью свободной для использования и модификации. Из отличительных особенностей также можно выделить наличие портативного режима и защиту конфигурации мастер-паролем [22].

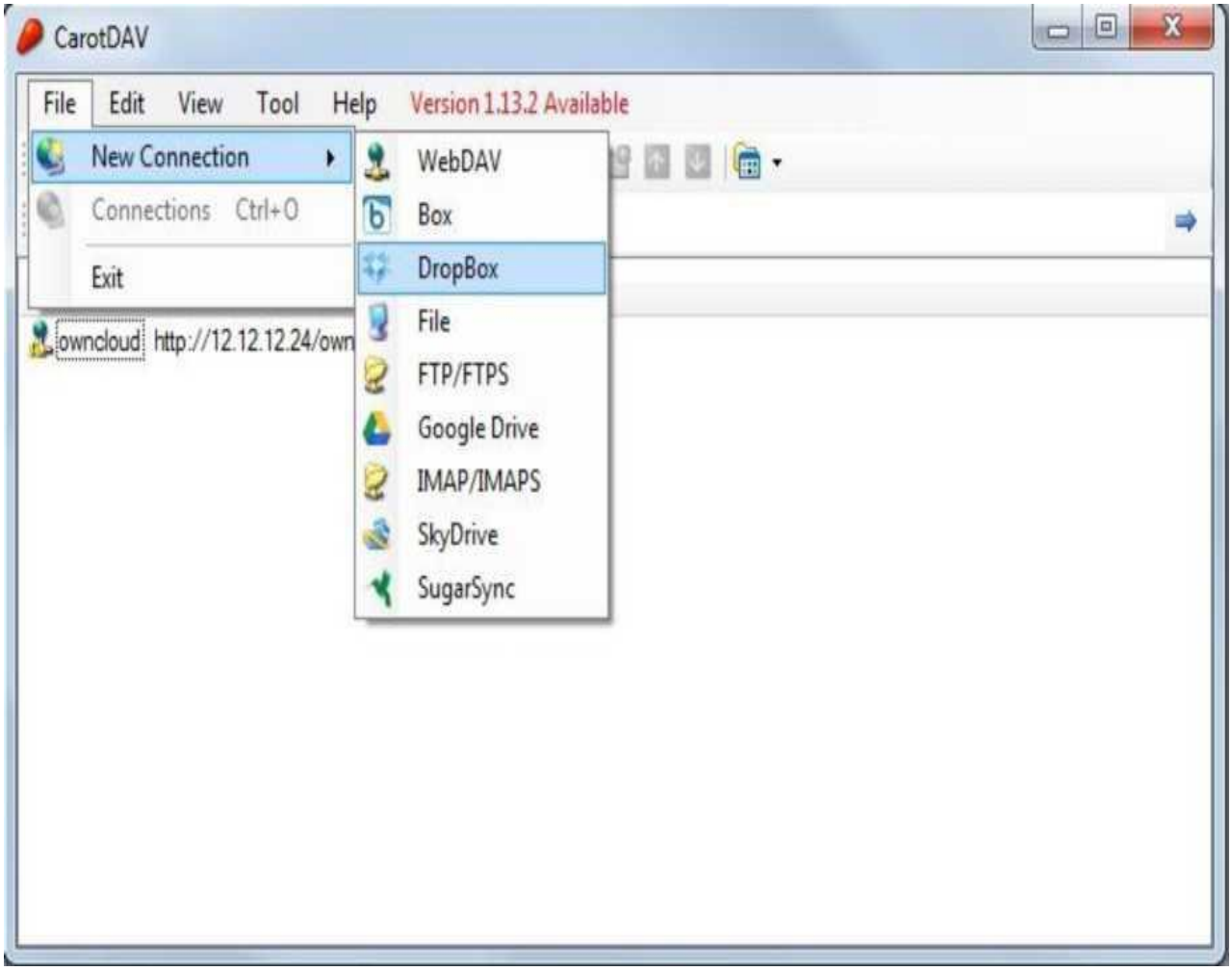

Рисунок 22 -Интерфейс программы CarotDAV

Недостатки:

— Возможны ошибки при работе с некоторым webdav облаками, которые можно решить увеличением времени ожидания соединения;

— Иногда возникают проблемы с поддержкой русского языка;

— Неудобный графический интерфейс пользователя и отсутствие управления через командную строку.

Учитывая вышеперечисленные факты, можно сформулировать методические рекомендаций по совершенствованию защиты информации при использовании виртуальных сред в ГБПОУ «МиМК»:

Меры по защите среды виртуализации. Основными направлениями безопасности виртуальной инфраструктуры являются:

- резервное копирование виртуальных машин;
- установление антивирусной защиты;
- мониторинг событий безопасности виртуальной инфраструктуры;
- разграничение доступа в виртуальной инфраструктуре;
- защита данных на виртуальных машинах;
- защита сети внутри виртуальной машины;
- обнаружение вторжений в виртуальную инфраструктуру;
- контроль уязвимостей в виртуальной инфраструктуре;
- аудит действий привилегированных пользователей.

Перечисленные меры по защите информации необходимы для нейтрализации актуальных угроз ИБ в виртуализированной инфраструктуре.

