



**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**

**Цифровая среда профессиональной образовательной организации в
условиях обеспечения информационной безопасности**

**Магистерская диссертация
по направлению: 44.04.04 Профессиональное обучение (по отраслям)
Направленность (профиль): Управление информационной безопасностью в
профессиональном образовании
Форма обучения заочная**

Проверка на объём заимствований:
88 авторского текста

Работа рекомендована к защите
«18» 07 2021 г.
Зав. кафедрой АТ, ИТ и МОТД
[подпись] В.В. Руднев

Выполнил:
студентка группы ЗФ-309/210-2-1,
Бугаевская Марина Витальевна
Научный руководитель:
к.п.н., ст. преподаватель
кафедры АТ, ИТ и МОТД
Гафарова Елена Аркадьевна

[подпись]

**Челябинск
2021**

Аннотация

на магистерскую диссертацию
Бугаевской Марины Витальевны

Тема магистерской диссертации «Цифровая среда профессиональной образовательной организации в условиях обеспечения информационной безопасности».

Магистерская диссертация содержит 96 страниц, 3 рисунка, 87 источника литературы.

Ключевые слова: цифровая образовательная среда, целевая модель цифровой образовательной среды, информационная безопасность, профессиональная образовательная организация.

Объектом исследования является процесс организации и функционирования цифровой образовательной среды.

Цель магистерской диссертации состоит в выявлении, теоретическом обосновании и экспериментальной проверке методических рекомендаций по совершенствованию системы обеспечения информационной безопасности функционирования цифровой образовательной среды

В процессе исследования осуществлены анализ изученности проблемы обеспечения информационной безопасности цифровой среды профессиональной образовательной организации; историографический анализ наиболее значимых нормативно-правовых документов по обеспечению информационной безопасности функционирования цифровой образовательной среды; определено содержание основных понятий исследуемой проблемы: цифровая среда, модель цифровой образовательной среды, информационная безопасность; произведен анализ цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» в условиях обеспечения информационной безопасности; описаны этапы совершенствования цифровой образовательной среды в условиях обеспечения информационной безопасности. Разработаны методические

рекомендации по совершенствованию системы обеспечения информационной безопасности в условиях функционирования цифровой образовательной среды; представлены результаты апробации данных рекомендаций.

В заключении диссертационной работы сделаны основные выводы по результатам исследования.

Магистрант: Бугаевская Марина Витальевна

(Ф.И.О.)

Подпись

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	6
ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ФУНКЦИОНИРОВАНИЯ ЦИФРОВОЙ СРЕДЫ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ В УСЛОВИЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	14
1.1 Нормативно-правовые основы организации и функционирования цифровой образовательной среды в условиях обеспечения информационной безопасности.....	14
1.2 Целевая модель цифровой образовательной среды	27
1.3 Характеристика цифровой образовательной среды профессиональной образовательной организации в условиях обеспечения информационной безопасности.....	32
Выводы по главе 1.....	44
ГЛАВА 2. АНАЛИЗ ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ГБПОУ «МИАССКИЙ ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ» В УСЛОВИЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	46
2.1 Анализ модели цифровой образовательной среды ГБПОУ «Миасский педагогический колледж».....	46
2.2 Анализ цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» по реализации мер информационной безопасности.....	49
Выводы по главе 2.....	59
ГЛАВА 3. СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ.....	62

3.1 Разработка методических рекомендаций по совершенствованию системы обеспечения информационной безопасности функционирования цифровой образовательной среды.....	62
3.2 Анализ результатов реализации методических рекомендаций по совершенствованию системы обеспечения информационной безопасности функционирования цифровой образовательной среды.....	66
Выводы по главе 3.....	73
ЗАКЛЮЧЕНИЕ	75
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	80
ПРИЛОЖЕНИЕ 1 Методические рекомендации по совершенствованию системы обеспечения информационной безопасности функционирования цифровой образовательной среды профессиональной образовательной организации	92
ПРИЛОЖЕНИЕ 2 Бланк оценочного листа для проведения экспертизы	149
ПРИЛОЖЕНИЕ 3 Дополнительная профессиональная программа повышения квалификации «Обеспечение информационной безопасности функционирования цифровой образовательной среды профессиональной образовательной организации»	150
ПРИЛОЖЕНИЕ 4 Памятка для педагогических работников по обеспечению информационной безопасности обучающихся.....	163

ВВЕДЕНИЕ

Актуальность исследования. В настоящее время стремительное развитие и массовое распространение цифровых технологий создает необходимость их применения и контроля во всех сферах деятельности общества и государства. Информатизация сферы образования осуществляется в приоритетном порядке.

Глобальная задача общемирового прогресса, в том числе, и прогресса государств заключается в развитии человеческого капитала, ориентированного на тренды цифровой экономики, которые свидетельствуют о необходимости формирования навыков, которые потребуются в будущем для полноценного участия в процессах, на основе которых будет функционировать «цифровое общество». В связи с этим программа «Цифровая экономика Российской Федерации», утвержденная распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р, выдвигает новые требования к системе профессионального образования.

Согласно ст. 68 Федерального закона РФ «Об образовании в Российской Федерации», среднее профессиональное образование направлено на решение задач интеллектуального, культурного и профессионального развития человека и имеет целью подготовку квалифицированных рабочих или служащих и специалистов среднего звена по всем основным направлениям общественно полезной деятельности в соответствии с потребностями общества и государства, а также удовлетворение потребностей личности в углублении и расширении образования. Реализация данных способностей у студентов в современном обществе не может обойтись без организации безопасной цифровой среды профессиональной образовательной организации, поскольку данная среда способствует обеспечению высокого уровня цифровой грамотности, изменению форм,

методов, технологий обучения, внедрению новых подходов в системе профессионального образования.

Понятие «цифровой среды профессиональной образовательной организации» определяет характеристику современной образовательной среды, которая подвержена процессам цифровизации с активным применением цифровых технологий и ресурсов, при этом, в первую очередь, решаются образовательные задачи, а, следовательно, может именоваться цифровой образовательной средой (ЦОС).

Кроме того, президентом Российской Федерации В.В. Путиным поставлена задача по созданию современной и безопасной цифровой образовательной среды до 2024 года, то есть, в правовых актах, регламентирующих стратегию развития образования, среда профессиональной образовательной организации определена как ЦОС. Внедрение цифровых технологий в систему образования является стратегической задачей государства.