Для нейтрализации выявленных актуальных угроз безопасности персональных данных ВИ необходимо выполнение следующих мер:

- идентификация и аутентификация объектов доступа и объектов доступа в виртуальной инфраструктуре, включая администраторов средств управления виртуализацией;
- контроль доступа субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;
- запись событий безопасности в виртуальном туре;
- управление (фильтрация, маршрутизация, управление соединениями,

односторонняя передача) информационными потоками между компонентами виртуальной инфраструктуры и периметром виртуальной инфраструктуры;

- утвержденная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией;

- управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;

- контроль целостности виртуальной инфраструктуры и ее надежности;

- резервное копирование данных, аппаратное резервное копирование, программное обеспечение виртуальной инфраструктуры и каналы связи в виртуальной инфраструктуре;

- развертывание и управление антивирусной защитой в виртуальной инфраструктуре;

- сегментация виртуальной инфраструктуры (сегментация виртуальной инфраструктуры) для обработки персональных данных отдельного пользователя и / или группы пользователей.

Кроме того, в информационных системах 3 уровня защищенности персональных данных должны применяться средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 5 класса. Единственное сертифицированное антивирусное программное обеспечение на рынке представлено «Лабораторией Касперского»: – программное изделие «Kaspersky Security для виртуальных сред» [20].

Согласно представленным мерам для виртуализированный инфраструктуры организации необходимо совместное применение:

– средства защиты информации виртуальной среды, реализующее меры;

– антивируса.

Поскольку средств защиты на рынке существует несколько, то выбор наиболее подходящего решения целесообразно производить на основе сравнения функциональных возможностей и применимости.

3.2. Экономическая составляющая проекта. Составление организационно-календарного плана

Реализация процесса общей трудоемкости разработки и этапов оперативно-календарного плана.

Осуществим экспертную оценку, чтобы рассчитать трудоемкость.

Для расчёта трудоемкости воспользуемся отработанной схемой из других подобных работ, в которой трудоемкость (S), была равна 90 чел/дн. и рассчитаем коэффициент приведения. Для подсчета коэффициента приведения создадим специально действующую комиссию, состоящую из

1. руководителя центра информатизации;
2. инженера-электроника;
3. техника-программиста.

Таблица 9-Мероприятия по оценке трудоемкости

Состав комиссии	Рекомендуемый коэффициент приведения, K_i	Весовой значение участия, V_i
Руководитель центра информатизации	1,3	0,35
Инженер- электроник	1,2	0,35
Техник-программист	1,2	0,30

Результирующий коэффициент приведения:

$K=\sum K_i * V_i = 1{,}3 * 0{,}35 + 1{,}2 * 0{,}3 = 1{,}24$

С учетом найденного коэффициента приведения можно произвести расчеты трудоемкости новой разработки:

$$S_н = S * К = 90 * 1{,}235 = 112 \text{ чел/дн}$$

Чтобы провести расчет трудоемкости по стадиям необходимо процесс разделить на этапы:

1. Подготовка;
2. Постановка целей и задач;
3. Изучение методик и специальной технической документации;
4. Выбор и установка оборудования;
5. Специализированная настройка сетей, специальных служб;
6. Пробный запуск и подстройка системы.

Таблица 10-Основные этапы трудоемкости

Этапы	Трудоемкость, чел/дни	Число рабочих, чел	Продолжительность, дни
Подготовка	3	3	1
Постановка целей и задач;	24	6	8
Изучение методик и специальной технической документации;	10	3	10
Выбор и установка оборудования;	15	3	5
Специализированная настройка программного обеспечения, специальных служб;	45	3	15
Пробный запуск и подстройка системы.	15	3	5
Итого:	112	3	44

Таблица 11-Должностные оклады сотрудников

Категория работников	Кол-во работающих, чел.	Должностной оклад, руб./мес.
Руководитель центра информатизации	1	3000
Инженер-электроник	1	1000
Техник-программист	1	1000
Итого:	3	5000

Длительность проектных работ.

Таблица 12- Содержание проектных работ и количество затраченных дней

Этап	**Содержание работ, входящих в этап**	**Вид отчетности по законченной работе**	**Должность исполнителей**	**Продолжительность работы, дни**
Подготовка Постановка целей и задач; Изучение методик и специальной технической документации;	Ознакомление с заданием на проект	Пояснительная записка	Руководитель центра информатизации	1
			Инженер-электроник	1
			Техник-програм-	1
Выбор и установка оборудования;	Написание Технического предложения. Оценка и подбор оборудования и	Техническое предложение Отчет по	Руководитель центра информатизации	8

Специализированная настройка программного обеспечения, спе-	комплектующих. Написание расчетов по проекту	техническому проекту	Инженер-электроник	8
			Техник-программист	8
Подготовка Постановка целей и задач; Изучение методик и специальной технической документации;	Ознакомление с документацией на оборудование и программное обеспечение	-	Руководитель центра информатизации	10
			Инженер-электроник	10
			Техник-программист	10
Выбор и установка оборудования; Специализированная настройка программного обеспечения, специальных служб;	Установка оборудования и подключение кабельных систем	Отчето выполненной работе	Руководитель центра информатизации	5
			Инженер-электроник	5
			Техник-программист	5
Подготовка Постановка целей и задач; Изучение методик и специальной технической документации;	Настройка оборудования (серверов, коммутационных узлов, сетевых хранилищ)	Отчето выполненной работе	Руководитель центра информатизации	15
			Инженер-электроник	15
			Техник-программист	15
Выбор и установка оборудования;	Проверка системы на работоспособность	Акт тестирования	Руководитель центра информатизации	5
			Инженер-электроник	5
			Техник-програм-	5
Итого:				44