Актуальность исследования на социально-педагогическом уровне определяется нормативно-правовыми документами РФ в сфере образования. В рамках национального проекта «Образование» представлен региональный проект «Цифровая образовательная среда», основной целью которого является создание современной и безопасной цифровой образовательной среды, обеспечивающей формирование ценности к саморазвитию и самообразованию у обучающихся. Реализация данного проекта позволит:

1. Создать условия для развития цифровизации образовательного процесса в соответствии с основными задачами, условиями и особенностями функционирования цифровой образовательной среды для разных уровней образования.
2. Усовершенствовать образовательный процесс по отдельным предметным областям путем внедрения современных цифровых технологий.

3. Предоставить возможность обучающимся использовать технологии виртуальной и дополненной реальности, цифровых двойников и другие технологии в освоении отдельных предметных областей.
4. Создать условия для подготовки высококвалифицированных кадров, обладающих актуальными компетенциями в сфере современных технологий и др.

Организация цифровой образовательной среды профессиональной образовательной организации должно осуществляться в соответствии требованиями информационной безопасности, поскольку ее функционирование сопровождается полем различного рода угроз.

Степень разработанности проблемы. К настоящему времени в различных областях современной науки имеется обширная теоретическая база по смежным аспектам рассматриваемого процесса.

Проблема информатизации и цифровизации образования раскрывается в работах А.А. Аксюхана, Л.М. Андрюхиной, В.И. Блинова, Я. А. Ваграменко, Е.Л. Варгановой, А.Ф. Зубаирова, С. Л. Лобачева, Н.П. Петровой, И.В. Роберта, Э.К. Самерхановой, У.Н. Тайлакова.

Проблема организации цифровой образовательной среды образовательной организации рассматривается в трудах А.А. Андреева, Р.К. Елжановой, Н.Б. Завьялова, Н.Н. Курова К.Г. Кязимова, В.Б. Моисеева, И.Р. Сташкевич и др.

Исследованию информационной безопасности посвящены работы Е.С. Афониной, Е.Б. Белова, Ю.И. Богатыревой, А.С. Ильина, А.А. Малюк, Г.В. Михалева, В.А. Пимонова, А.Н. Привалова, А.Ф. Чипига, Е.М. Шпагиной, М.И. Шубинского, В.И. Ярочкина и др.

Однако вышеперечисленные труды рассматривают различные аспекты создания цифровой среды в условиях обеспечения информационной безопасности, тогда как специфика функционирования данной среды в профессиональной образовательной организации рассмотрена недостаточно.

Актуальность исследования на научно-теоретическом уровне обусловлена необходимостью системно представить обоснование проблемы реализации информационной безопасности в рамках цифровой среды, выявить условия и разработать методику обеспечения информационной безопасности в процессе создания и функционирования цифровой среды профессиональной образовательной организации.

Реализация приоритетного проекта «Современная цифровая образовательная среда в Российской Федерации» требует особых подходов к организации цифровой среды образовательной организации, которая должна быть «открытой» и обеспечивать возможность и право пользователей использовать разные информационные системы в ее составе, заменять их или добавлять новые. В связи с этим особое внимание необходимо уделять обеспечению информационной безопасности, направленной на ограждение обучающихся от информации, которая может негативно повлиять на их формирование и развитие, то есть пропаганду различной направленности. Однако в настоящее время не разработаны методические рекомендации по обеспечению информационной безопасности (ИБ) в процессе создания и функционирования цифровой образовательной среды профессиональной образовательной организации. Это актуализирует рассматриваемую проблему на научно-методическом уровне.

Сравнительный анализ существующих теоретических и практических исследований в области обеспечения информационной безопасности в процессе создания и функционирования цифровой среды профессиональной образовательной организации позволили выявить следующие противоречия:

- на социально-педагогическом уровне – между потребностью создания современной и безопасной цифровой образовательной среды, обеспечивающей формирование ценности к саморазвитию и самообразованию у обучающихся и недостаточной динамичностью и гибкостью системы среднего профессионального образования в

обеспечении информационной безопасности функционирования цифровой среды;

- на научно-теоретическом уровне – между необходимостью обеспечения информационной безопасности функционирования цифровой образовательной среды и недостаточной теоретической и методической разработанностью данного процесса в педагогической науке;
- на научно-методическом уровне – между необходимостью повышения информационной безопасности функционирования цифровой образовательной среды и отсутствием соответствующего методического инструментария.

Установленные противоречия позволяют утверждать, что в теории и практике среднего профессионального образования существует проблема: каковы условия и методика обеспечения информационной безопасности функционирования цифровой образовательной среды профессиональной образовательной организации.

Существование данной объективной проблемы в системе профессиональной подготовки студентов колледжа, необходимость ее научнообоснованного решения свидетельствуют об актуальности исследования и позволяют сформулировать его тему как «Цифровая среда профессиональной образовательной организации в условиях обеспечения информационной безопасности».

Цель исследования состоит в выявлении, теоретическом обосновании и экспериментальной проверке методических рекомендаций по совершенствованию системы обеспечения информационной безопасности функционирования цифровой среды профессиональной образовательной организации.

Объектом исследования является процесс организации и функционирования цифровой среды профессиональной образовательной организации.

Предмет исследования: процесс обеспечения информационной безопасности функционирования цифровой среды профессиональной образовательной организации.

Ограничение в диссертации: исследование проводилось на базе профессиональной образовательной организации среднего профессионального образования.

Гипотеза исследования состоит в предположении о совершенствовании системы обеспечения информационной безопасности функционирования цифровой среды профессиональной образовательной организации при реализации методических рекомендаций, обоснованных анализом модели цифровой среды и современными требованиями обеспечения ИБ.

Цель исследования достигается за счет постановки и решения следующих **задач**:

- 1) изучить законодательные акты и нормативно-правовые документы в области организации и функционирования цифровой среды профессиональной образовательной организации;
- 2) описать целевую модель цифровой среды;
- 3) представить характеристику ЦОС профессиональной образовательной организации в условиях обеспечения информационной безопасности;
- 4) проанализировать модель цифровой среды профессиональной образовательной организации (на примере базы исследования) в условиях обеспечения информационной безопасности;
- 5) разработать и апробировать методические рекомендации по совершенствованию системы обеспечения информационной безопасности функционирования цифровой среды профессиональной образовательной организации (на примере базы практики).