Для организации контроля составим график

Таблица 13 -График календарного плана

Исполнители:	Продолж. работы	март 2023																												
Ведущий инженер	21	1 э1	2	3	4 э2	5 э2	6 э2	7 э3	8 э3	9	10	11 э3	12 э3	13 э3	14 э4	15 э4	16	17	18 э4	19 э4	20 э4	21 э4	22 э4	23	24	25 э4	26 э4	27 э4	28 э5	29 э5	30	31
Инженер	21	1 э1	2	3	4 э2	5 э2	6 э2	7 э3	8 э3	9	10	11 э3	12 э3	13 э3	14 э4	15 э4	16	17	18 э4	19 э4	20 э4	21 э4	22 э4	23	24	25 э4	26 э4	27 э4	28 э5	29 э5	30	31
Инженер	21	э1	2	3	4 э2	5 э2	6 э2	7 э3	8 э3	9	10	11 э3	12 э3	13 э3	14 э4	15 э4	16	17	18 э4	19 э4	20 э4	21 э4	22 э4	23	24	25 э4	26 э4	27 э4	28 э5	29 э5	30	31

Исполнители:	Продолж. работы	апрель-май 2023																												
Ведущий инженер	23	1 э5	2 э5	3 э5	4 э6	5 э6	6	7	8 э6	9 э6	10 э6	11 э6	12 э6	13	14	15 э6	16 э6	17 э6	18 э6	19 э6	20	21	22 э6	23 э6	24 э6	25 э7	26 э7	27	28	29 э7	30 э7	1 э7
Инженер	23	1 э5	2 э5	3 э5	4 э6	5 э6	6	7	8 э6	9 э6	10 э6	11 э6	12 э6	13	14	15 э6	16 э6	17 э6	18 э6	19 э6	20	21	22 э6	23 э6	24 э6	25 э7	26 э7	27	28	29 э7	30 э7	1 э7
Инженер	23	1 э5	2 э5	3 э5	4 э6	5 э6	6	7	8 э6	9 э6	10 э6	11 э6	12 э6	13	14	15 э6	16 э6	17 э6	18 э6	19 э6	20	21	22 э6	23 э6	24 э6	25 э7	26 э7	27	28	29 э7	30 э7	1 э7

Расчет себестоимости проекта.

Расчет затрат на оплату труда и сопутствующие расходы.

В оплату труда заложены расходы:

- Основная заработная плата;
- Отчисления в социальные фонды;
- Расходы на служебные командировки;

Расчет фонда заработной платы разработчиков ведется исходя из сложности человеко-дня, количества работников и трудоемкости. Длительность работ, проводимых каждым исполнителем на каждом этапа

Таблица 14-Основная заработная плата.

Номер этапа	Длительность работ, дней		
	Руководитель центра информатизации	Инженер- электроник	Техник-программист
1	1	1	1
2	8	8	8
3	10	10	10
4	5	5	5
5	15	15	15
6	5	5	5
ИТОГ	44	44	44

Стоимость одного человеко-дня рассчитываем по формуле:

$$С_{чел.дн} = О/22$$

где О - должностной оклад работника, а 22 - среднее количество рабочих дней в месяце. Оклады для исполнителей приведены в таблице 11.

Проведем расчет фонда заработной платы разработчиков:

$$З_{пр}=\sum С_i * Т_i = \frac{3000}{22} * 44 + \frac{1000}{22} * 44 + \frac{1000}{22} * 44 = 10000$$

Так как премия для инженерно-технических разработчиков учитывается в их окладах, то ЗОСН = ЗПР. Единый социальный налог. На эту статью относятся отчисления на социальное страхование, отчисления в пенсионный фонд, затраты на медицинское страхование работников и общее страхование от несчастного случая: в Пенсионный фонд, в Фонд социального страхования, в Федеральный и территориальный фонд медицинского страхования.

Итоговые отчисления составляют 26% от суммы основной и дополнительной заработной платы и составляют:

Sсоц = Зосн*0,26 = 10000*0,26 = 2600 рублей

Расходы на служебные командировки. На эту статью относятся расходы на все виды служебных командировок. Они составляют 3% от фонда основной заработной платы, рассчитываются по формуле и составляют:

Sком = Зосн*0,03 = 10000*0,03 = 300 рублей

Таким образом, расходы на оплату труда и сопутствующие расходы составляют 12900 рублей.

Представлено следующими комплектующими: серверы, коммутационное оборудование, сетевые хранилища, дополнительное оборудование.

Таблица 15- Затраты на оборудование виртуальной среды

Наименование комплектующих	**Тип, марка оборудования**	**Кол-во**	**Стоимость единицы, руб.**	**Общая стоимость, руб.**
Сервер сегмента виртуализации	Supermicro SYS-5017C-TF: Intel Xeon E3-1225 V2 (3.20 GHz, 4 ядра) - 16Gb RAM (2x Kingston KVR16E11/8 DDR3 1600) - 4Tb SSHD (2x Seagate Desktop SSHD ST2000DX001 2Tb)	1	4000	4000
Основное сетевое хранилище	HIKVISION H200 NAS 2 Гб ОЗУ	1	3500	3500
Сетевое хранилище резервных копий	Netgear ReadyNAS RN102 16ТБ	1	6000	6000
Сетевой коммутатор для серверного сегмента	D-Link DGS-1016D	1	5 600	5 600
Межсетевой экран	Ideco UTM Enterprise	1	4500	4500
Источник бесперебойного питания	ИБП HIPER CITY-650	1	1000	1000
Прочие комплектующие и расходные материалы	сетевые кабели, коннекторы, устройства ввода-вывода и.т.п.	1	1500	1500
Итого:				26100
Транспортные расходы (3% от общей суммы):				783
Всего:				26883

Часть программного обеспечения виртуальной среды будет бесплатным, распространяемым по лицензии GNU GPL (веб-сервер). Другая часть будет платной. Цены, количество и наименование приобретаемых лицензионных продуктов.

Таблица 16- Затраты на программное обеспечение.

Наименование	Название продукта	Кол-во	Стоимость единицы, руб.	Общая стоимость, руб.
Операционная система для vCenter	VMware vSphere vCenter CentOS Linux	1	1000	1000
Среда виртуализации VMware	VMware vCenter Linux Client	1	2000	2000
Итого:				3000

После проведения расчетов приходим к выводу, что затраты на программное обеспечение для виртуальной образовательной среды будут равны 3000 рублей.

Проведём вычисления да расчёта затрат на электроэнергию, необходимую для разработки.

Стоимость одного киловатта в час для юридических лиц в Челябинской области составляет Сквт =2,28 руб.

Вычислим затраты на электроэнергию, необходимую для разработки

Сэл=Сквт*Т*Эп*К*п

Таблица 17- Затраты на программное обеспечение. Основные потребители энергии.

Потребители	Время экспл.$T_э$ руб.	Кол-во n, шт.	max, энергопотребление $Э_П$, кВт/ч.	Коэф. исп. K	Стоимость эл. энергии $C^{эл}$,руб.
Серверы ЦОД	30х24ч.	2	0,5	0,99	1625
Сетевые хранилища	30х24ч.	2	0,5	0,99	1625
Коммутационное оборудование	30х24ч.	1	0,085	0,99	138

Светильник	22х8ч.	2	4х0,04	0,8	102
Прочие потребители энергии (кондиционер)	30х8ч.	1	0,5	0,99	270
Итого:					3760

Примечание: после ввода в эксплуатацию ЦОД энергопотребление оборудования должно быть пересмотрено. Общая стоимость затраченной электроэнергии на разработку системы составила Сэл.общ = 3760 рублей. Таким образом, за период работ равный двум месяцам, на оплату электроэнергии потребуется 7520 рублей.

Амортизационные отчисления.

Амортизационные отчисления определяются исходя из норм амортизации и балансовой стоимости по видам оборудования:

$$K = (1/n) \times 100\%$$

где K - норма амортизации в процентах к остаточной стоимости, применяемая к данному объекту амортизируемого имущества.

n - срок полезного использования данного объекта амортизируемого имущества, выраженный в месяцах.

При использования информационной системы в течение десяти лет норма амортизации будет 0,833% в месяц.

Сумма амортизации на оборудование ЦОД за период в один месяц будут:

26100* 0,833% = 217 рублей

Амортизационные расходы на оборудование за период создания ЦОД равный двум месяцам, будут 434 рубля.

Смета затрат на разработку проекта.

Таблица 18- Смета затрат на разработку виртуальной среды указана в таблице

Наименование затрат	Сумма затрат, руб.
Расчет затрат на оплату труда и сопутствующие расходы	12900
Затраты на оборудование	26883
Затраты на программное обеспечение	3000

Затраты на электроэнергию, необходимую для разработки системы	7520
Амортизационные отчисления	434
Итого:	50737

Общие затраты на создание проекта составляют 50737 рублей.

Виртуализация инфраструктуры, применяемая виртуальной среды, обеспечивает снижение расходов и при этом увеличивает эффективность, коэффициент использования и повышает гибкость имеющихся активов:

- Увеличение отдачи от аппаратных ресурсов: объединение общих ресурсов инфраструктуры в пулы (консолидация серверов), увеличение уровня использования серверного оборудования.
- Снижение расходов на виртуальную среду за счет уменьшения физической инфраструктуры. Уменьшение числа серверов и сопутствующих устройств влечет за собой уменьшение необходимой площади помещений и сокращение потребностей в электроэнергии на питание и охлаждение.
- Увеличение доступности оборудования и приложений для повышения уровня непрерывности бизнеса: надежное резервное копирование и перенос виртуальных сред целиком без прерывания работы. Исключение плановых простоев и быстрое восстановление после непредвиденных сбоев.
- Эксплуатационная гибкость: оперативное реагирование на изменения рынка благодаря динамическому управлению ресурсами и ускоренной инициализации серверов.
- Улучшение управляемости: развертывание и администрирование виртуализированных ресурсов значительно удобнее и эффективнее за счет консолидации программной составляющей и дополнительной централизации управления.

Все эти требования успешно выполняет новый виртуальный виртуальной среды.

3.3 Экономическое обоснование внедрения рекомендаций по совершенствованию защиты информации при использовании виртуальных сред в колледже

Самой большой проблемой для руководителей организаций и IT- специалистов являются целесообразность перехода на облачную платформу и оценка экономических выгод и рисков от внедрения облачных вычислений. Оценка экономической эффективности является необходимым компонентом любого технико-экономического обоснования ИТ-проекта. Это увеличивает важность вопросов по выбору методики по оценке эффективности и рисков от внедрения ИТ.