Методологической и теоретической базой исследования являются фундаментальные работы в области:

– педагогики и психологии (Ю.К. Бабанский, В.П. Беспалько, Л.С. Выготский, П.Я. Гальперин, И.Я. Лернер, В.А. Сластенин и др.);

– информатизации образования (С.А. Бешенков, А.А. Кузнецов, М.П. Лапчик, Л.П. Мартиросян, А.Н. Привалов, И.В. Роберт и др.);

– компетентностного подхода к организации образовательного процесса (В.И. Байденко, А.С. Белкин, Э.Ф. Зеер, И.А. Зимняя, А.К. Маркова, А.В. Хуторской, Н.Ф. Ефремова);

– системного подхода (В.И. Андреев, Ю.К. Бабанский, А.П. Беляев, В.П. Беспалько, С.М. Маркова, В.А. Сластенин, Н.Ф. Талызина);

– разработки и использования автоматизированных обучающих систем в образовании (С.Г. Данилюк, А.Д. Дараган, В.Л. Латышев, А.А. Павлов, Ю.А. Романенко, В.И. Сердюков и др.);

– исследования проблем информационной, информационно-психологической безопасности (Ю.Д. Бабаева, Л.Н. Бабанин, С.В. Бондаренко, И.В. Бурлаков, В.А. Голубев, Л.О. Пережогин, Т.Л. Тропина, К. Янг и др.);

– аспекты нормативно-правового обеспечения информационной безопасности (В.М. Алексеев, Ю.М. Батулин, Р.И. Дремлюга, Г.О. Крылов, Т.А. Полякова, D.V. Thaw и др.);

– аспекты информационной безопасности как педагогической проблемы (Р.В. Амелин, О.В. Казарин, А.А. Марков, В.Н. Яснев и др.);

– практические аспекты информационной безопасности и защиты информации (В.А. Галатенко, А.П. Даньков, А.А. Круглов, А.В. Крысин, В.В. Мельников, В.В. Минин, Ю.С. Уфимцев и др.).

Методы исследования: анализ, синтез и обобщение теоретических положений, систематизация, структурирование информации, методы педагогического проектирования: структурирование, моделирование, алгоритмизация, апробация и внедрение.

Научная новизна исследования: разработана модель функционирования цифровой среды профессиональной образовательной организации в условиях обеспечения информационной безопасности.

Теоретическая значимость исследования: определены компоненты системы информационной безопасности функционирования цифровой среды профессиональной образовательной организации.

Практическая значимость работы определяется: разработкой методических рекомендаций по совершенствованию системы информационной безопасности функционирования цифровой среды профессиональной образовательной организации.

Апробация и внедрение результатов исследования осуществлялись в процессе педагогической и экспериментальной деятельности в ГБПОУ «Миасский педагогический колледж».

Результаты исследования докладывались и обсуждались на международных научно-практических конференциях: «Международная научно-практическая конференция «Среднее профессиональное образование в информационном обществе» (Челябинск, 2019, 2020).

База исследования: ГБПОУ «Миасский педагогический колледж».

Структура работы. Магистерская диссертация состоит из введения, трех глав, заключения, списка использованной литературы, состоящего из 87 наименований, приложений. Работа содержит 3 рисунка, 6 таблиц, 4 приложений.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ФУНКЦИОНИРОВАНИЯ ЦИФРОВОЙ СРЕДЫ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ В УСЛОВИЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Нормативно-правовые основы организации и функционирования цифровой образовательной среды в условиях обеспечения информационной безопасности

В настоящее время одной из главных целей государственной политики является становление цифрового общества. Для реализации данной цели нормативно-правовая документация сферы образования регулярно претерпевает изменения: вносятся поправки в ранее действующие законы и стандарты, разрабатываются приоритетные проекты, вступают в силу стратегические целевые программы федерального и регионального уровней.

Основой нормативно-правовой базы, нацеленной на становление цифрового образования и общества в Российской Федерации, является Указ Президента РФ от 09.05.2017 №203 «О Стратегии развития информационного общества в РФ на 2017 - 2030 годы». Данная стратегия устанавливает пути и порядок реализации государственной политики в области применения государственными организациями информационных и коммуникационных технологий при предоставлении услуг гражданам страны. Представленный в правовом акте приоритетный сценарий определит развитие информационного общества в России.

К настоящему времени в рамках исполнения указа Президента России №203 выполнены следующие задачи:

1. Министерство образования и науки Российской Федерации обновило правила использования электронного обучения и технологий дистанционного образования в образовательных организациях. А именно установлено, что организации, предоставляющие образовательные услуги, имеют право реализовывать образовательные программы, как в целом, так и их части,

используя только электронное обучение и технологии дистанционного образования.

2. Приняты к исполнению следующие приоритетные проекты в области образования:

– приоритетный проект «Создание современной образовательной среды для школьников», в рамках которого правительство РФ стремится предоставить максимальную доступность обучающимся к качественному общему образованию;

– приоритетный проект «Цифровая школа», нацеленный на обеспечение к 2024 году всех общеобразовательных учреждений современной и безопасной цифровой образовательной средой, гарантирующей достижение необходимого уровня информатизации образования;

– приоритетный проект «Современная цифровая образовательная среда в Российской Федерации», предоставляющий возможность гражданам Российской Федерации получить необходимое им качественное образование с любой точки страны посредством дистанционного онлайн-обучения.

Проблемы информационной безопасности и правовой защиты данных рассматриваются в следующих документах:

1. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646.

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

3. Федеральный закон РФ от 27.07. 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 18.03.2019 г.)

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

5. Федеральный закон Российской Федерации от 28 июля 2012 года № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет».

6. Федеральный закон РФ от 27.07. 2006 г. № 152-ФЗ «О персональных данных» (ред. от 25.07.2011 г.)

7. 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».

8. 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».

Кроме вышеперечисленных документов, нормативно-правовым обоснованием контентной фильтрации следует считать:

– Федеральный закон Российской Федерации от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребёнка в Российской Федерации»;

– ст. 4 Закона Российской Федерации от 27 декабря 1991 № 2124-1 «О средствах массовой информации» (в ред. 06.06.2019 г.);

– ст. 5 Федерального закона Российской Федерации от 13.03.2006 № 38-ФЗ «О рекламе» (с изменениями, внесенными Федеральным законом РФ от 01.05.2019 № 89-ФЗ);

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

– Письмо Роспотребнадзора от 17.09.2008г. № 01/10237-8-32 «О мерах, направленных на нераспространение информации, наносящей вред здоровью, нравственному и духовному развитию детей и подростков».

Рассмотрим содержание основополагающих нормативно-правовых документов обеспечения информационной безопасности.

Одним из таких документов является Доктрина информационной безопасности Российской Федерации (далее – Доктрина).

Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере. В ней определены стратегические цели и основные направления обеспечения информационной безопасности, проанализированы основные информационные угрозы.