Главной особенностью принятия решений на внедрение облачных технологий является то, что они принимаются в условиях высокой неопределенности среды. Также важно понимать, что технико-экономические расчеты носят ориентировочный характер. Их стоит проводить, если ваша задача - обосновать целесообразность модернизации ИТ-инфраструктуры на конкретном объекте и выбрать наиболее эффективный, в том числе и с экономических позиций, вариант реализации данной инфраструктуры из числа возможных альтернатив. При неполноте и невысоком качестве исходной информации лицо, принимающее решение, вынуждено отклониться от точных числовых оценок, заменяя качественными характеристиками. К сожалению, все еще не существует идеального метода защиты данных, доступных для рядового потребителя облачных сервисов. В каждом из рассмотренных вариантов предоставления облачных услуг существуют свои особенности, способные привлечь пользователей и отвечать их поставленным задачам. Но, так как облачные услуги появились сравнительно недавно, можно ожидать, что в скором времени появится больше вариантов решения данной проблемы.

Преимущества:

- Экономия на аппаратном обеспечении при консолидации серверов;
- Оборудование для системы занимает меньше места в стойке;

- Добавляются дополнительные возможности администрирования;
- Улучшается система безопасности;
- Значительно упрощается процесс делегирования полномочий;
- На одном компьютере возможно использование серверов под управлением различных ОС;
- Возможность поддержания старых операционных систем в целях обеспечения совместимости;
- Возможность изолировать потенциально опасные окружения;
- Возможность создания требуемых аппаратных конфигураций;
- На одном хосте может быть запущено одновременно несколько виртуальных машин, объединенных в виртуальную сеть.

Недостатки:

- Невозможность эмуляции всех устройств;
- Виртуализация требует дополнительных аппаратных ресурсов;
- Платформы виртуализации требовательны к аппаратному обеспечению;
- Хорошие платформы виртуализации достаточно дорогие.

Выводы по главе 3

Проанализировав во второй главе виртуальную образовательную среду ГБПОУ «Миасский машиностроительный колледж» в условиях обеспечения информационной безопасности, в третьей главе магистерской диссертации были описаны аспекты осуществления разработки и реализации методических рекомендаций по совершенствованию системы обеспечения информационной безопасности функционирования виртуальной среды колледжа.

Методические рекомендации по совершенствованию системы обеспечения информационной безопасности функционирования виртуальной среды ГБПОУ «Миасский машиностроительный колледж» представлены в Приложении 2. Перед внедрением любых новшеств в систему информационной без-

опасности любые нововведения проходят экспертную оценку или процесс согласования. Экспертами методических рекомендаций выступили члены администрации и специалист по информатизации, ответственный за различные аспекты обеспечения информационной безопасности колледжа.

Все эксперты поставили высокие оценки методическим рекомендациям по совершенствованию системы обеспечения информационной безопасности функционирования виртуальной образовательной среды ГБПОУ «Миасский машиностроительный колледж», рекомендовали их к внедрению.

На основании результатов экспертизы были приняты следующие решения:

отдельные меры по проектированию модели виртуальной образовательной среды профессиональной образовательной организации, а также меры по совершенствованию системы защиты информации включены в план работы на 2024–2025 учебный год.

отдельные меры по обеспечению информационной безопасности студентов в процессе функционирования виртуальной образовательной среды и меры по совершенствованию осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в виртуальной образовательной среды включены в план работы на 2023–2024 год.

Работа по выполнению методических рекомендаций, направленных на совершенствование системы обеспечения информационной безопасности функционирования виртуальной образовательной среды ГБПОУ «Миасский машиностроительный колледж» не исчерпывается и будет продолжена в соответствии с планом работы на учебный год.

ЗАКЛЮЧЕНИЕ

В настоящее время виртуальные среды получили активное распространение как среди организаций, нуждающихся в дополнительной вычислительной мощности, так и среди простых людей, желающих упростить процесс обработки и хранения данных. Но вместе с ростом пользователей увеличилось и количество выявленных уязвимостей этого метода обработки данных. Как и любые другие средства обработки данных, облачные сервисы имеют свои преимущества и недостатки.

Выделяют несколько преимуществ, связанных с использованием облачных технологий:

1. Доступность.

Доступ к информации, хранящейся в облачном сервисе, может получить любой человек, имеющий в своем распоряжении компьютер, планшет, либо любое мобильное устройство, подключенное к сети интернет.

2. Мобильность.

У пользователя нет постоянной привязанности к одному рабочему месту. Обработка информации может проводиться из любой точки мира со скоростью, равной скорости интернет-соединения пользователя.

3. Экономичность.

Одним из важных преимуществ является сниженная затратность использования облачных сервисов по сравнению со стандартными центрами обработки данных, так как в данном случае у пользователя нет необходимости в покупке дорогостоящих компьютеров и программного обеспечения, а также он освобождается от необходимости нанимать специалиста по обслуживанию локальных IT-технологий.

4. Аренда.

Пользователь имеет право получать только необходимые пакеты услуг с

фактической оплатой потребляемой мощности и не переплачивать за ненужные функции.

5. Гибкость.

Все необходимые ресурсы предоставляются провайдером автоматически.

6. Высокая технологичность.

Провайдеры стремятся предоставить клиентам все большие вычислительные мощности, которые можно использовать для хранения, анализа и обработки данных. Поэтому данная отрасль активно развивается в настоящее время.