Отмечается, что внедрение информационных технологий должно быть тесным образом связано с обеспечением информационной безопасности, иначе существенно повышается вероятность проявления различных информационных угроз. Кроме того, что существует тенденция к росту масштабов компьютерной преступности и широкого использования механизмов информационного воздействия террористическими, экстремистскими организациями и организациями деструктивного характера [1].

В Доктрине информационной безопасности Российской Федерации приведены основные направления обеспечения информационной безопасности в области обороны, государственной и общественной безопасности, в экономической сфере, в области науки, технологий и образования, стратегической стабильности и равноправного стратегического партнерства. В частности, основными направлениями обеспечения информационной безопасности в области науки, технологий и образования являются:

– создание и использование информационных технологий, устойчивых к различным видам воздействия;

- развитие кадрового потенциала в области обеспечения информационной безопасности и применения различных информационных технологий;

- обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

Рассмотрим содержимое Концепции информационной безопасности детей (далее – Концепция). В данной концепции сформулированы основные принципы ИБ детей исходя из понимания необходимости безусловной защиты детей от негативного воздействия информационной продукции и создания информационной среды для положительной социализации и индивидуализации, всестороннего развития личности, сохранения психического и психологического здоровья, формирования позитивного мировоззрения.

Приоритетные задачи семьи, государства и общественных организаций, заинтересованных в обеспечении информационной безопасности детей сформулированы следующим образом:

- формирование навыков самостоятельного и ответственного потребления информационной продукции, повышение уровня медиаграмотности;

- усвоение системы семейных ценностей, развитие системы социальных и межличностных отношений;

- формирование позитивной картины мира и адекватных базисных представлений об окружающем мире и человеке, ценностное, моральное и нравственно-эстетическое развитие детей, воспитание ответственности за свою жизнь и здоровье;

- развитие познавательных потребностей, любознательности, творческих способностей детей; воспитание толерантности, развитие гражданской, этнической и гендерной идентичности, формирование здоровых представлений о сексуальной жизни человека;

– эмоционально-личностное развитие детей.

Кроме того, в Концепции информационной безопасности детей отмечается, что совместные усилия всех участников медиарынка должны быть направлены на минимизацию рисков десоциализации, развития и закрепления девиантного и противоправного поведения детей.

Из возможных вариантов регулирования информационного потребления с целью обеспечения безопасности детей в Российской Федерации выбран вариант сорегулирования медиа и государства. Наряду с запретом информационной продукции, которая может принести вред развитию и здоровью ребенка, необходима организация последовательных и регулярных мероприятий, направленных на повышение уровня медиаграмотности детей, формирование навыков безопасного поведения в современном информационном пространстве [9].

Усилия семьи, общественных организаций и государства должны быть направлены на выработку у детей навыка самостоятельной оценки контента, умение анализировать информацию, противостоять манипулированию, рекламе асоциального поведения и дезинформации.

Рассмотрим некоторые положения Закона РФ «О защите детей от информации, причиняющей вред их здоровью и развитию» и Закона РФ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию», а также отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет» (далее – Закон).

В Законе информационная безопасность детей определяется как состояние защищенности детей, отсутствие риска, связанного с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В статье 5 п 2. перечисляются виды информации, запрещенной для распространения среди детей. Это информация побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в

том числе, самоубийству; способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством; обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным; отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи; оправдывающая противоправное поведение; содержащая нецензурную брань; содержащая информацию порнографического характера.

Пункт 3. той же статьи содержит указание на необходимость органичения таких видов информации: представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия; вызывающая у детей страх, ужас или панику, в том числе информация об унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий; представляемая в виде изображения или описания половых отношений между мужчиной и женщиной; содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Глава 3 содержит требования к обороту информационной продукции, в частности, без знака информационной продукции допускается оборот учебников и учебных пособий, рекомендуемых или допускаемых к использованию в образовательном процессе в соответствии с законодательством Российской Федерации в области образования; телепрограмм, телепередач, транслируемых в эфире без предварительной записи; информационной продукции, распространяемой посредством радиовещания; информационной продукции, демонстрируемой посредством зрелищных мероприятий; периодических печатных изданий,

специализирующихся на распространении информации общественнополитического или производственно-практического характера (статья 11. пункт 4).

Статья 14 «Дополнительные требования к распространению информации посредством информационно-телекоммуникационных сетей» обязывает операторов связи, оказывающих телематические услуги связи в пунктах коллективного доступа, применять технические и программно-аппаратные средства защиты детей от информации, причиняющей вред их здоровью и (или) развитию» [83].

Отдельные аспекты информационной безопасности находят свое отражение в Законе РФ «Об информации, информационных технологиях и о защите информации». Настоящий Закон регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации [54].

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на принципах:

- свободы поиска, получения, передачи, производства и распространения информации любым законным способом;
- открытости информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- установления ограничений доступа к информации только федеральными законами;
- достоверности информации и своевременности ее предоставления;
- равноправия языков народов РФ при создании информационных систем и их эксплуатации;

- обеспечения безопасности РФ при создании информсистем и их эксплуатации и защите, содержащейся в них информации;
- неприкосновенности частной жизни, недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- равноправие языков народов РФ при создании информационных систем и их эксплуатации.

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

- свободно распространяемую;
- предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- которая в соответствии с федеральными законами подлежит предоставлению или распространению,
- распространение которой в РФ ограничивается или запрещается.

Статья 15.1 Закона РФ «Об информации, информационных технологиях и о защите информации» регулирует порядок включения доменных имен, указателей страниц сайтов в сети Интернет, а также сетевых адресов, позволяющих идентифицировать сайты в сети в реестр, содержащих информацию, распространение которой в РФ запрещено [54].

Основание для включения в реестр является распространение посредством сети «Интернет»:

- материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

– информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;

– информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

– информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

– информации, нарушающей требования Федерального закона от 29 декабря 2006 года № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» и Федерального закона от 11 ноября 2003 года № 138-ФЗ «О лотереях» о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети Интернет и иных средств связи;

– информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции, и (или) спиртосодержащей пищевой продукции, и (или) этилового спирта, и (или) спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена законодательством о государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции;

– информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц.

Незамедлительно с момента получения от оператора реестра уведомления о включении доменного имени и (или) указателя страницы сайта в сети «Интернет» в реестр провайдер хостинга обязан проинформировать об этом обслуживаемого им владельца сайта в сети «Интернет» и уведомить его о необходимости удаления интернет-страницы, содержащей информацию, распространение которой в Российской Федерации запрещено.

Незамедлительно с момента получения от провайдера хостинга уведомления о включении доменного имени и (или) указателя страницы сайта в сети Интернет в реестр владелец сайта в сети Интернет обязан удалить интернет-страницу.

В статье 16 Закона РФ «Об информации, информационных технологиях и о защите информации» рассматриваются проблемы защиты информации.

Владелец информации, оператор информационной системы обязан обеспечить защиту информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также, своевременное обнаружение несанкционированного доступа к информации, недопущение воздействия на технические средства обработки информации, возможность мгновенного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

Статья 17. данного Закона содержит информацию об ответственности за правонарушения в сфере информации и защиты информации [54].

Рассмотрим основные положения Закона РФ «О персональных данных».

По типу доступа информационная продукция подразделяется по категориям открытого доступа, в частности, массовая информация, и ограниченного доступа, которая, в свою очередь делится на

конфиденциальную и отнесенную к государственной тайне. Персональные данные о гражданах отнесены Законом к категории конфиденциальных [53].

В соответствии с законодательством РФ информационная система персональных данных (ИСПДн) должна быть классифицирована, разработана Модель угроз безопасности персональным данным при их обработке в ИСПДн, определены границы контролируемой зоны ИСПДн. Кроме того, должно быть разработано положение об организации и проведении работ по обеспечению безопасности ПДн при их обработке в ИСПДн; требования по обеспечению безопасности ПДн при обработке в ИСПДн; должностные инструкции персоналу в части обеспечения безопасности ПДн при их обработке в ИСПДн; инструкции по использованию программных и аппаратных средств защиты информации, образец Уведомления об обработке ПДн.

В организации должен быть разграничен доступ сотрудников к персональным данным, назначен администратор безопасности ИСПДн, утвержден список лиц, которым разрешен доступ к ПДн, обрабатываемым в ИСПДн, для выполнения ими своих служебных обязанностей.

Анализ законодательства РФ и субъектов РФ, подзаконных нормативных правовых актов и документов стратегического планирования в сфере образования позволил выявить наличие следующих организационных барьеров в этой сфере.

Так, в документах стратегического планирования федерального уровня главный организационный барьер – это ориентация на создание и развитие российского цифрового образовательного пространства при незакрепленности конкретных задач, мероприятий, целевых индикаторов и показателей в отношении цифровых технологий в государственной программе «Развитие образования».

В свою очередь на уровне законодательства субъектов РФ обнаруживается сразу несколько организационных барьеров. Во-первых, налицо фрагментарность самой этой законодательной среды. Так, лишь в

некоторых субъектах РФ государственные программы развития образования предусматривают совершенствование цифровой образовательной среды.

Во-вторых, в них нет положений о цифровизации или цифровой трансформации отрасли образования в целом.

В-третьих, не определены конкретные показатели внедрения и применения цифровых технологий.

К правовым барьерам на уровне федерального законодательства об образовании нужно отнести ориентацию на традиционное информационное обеспечение и отсутствие правового регулирования применения прорывных цифровых технологий в сфере образования.

На уровне законодательства субъектов РФ, помимо общей ориентации на традиционную информатизацию (т. е. информационное обеспечение существующих отношений в сфере образования, но без применения прорывных цифровых технологий), барьером является также фрагментарность закрепления элементов механизма правового регулирования применения информационных технологий в целом.

Кроме того, на этом уровне выявлены отсутствие правового регулирования применения цифровых технологий и механизмов оценки их влияния на образование при разработке нормативных правовых актов; фрагментарность правового регулирования проведения экспериментов в сфере образования. На уровне подзаконных нормативных правовых актов РФ и субъектов РФ выявлено значительное число барьеров, которые относятся не собственно к цифровизации, а к информатизации как ее этапу.

Таким образом, в законах РФ затронуты только отдельные аспекты правового регулирования цифровизации образования и обеспечения информационной безопасности, в то время как необходима ее системная нормативная институционализация.

1.2 Целевая модель цифровой образовательной среды

Цифровая образовательная среда (ЦОС) – это цифровое пространство, состоящее из открытой совокупности информационных систем, которые объединяют всех участников образовательного процесса – администрацию, педагогов, обучающихся и их родителей [77].

Основной задачей федерального проекта «Цифровая образовательная среда» проекта является создание современной и безопасной цифровой образовательной среды, обеспечивающей высокое качество и доступность образования всех видов и уровней.

К 2024 году будет обеспечено:

- внедрение целевой модели цифровой образовательной среды по всей стране;
- внедрение современных цифровых технологий в образовательные программы 25% общеобразовательных организаций 75 субъектов Российской Федерации для как минимум 500 тысяч детей;
- обеспечение 100% образовательных организаций в городах Интернетом со скоростью соединения не менее 100 Мб/с, в сельской местности – 50 Мб/с;
- создание сети центров цифрового образования «IT-куб», охватывающей в год не менее 136 тысяч детей.

Общий бюджет федерального проекта составляет более 79,8 млрд. рублей.

Проект позволит обеспечить обновление содержания образования и предоставит возможность обучающимся свободно и безопасно ориентироваться в цифровом пространстве. Цифровая образовательная среда обеспечит повышение квалификации педагогов и оснащение образовательных организаций необходимой инфраструктурой. Будет создана цифровая экосистема, благодаря которой станет возможным переход к автоматизированному делопроизводству, работе с цифровыми

инструментами, использованию широкого спектра современных методик и технологий обучения.

Рассмотрим особенности внедрения Целевой модели цифровой образовательной среды.

В соответствии с методическими рекомендациями по вопросам внедрения Целевой модели цифровой образовательной среды в субъектах Российской Федерации, внедрение целевой модели ЦОС осуществляется в образовательных организациях, осуществляющих деятельность в сфере общего образования, среднего профессионального образования и соответствующего дополнительного профессионального образования, профессионального обучения, дополнительного образования детей и взрослых, воспитания в рамках полномочий Минпросвещения России (далее – образовательные организации), органов исполнительной власти субъектов Российской Федерации, осуществляющих государственное управление в сфере образования, органов местного самоуправления [57].

Внедрение целевой модели ЦОС в субъекте Российской Федерации осуществляется органом исполнительной власти субъекта РФ, осуществляющим государственное управление в сфере образования во взаимодействии с органом исполнительной власти субъекта Российской Федерации, осуществляющим государственное управление в сфере цифрового развития, информатизации, связи и массовых коммуникаций по следующим направлениям:

- создание административно-управленческих и организационно-технических
- условий для внедрения целевой модели ЦОС;
- внедрение и использование федеральной информационно-сервисной платформы цифровой образовательной среды;
- развитие материально-технической базы и информационно-телекоммуникационной и технологической инфраструктуры в образовательных организациях;

– развитие информационных систем и ресурсов (далее - региональные ИСИР), созданных за счет средств бюджета субъектов Российской Федерации в сфере образования, в том числе обеспечение их взаимодействия с информационными системами и ресурсами платформы ЦОС.