7. Надежность.

Некоторые эксперты утверждают, что надежность, которую обеспечивают современные облачные вычисления, гораздо выше, чем надежность локальных ресурсов, потому что только небольшое количество предприятий способно позволить себе полноценный центр обработки данных и обеспечить ему надлежащее содержание и безопасность.

Несмотря на все положительные отзывы, существует и определенная критика в адрес облачных технологий. Согласно исследованиям аналитической фирмы IDC, многие компании, в первую очередь, связывают с «облачными» сервисами большие проблемы по части безопасности. А независимая исследовательская организация PortioResearch только подтвердила это, указав конкретные цифры: 68 % опрошенных руководителей европейских IT-компаний, в целях безопасности, отказываются использовать облачные технологии. Это связано с тем, что надёжность, своевременность получения и доступность данных, расположенных облачном хранилище, очень сильно зависит от многих промежуточных параметров, таких как: каналы передачи данных на пути от клиента к платформе, качество работы интернет-провайдера клиента, доступность облачного сервиса в данный момент времени. Также существует угроза того, что компания, предоставляющая облачные услуги будет

ликвидирована по тем или иным причинам, и клиент не сможет получить доступ к своим данным. Но, вне зависимости от этого, большинство экспертов придерживается того мнения, что преимущества данной технологии перевешивают ее недостатки.

В зависимости от нужд клиентов предоставляются несколько моделей реализации облачных технологий. Самой безопасной из них является модель частного облака, а наиболее уязвимой - модель публичного облака. Также облака делятся по моделям обслуживания. Каждая из них имеет свои преимущества и недостатки и выбирается пользователем исходя из преследуемых целей. Среди индивидуальных клиентов наибольшее распространение получила модель обслуживания SaaS. В настоящий момент времени все большее количество компаний предлагают свои приложения на основе данной модели. Но, в то же время, эта услуга по обработке информации является наименее безопасной.

В соответствии с поставленными задачами в данной работе были рассмотрены существующие модели угроз в облачных вычислениях и протестированы возможные меры по повышению безопасности пользовательских файлов. Методы аутентификации и разграничения доступа не были рассмотрены в силу того, что они не являются доступными рядовому пользователю.

В силу стремительного развития облачной инфраструктуры стоит ожидать появления в скором времени универсальных методов обеспечения безопасности данных. Но на сегодняшний день выделение наиболее оптимального метода защиты не является возможным, так как к каждому типу услуги должен быть применен индивидуальный подход в соответствии с преследуемыми целями заказчика облачных сервисов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аксюхин, А.А. Информационные технологии в образовании и науке / Аксюхин А.А., Вицен А.А., МекшеневаЖ.В. // Современные наукоемкие технологии, 2019. № 11. С. 50–52.

2. Афонина, Е. С. Модель обеспечения информационной безопасности школьников при создании единого информационного пространства школы [Текст] / Е. С. Афонина. // Молодой ученый. – 2015. – № 6.4 (86.4). – С. 68-71.

3. Блинов В. И. Цифровая дидактика: модный тренд или новая наука? / Профессиональное образование // Столица. 2019. – № 3. – С. 27

4. Вартанова, Е.Л. Индустрия российских медиа: цифровое будущее: академическая монография / Е.Л.Вартанова, А.В. Вырковский, М.И. Максеенко, С.С. Смирнов. М.: МедиаМир, 2017. 160 с.

5. Главный тренд российского образования – цифровизация. [Электронный ресурс] // URL: http://www.ug.ru/article/1029/ (дата обращения: 30.09.2022).

6. Игнатов, С. Д. Обеспечение защиты информации в виртуализированной инфраструктуре / С. Д. Игнатов, А. А. Быстров. — Текст : непосредственный // Молодой ученый. — 2021. — № 24 (366). — С. 30–34. — URL: https://moluch.ru/archive/366/82146/ (дата обращения: 21.11.2023).

7. Мельников В.П. Информационная безопасность и защита информации: учеб.пособие для студентов высших учебных заведений.– М.: Издательский центр «Академия», 2008. – 336 с.

8. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости (утв. Министерством здравоохранения и социального развития РФ 23 декабря 2009 г.).

9. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информаци-

онных системах персональных данных с использованием средств автоматизации [Электронный ресурс]: утв. ФСБ РФ 21 февраля 2008г. N149/54-144 //СПС Консультант Плюс.

10. Михеева Е.В. Информационные технологии в профессиональной деятельности: учебник / Е.В. Михеева, О.И. Титова. М.: Издательский центр «Академия», 2019. - 416 с.

11. Моисеев, В.Б. Информационные технологии в системе высшего образования. / В.Б. Моисеев. Пенза: Изд-во Пенз. технол. ин-та, 2014. – 100с.

12. Моисеев, В.Б. Элементы информационно-образовательной среды высшего учебного, заведения. / В.Б. Моисеев. Ульяновск: Изд-во Ул. ГТУ, 2015. – 122с.

13. Мушкина, И.А. Организация самостоятельной работы студента: учебное пособие для вузов / И. А. Мушкина, Е. Н. Куклина, М. А. Мазниченко. 2-е изд., испр. и доп. Москва: Издательство Юрайт, 2016. - 186 с.

14. Обеспечение информационной безопасности организации. – URL: http://www.iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/ (дата обращения: 20.05.2023).