Цифровая образовательная среда (ЦОС) образовательной организации включает:

- комплекс информационных образовательных ресурсов, в том числе цифровые образовательные ресурсы;
- совокупность технологических средств информационных и коммуникационных технологий: компьютеры, иное ИКТ оборудование, коммуникационные каналы;
- систему современных педагогических технологий, обеспечивающих обучение в современной ЦОС [29].

Подсистемы современной цифровой образовательной среды представлены на рисунке 1.



Рисунок 1 – Подсистемы цифровой образовательной среды

Цифровая информационно-образовательная среда образовательной организации должна обеспечивать:

- информационно-методическую поддержку образовательного процесса;

- планирование образовательного процесса и его ресурсного обеспечения;
- мониторинг и фиксацию хода и результатов образовательного процесса;
- мониторинг здоровья обучающихся;
- современные процедуры создания, поиска, сбора, анализа, обработки, хранения и представления информации;
- дистанционное взаимодействие всех участников образовательного процесса (обучающихся, их родителей (законных представителей), педагогических работников, органов управления в сфере образования, общественности), в том числе, в рамках дистанционного образования;
- дистанционное взаимодействие образовательного учреждения с другими организациями социальной сферы: учреждениями дополнительного образования детей, учреждениями культуры, здравоохранения, спорта, досуга, службами занятости населения, обеспечения безопасности жизнедеятельности.

ЦОС образовательной организации обеспечивает возможность осуществления в электронной (цифровой) форме следующих видов деятельности:

- планировать образовательный процесс;
- размещать и сохранять материалы образовательного процесса, в том числе работ обучающихся и педагогов, используемых участниками образовательного процесса информационных ресурсов;
- фиксировать ход образовательного процесса и результатов освоения основной образовательной программы;
- использовать данные, формируемые в ходе образовательного процесса, для решения задач управления образовательной деятельностью;

- взаимодействовать между участниками образовательного процесса, в том числе дистанционно посредством сети Интернет;
- контролировать доступ участников образовательного процесса к информационным образовательным ресурсам в сети Интернет (ограничение доступа к информации, несовместимой с задачами духовно-нравственного развития и воспитания обучающихся);
- осуществлять взаимодействие образовательного учреждения с органами, отвечающими за управление в сфере образования, и с другими образовательными учреждениями, организациями [38].

Цели формирования и использования ЦОС отражают интересы учителя, обучаемого, а также родителей и предусматривают следующее.

Для обучающегося:

- расширение возможностей построения собственной образовательной траектории;
- доступ к самым новым образовательным ресурсам;
- растворение рамок образовательных организаций до масштабов всего мира.

Для родителя:

- расширение образовательных возможностей для ребенка;
- снижение затрат, вызванное усилением конкуренции на рынке образовательных услуг;
- увеличение прозрачности образовательного процесса;
- облегчение общения со всеми участниками образовательного процесса;
- сокращение бюрократической нагрузки за счет автоматизации;
- повышение удобства мониторинга образовательного процесса;
- формирование новых условий мотивации учащихся при создании и выполнении заданий, организация условий для выработки индивидуальной образовательной траектории учащегося.

Для педагога:

- снижение бюрократической нагрузки за счет автоматизации;
- повышение удобства мониторинга образовательного процесса;
- формирование новых условий мотивации учащихся при создании и выполнении заданий, организация условий для выработки индивидуальной образовательной траектории обучающегося.

При этом открытая цифровая образовательная среда, формирует умения конкурировать в цифровом пространстве, сотрудничать, взаимообучать, давать объективную оценку и вносить коррективы с учетом возможностей обучающихся.

Критериями успешного внедрения ЦОС являются

- сокращение бюрократического аппарата;
- снижение интенсивности документооборота, созданного руками сотрудников образовательных организаций;
- рост трафика добровольного использования ЦОС, прежде всего обучающимися [43].

Таким образом, цифровая образовательная среда образовательной организации представляет собой управляемую и динамично развивающуюся с учетом современных тенденций модернизации образовательную систему эффективного и комфортного предоставления информационных и коммуникационных услуг, цифровых инструментов объектам процесса обучения.

1.3 Характеристика цифровой образовательной среды профессиональной образовательной организации в условиях обеспечения информационной безопасности

Программа «Цифровая экономика Российской Федерации», утвержденная распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р, выдвигает новые требования к системе

профессионального образования. Цифровизация экономики сопровождается и цифровизацией профессионального образования, призванных обеспечивать все отрасли экономики и социальной сферы высококвалифицированными кадрами.

Вслед за принятием термина «цифровая экономика» в широкий оборот вводятся и другие термины, в том числе «цифровое образование», «цифровая образовательная среда», «цифровые образовательные технологии» и др.

В работах К.Г. Кязимова под цифровизацией профессионального образования и обучения понимается «применение инновационных образовательных технологий, построенных на алгоритмах, при реализации которых обеспечивается высокая эффективность образовательного процесса с применением современного программного обеспечения» [44].

В отечественной педагогической науке и практике ещё нет чёткого толкования новых терминов, связанных с развитием цифрового образования. Анализируя мнения разных авторов относительно содержания терминов «цифровое образование», можно сформулировать определение понятия «цифровое образование». Цифровое образование – процесс организации взаимодействия между преподавателями и обучающимися при движении от цели к результату в цифровой образовательной среде, основными средствами данной среды являются цифровые технологии, цифровые инструменты как результаты учебной деятельности в цифровом формате.

Как отмечалось выше, термин «цифровое образование» можно заменить другим научным термином: «цифровые технологии в образовании». Основными компонентами цифровых технологий в профессиональном образовании являются: ЦОС, цифровые процессы организации учебного процесса, цифровые технологии проверки знаний, навыков, умений, профессиональных общекультурных компетенций учащихся и студентов.

Рассмотрим более подробно один из компонентов цифровых технологий в профессиональном образовании – ЦОС.

Цифровая образовательная среда – это совокупность педагогических, психологических, материально-технических и организационных условий, целенаправленно созданных в профессиональной образовательной организации на единых ценностно-целевых основаниях и обеспечивающих инновационность учебно-воспитательного процесса [3].