15. Омелаенко, Н.В. Методика и организация самостоятельной работы студентов / Н.В. Омелаекно // Современные наукоемкие технологии. 2016. – № 2-3. – С. 538-542.

16. Официальный сайт ГБПОУ «Миасский машиностроительный колледж». – URL: https://miassmk.ru (дата обращения: 22.11.2022).

17. Положение об электронных образовательных ресурсах ГБПОУ «Миасский машиностроительный колледж». – URL: https://miassmk.ru (дата обращения: 22.11.2022).

18. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну (утв. приказом ФСТЭК России от 29 апреля 2021 г. № 77).

19. Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн при использовании средств криптографической защиты информации» // «Российская газета» от 17 сентября 2014 г. N 211.

20. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // «Российская газета», № 107, 22.12.2022.

21. Роберт, И.В. Основные понятия Единого информационного образовательного пространства / И.В. Роберт, Ю.А. Прозорова, В.А. Касторнова // Ученые записки ИИО РАО. – М.: 2015. Вып. 6. С. 5-12.

22. Роберт, И.В. Толковый словарь терминов понятийного аппарата информатизации образования / И.В. Роберт. – М.: Институт информатизации образования РАО, 2006. – 88 с.

23. Рогозин В.В. Основы информационной безопасности: учеб. пособие. – М.: Юнита-Дана, 2016. – 287 с.

24. Российская педагогическая энциклопедия. [электронный ресурс] – URL: http://www.gumer.info/bibliotek_Buks/Pedagog/russpenc/15.php.

25. Рыжко, А.Л. Экономика информационных систем: учебное пособие. / А.Л. Рыжко, Н.М. Лобанова, Н.А. Рыжко, Е.О. Кучинская – М.: Финансовый университет, 2014. – 204 с.

26. Савостикова, О.В. Выбор и классификация средств разработки электронных учебных пособий / О.В.Савостикова. URL: http://www.ict.edu.ru/vconf/ files/ 11684.pdf (дата обращения 21.01.2023).

27. Шарафутдинова, А.Р., Пядышев, В.С. Защита информации в образовательных учреждениях [Текст] / А.Р. Шарафутдинова, В.С. Пядышева. – URL:http://www.rusnauka.com/17_APSN_2013/Matemathics/2_140911.doc.htm.

28. Шоломицкий А.Г. Теория риска. Выбор при неопределенности и моделирование риска: Учеб. пособие для колледжов. Гос. ун-т - Высшая школа экономики. - М.: Изд. дом ГУ ВШЭ, 2015. - 400 с.

29. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации: учеб. пособие. - М.: Гелиос АРВ, 2015. - 224 с.

30. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. - СПб: Наука и техника, 2014. - 384 с.

31. Ямалов И.У. Моделирование процессов управления и принятия решений в условиях чрезвычайных ситуаций. - М.: Лаборатория Базовых Знаний, 2017.-288 с.

32. Ярочкин, В.И. Информационная безопасность [Текст]: Учебник для вузов / В.И. Ярочкин. – М.: Академический Проект, 2018. – 544 с.

33. Ярочкин, В.И. Информационная безопасность: Учебник для вузов

ПРИЛОЖЕНИЕ 1Сравнение типов подключения

Подключение	Требования на стороне сервис-провайдера	Подключение клиента	Плюсы	Минусы
RDP-клиент	Наличие выделенного сервера терминалов (Terminal Server)	Запуск клиента RDP	Мультиплатформность, гибкая система настройки	Слабое шифрование при использовании настроек по умолчанию, необходимость использовать дополнительные методы защиты
RemoteApp	Наличие сконфигурировано го RD Session Host Server с размещенным на нем списком соответствующих программ (RemoteApp Programslist)	Запуск иконки приложения с рабочего стола или из меню Start для инициирования подключения к приложению по RDP (из списка RemoteApp Programslist).	Обеспечение доступности приложения в условиях низкой скорости интернета, позволяет совмещать работу на локальной машине и использования приложения в облаке	Дает доступ только к одному приложению
Веб-доступ	Наличие выделенного сервера терминалов (Terminal Server)	Использование URL для доступа к ресурсу посредством веб-браузера.	Легкость использования	Нет защищенной линии передачи, требуется проходить аутентификацию
Remote access VPN	Наличие сконфигурирванно го VPN-сервера	Запуск ярлыка для подключения к VPN-серверу.	Не надо устанавливать дополнительные приложения	Наличие VPN-сервера на стороне провайдера, необходимо проходить аутентификацию
VPN site-tosite	Наличие двух	При	Отсутствие	Необходим

	сконфигурированных VPN-серверов.	обращении к ресурсам VPN-подключение организуется автоматически на уровне серверов	необходимости создания и запуска ярлыка VPN-подключения, прозрачно для конечного пользователя	VPN-сервер в компании и VPN-сервер в облаке
DirectAccess	Наличие одного или более серверов DirectAccess в составе домена, Наличие центра сертификации (PKI), Windows-инфраструктура	При наличии доступа к сети Интернет происходит автоматическое построение надежного туннеля между клиентом и сервером	Доступ к ресурсам компании прозрачен для пользователя, Физическое местоположение клиента не имеет значения	Ограниченный список клиентских ОС, с которых возможно подключение: Windows 7 Enterprise или Windows 7 Ultimate, Компьютер клиента должен входить в состав домена.
VDI	Развернутая инфраструктура виртуальных рабочих столов VDI (решения от VMware, Citrix, Microsoft)	Пользователь получает свой собственный виртуальный ПК	Можно подключаться с помощью тонкого клиента, настольного ПК, ноутбука, планшета, мобильного телефона	При сбое в приложения в терминальном режиме вместе с пользователем, запустившим такое приложение, перезагрузятся и остальные пользователи, работающие на этом же сервере

ПРИЛОЖЕНИЕ 2

Методические рекомендации по совершенствованию системы обеспечения информационной безопасности функционирования виртуальной образовательной среды ГБПОУ «МиМК»

Необходимостью использования контроля во всех сферах деятельности человека, общества и государства обуславливается огромное распространение виртуальных технологий. Приоритетный порядок представляется информатизации всех сфер профессионального образования.

В направленности на основные тренды экономики и процессы развития капитала человека заключается общемировой прогресс, в котором полноценными участниками прогресса будут в совершенстве владеющие цифровыми навыками.

Для обеспечения информационной безопасности функционирования виртуальной образовательной среды в ГБПОУ «МиМК» необходимо проводить мероприятия по плану:

- блокировку утечки персональных данных в полном или частичном объеме и нарушения конфиденциальности;
- запрет на доступ к персональным данным и защищенным данным;
- организацию прерывания доступности к компонентам программы;
- мониторинг изменения целостности, проникновения в служебные данные;
- отслеживание нестабильного или не свойственного проведение операций для компонентов;
- блокировка нарушения способов передачи и функциональности.

Своевременное обнаружение случаев чрезвычайных ситуаций, в которых должна обеспечиться безопасность информации и функционирование системы с исключением создания угроз, необходимо проводить при строгом соблюдении норм и требований федерального законодательства.

После проведения процедуры оценки источников угроз безопасности информации необходимо выявить, какие виды нарушителей могут совершить действия по преодолению средств защиты, и с какой целью они проводят эти преступления, а также исключить возможность для создания условий для совершения непреднамеренных угроз безопасности.

Для своевременного обнаружения ситуаций, в которых должна обеспечиться безопасность информации и функционирование системы с исключением создания угроз необходимо анализировать предполагаемые мотивы сторонних и внутренних нарушителей, которые заинтересованы в нарушении безопасности конкретной системы.

Сценарии для осуществления опасных действий для сетей, которые реально могут разрушить безопасность, могут быть следующими:

- поиск уязвимостей программного обеспечения, которые можно использовать для нанесения сетям повреждений;
- использование программного обеспечения, которое преднамеренно наносит вред;
- использование нелицензионного программного обеспечения или некачественных технических средств;
- встраивание в систему программы или изменение фрагмента программы путем скрытого внедрения;
- распространение конфиденциальной информации в случаях осуществления атак по скрытым каналам;
- перехват средством измерений побочных электромагнитных излучений, наводок различных средств вычислительной техники, используемой для распространения конфиденциальной информации;
- преодоление всех уровней защиты различных средств вычислительной техники, используемой для распространения конфиденциальной информации;

− преднамеренные технические нарушения при проведении настройки всех уровней защиты различных средств вычислительной техники, используемой для распространения конфиденциальной информации;

− не преднамеренные технические нарушения при проведении настройки всех уровней защиты различных средств вычислительной техники, используемой для распространения конфиденциальной информации.

Оценка действий осуществления опасных действий для сетей также проводится с целью исключения рисков возможных сценариев при совершении преднамеренных угроз безопасности объектами, которые реально могут ее разрушить.

Ответственный подход при работе с сотрудниками организации, которые не поддаются провокациям и не вступают в сговор со сторонними нарушителями, исключает возможные сценарии для совершения непреднамеренных угроз безопасности, и представители служб разведки недружественных государств, радикально - ориентированные группы, нарушители законодательства, хакеры и конкуренты не смогут с помощью внутренних специалистов совершить противоправные действия и разрушить безопасность.

ПРИЛОЖЕНИЕ 3

Памятка для педагогических работников по обеспечению информационной безопасности обучающихся

1. Доведите до сведения студентов правила безопасного поведения в Интернете, проведите разъясняющие беседы о законодательной базы мерах ответственности за их нарушение

2. Продумайте алгоритм действий студентов, если произошло нарушение безопасности поведения.

3. Сформируйте правила уважительного и равноправного поведения студентов в информационном пространстве, проведите разъясняющие беседы о законодательной базе и ответственности за их нарушение авторских прав.

4. Проводите мониторинг социальных сетей студентов и доводите до сведения при необходимости родителям (законным представителям) о небезопасных ситуациях.

5. Способствуйте формированию ответственности при работе с источниками из интернет-пространства.

6. Запретите посещать запрещённые сайты и научите проверять достоверность полученной информации.

7. Реализуйте мероприятия программы воспитания, стараясь разнообразить перечень воспитательных мероприятий для правильного восприятия реальной жизни.

8. Организуйте мероприятия по профилактике интернет-зависимости.

9. Мотивируйте студентов на использование в качестве источников информации не только интернет-источники, но и другие более традиционные.

10. После проводите мониторинг социальных сетей студентов при обнаружении небезопасных ситуациях, привлекайте при необходимости психолога, социальных педагогов.

11. Организуйте свое обучение по повышению компетенций цифровой грамотности.

12. Приводите студентам примеры по ответственному поведению в интернет-пространстве.