Иными словами, ЦОС – это совокупность условий, обеспечивающих информационное взаимодействие между преподавателями, обучающимися и студентами, и информационными ресурсами, и функционирование структур управления учебно-воспитательным процессом.

В современной педагогике образовательная среда трактуется как часть социокультурного пространства, зона взаимодействия образовательных систем, их элементов, образовательных материалов и субъектов образовательного процесса. Цифровая образовательная среда обеспечивает новые возможности для:

- перехода от обучения в конкретной аудитории к обучению, которое осуществляется в разных местах и в разное время;
- проектирования индивидуального образовательного маршрута, удовлетворения образовательных потребностей личности учащихся и студентов.

Цифровая электронная образовательная среда профессиональной образовательной организации (ПОО) – это открытая совокупность информационных систем, предназначенных для обеспечения основных задач учебно-воспитательного процесса.

Слово «открытая» означает возможность и право пользователей использовать разные информационные системы в составе цифровой образовательной среды, заменять их или добавлять новые. Можно утверждать, что ЦОС ПОО – это управляемая и динамично развивающаяся система эффективного предоставления информационных и коммуникационных услуг, цифровых инструментов профессионального образования.

Согласно требованиям ФГОС среднего профессионального образования для реализации образовательных программ ЦОС должна включать в себя следующие условия:

- эффективное управление организациями профессионального образования с использованием цифровых инструментов и механизмов финансирования;
- учебные кабинеты, лаборатории, мастерские, оснащенные необходимым оборудованием;
- библиотеки, оборудованные читальными залами и книгохранилищами;
- обеспечение доступа в библиотеке к информационным ресурсам сети Интернет, учебной литературе, коллекциям медиа -ресурсов на электронных носителях;
- размещение продуктов учебной и проектной деятельности студентов и учащихся;
- планирование учебного процесса, фиксирование его реализации и отдельных этапов (лекций, презентаций, вебинаров, дискуссий, выступлений);
- планирование учебного процесса, фиксацию его итоговых результатов.

В концепции целевой программы развития образования до 2020 года указывается, что необходимость применения информационно-коммуникационных технологий, создание целостной электронной образовательной среды, является одним решающих факторов повышения качества профессионального образования, а значит, и конкурентоспособности выпускников ПОО [19].

Для успешного применения цифровых технологий в цифровой образовательной среде необходимо:

1. Прежде всего, с участием работодателей повышать качество подготовки выпускников ПОО, создавать основу для их дальнейшей профессионального развития, применять в учебном процессе цифровые образовательные технологии.

Формирование профессиональной компетентности молодых специалистов должно осуществляться совместными усилиями ПОО и работодателей в два этапа. На первом этапе обучение в вузах, колледжах и техникумах является начальной стадией формирования у выпускников профессиональной компетентности. На этом этапе происходит освоение студентами знаний, умений, навыков, ценностей, цифровых технологий, учебных и производственных практик, общекультурных и профессиональных компетенций, гуманитарное развитие. На втором этапе – успешное трудоустройство выпускников по полученной профессии, адаптация и наставничество в организациях, приобретение творческого опыта трудовой деятельности, периодическое повышение квалификации.

2. Повышение ответственности работодателей за воспроизводство квалифицированных кадров через систему профессионального образования и внутрифирменного обучения персонала, установление связей ПОО с предприятиями, структурами – разработчиками ИКТ, применяющими цифровые технологии на практике.

3. Создание в ПОО и в системе внутрифирменного обучения персонала учебной ЦОС, применение в такой среде инновационных образовательных электронных технологий и пособий. Данная цифровая образовательная среда может создавать благоприятные условия для разработки и использования печатных и электронных учебников, учебных пособий и презентаций, повышать активность как преподавателей, так и студентов.

Создание ЦОС является необходимым, но не достаточным условием, так как важна и организация практических занятий по формированию у

обучающихся и студентов профессиональных и общекультурных компетенций.

4. Внедрение в учебный процесс цифровых технологий обуславливает необходимость материально-технического оснащения профессиональной образовательной организации и других организаций, создания в них цифровой библиотеки, учебных лабораторий и подразделений с постоянно обновляемой материально-технической базой, а по техническим профессиям – соответствующих производственных лабораторий и мастерских. Как показывает практика, использование цифровой библиотеки, обеспечивает оперативный доступ студентов и преподавателей организаций к учебной и научной литературе независимо от места нахождения и времени суток.

5. ППО должны готовить выпускников, способных создавать инновации, действовать в условиях неопределенности и недостатка ресурсов, достигать успехов, где многие процессы под действием цифровизации будут передаваться роботам и машинам, и сопровождаться высвобождением работников. Такие новые вызовы обуславливают необходимость фундаментальной подготовки специалистов широкого профиля, способных к смене сферы трудовой деятельности и быстрому переориентированию.

6. Требуется постоянный профессиональный рост педагогов, которые в цифровой образовательной среде могут избавляться от рутины и больше времени уделять творческому труду и проектной деятельности.

Создание ЦОС и применение цифровых технологий обучения является эффективным, как для студентов и обучающихся, так и для преподавателей.

Успешное функционирование ЦОС помогает студентам:

- использовать учебные объекты с сочетанием различных способов: с помощью текста, видео, графиков, фото, звука и анимации;
- доступ к разнообразным печатным и электронным образовательным ресурсам;

- проектировать индивидуальный образовательный маршрут, удовлетворять образовательные потребности личности учащихся и студентов.

Преподавателям:

- использовать современные цифровые образовательные технологии;
- применять различные печатные и электронные образовательные ресурсы;
- представлять учебные объекты, сочетающие в себе различные способы представления информации (текст, графики, фото, видео, звук и анимация);
- устранять бюрократические нагрузки за счет ее автоматизации;
- снижать нагрузки по контролю выполнения заданий студентам и учащимся за счет автоматизации;
- улучшать возможности и удобства организации и мониторинга образовательного процесса;
- стимулировать и мотивировать студентов и обучающихся при освоении учебного материала и выполнении заданий;
- превращать студентов из пассивных объектов в активных субъектов учебного процесса.

В процессе организации цифровой образовательной среды ПОО может возникать ряд рисков [29].

Риск 1. Недостаточное финансирование и/или увеличение финансовой нагрузки на ПОО. Подключение образовательных организаций к высокоскоростному Интернету, повышение квалификации педагогических работников по вопросам внедрения цифровых технологий в образовательный процесс, закупка оборудования финансируются из федерального и регионального бюджета. Кроме того, использование электронных библиотек в учебном процессе может снизить затраты на закупку учебно-методической литературы.

Риск 2. Недостаточное кадровое обеспечение на начальном этапе становления цифровой образовательной среды. Эффективность образования всегда зависела от уровня подготовки педагога. Сегодня преподаватель по-прежнему остаётся ведущим звеном всего процесса обучения, однако интеграция информационных технологий и образования способствует формированию новой роли педагога. Повышение квалификации педагогических работников, осуществляющих образовательную деятельность, является одной из задач регионального проекта «Цифровая образовательная среда» и позволит обеспечить актуализацию знаний, умений и навыков ведущего кадрового состава системы образования в части внедрения и использования современных цифровых технологий в образовании. Тем не менее, необходимым является введение должности «Заместитель директора по ИКТ» и/или организация наставничества по вопросам цифровизации.

Риск 3. Незавершенность цифровой дидактики. Является наиболее реальным риском. Относительная инертность педагогики как науки идет вразрез с быстрым, молниеносным внедрением цифровых технологий.

Риск 4. Технические неполадки, сбои, происходящие в техногенной среде.

Риск 6. Замена живого общения уроками в режиме онлайн отрицательно скажется на качестве образования.

Риск 7. Риск подмены цифровизации образования оцифровкой. Для педагогически неэффективной «оцифрованной» дидактической практики характерны, в том или ином сочетании, следующие особенности:

- использование информационно-коммуникационных технологий, не сфокусированных на решение конкретных педагогических задач;
- использование в оцифрованном виде традиционных дидактических элементов образовательного процесса (содержания, форм, методов, приемов обучения, прежней системы оценивания и контроля знаний) без какой-либо принципиальной их трансформации.

Риск 8. Обеспечение информационной безопасности цифровой образовательной среды.

Рассмотрим данный риск более подробно.

Информационная безопасность выражается в защищенности, гарантии сохранности состояния человека, общества, ресурсов, условий и т.д., то есть, среды, в которой живёт, действует и развивается личность. Иными словами, информационная безопасность – понятие многоаспектное, включающее:

1. Безопасность человека как основного носителя, производителя и потребителя информации (безопасность его внутренней и внешней среды).
2. Безопасность информационных процессов и процессов информатизации.
3. Безопасность состояния, содержания и формы информационных ресурсов, систем, объектов информационной среды.
4. Безопасность сохранения информации, защищенность от внешних негативных воздействий, защищенность среды в аспекте информационного взаимодействия.

Зарубежный и отечественный опыт позволяет определить следующие угрозы информационной безопасности, которые стоят перед образовательными организациями [51]:

1. Фильтрация нежелательной информации. Данная группа угроз напрямую связана с противодействием экстремистской идеологии, но не ограничивается только ей. При рассмотрении угроз доступа к нежелательной информации следует также учитывать вопросы распространения провокационных материалов, порнографии, пропаганды наркотиков и алкоголя, и т.п.
2. Несанкционированный доступ к данным. Эта группа угроз включает в себя искажение данных в электронных журналах, архивах, хищение информации экзаменационных билетов, личных данных студентов и их родственников и т.п. Анализируя рекомендации по организации схем

обеспечения информационной безопасности, можно сделать вывод о том, что специалисты ограничиваются только технической сферой.

3. Проблемы регулирования использования социальных сетей. Именно в этой зоне осуществляется активное давление на обучающихся, запугивание, а также относительно новый феномен киберхулиганства.

4. Кибертерроризм. Эта группа угроз находится в ведении соответствующих силовых ведомств, однако она частично может решаться и на уровне образовательных организаций. Создание безопасной цифровой образовательной среды серьезно осложняет возможные кибератаки на объекты образования, которые могут привести к нарушению функционирования управляющих автоматических систем и последующему повреждению инфраструктуры. Следует отметить, что данная группа угроз остается пока во многом гипотетической, так как учебные заведения в силу низкой их насыщенности автоматизированными управляющими системами не рассматриваются в качестве приоритетных целей для кибератак.

В процессе создания и функционирования ЦОС возникает поле технических угроз. Современные образовательные организации широко используют в своей деятельности информационные технологии для ведения журналов, контроля успеваемости, административно-хозяйственной деятельности и т.д. Однако, информационные системы, которые используются в профессиональной образовательной организации, в большинстве своем, не отвечают даже минимальным требованиям обеспечения безопасности. Данные информационные системы зачастую не проходят какой-либо сертификации, стандартизации, создаются низкоквалифицированными разработчиками, очень часто на основе устаревших решений.

Перечисляя проблемы, характерные для таких информационных систем, можно отметить:

1. Использование разнородных, устаревших и заведомо небезопасных платформ. Уязвимости в информационных системах, базах данных и

других информационных средствах выявляются регулярно, и любая устаревшая платформа должна считаться заведомо небезопасной, если не проведены работы по устранению этих проблем. Во многих случаях информационные системы не связаны между собой, используют разные платформы, что резко осложняет их использование и поддержку.

2. Отсутствие стандартизации. Несмотря на предпринятые попытки разработать унифицированные информационно-технические решения, большинство учебных заведений используют те решения, которые оказались под рукой.
3. Использование публичного открытого соединения. Любая информационная система для обеспечения безопасности должна организовывать передачу данных с использованием зашифрованных соединений по умолчанию во избежание перехвата данных.
4. Отсутствие практики регулярной проверки безопасности. Без постоянного аудита и выявления потенциальных проблем даже качественно спроектированные информационные системы могут стать небезопасными при появлении новых видов уязвимостей.
5. Использование пиратского программного обеспечения. Многие образцы «взломанных» программ могут содержать в себе троянский код, упрощающий внедрение в информационные системы. Кроме того, пиратское программное обеспечение часто исключает возможность его обновления, что не позволяет противостоять вновь возникающим угрозам.
6. Низкая квалификация обслуживающего персонала или отсутствие должности специалиста по поддержке информационных систем в принципе. Качественная поддержка информационных систем требует регулярного мониторинга их работы и устранения неполадок.
7. Недофинансирование. Данная проблема является основополагающей, так как решению всех описанных проблем можно подходить на

различных уровнях. Наилучшим вариантом могла бы стать разработка единой платформы для всех образовательных организаций среднего профессионального образования и ее централизованная удаленная поддержка высококвалифицированными специалистами, которые обладают необходимыми знаниями в области обеспечения безопасности информационных систем. Однако такой вариант возможен только в дальней перспективе, в реальности же все возникающие проблемы учебные заведения вынуждены решать самостоятельно [61].

Таким образом, создание и функционирование цифровой образовательной среды профессиональной образовательной организации должно соответствовать всем требованиям информационной безопасности. Именно тогда, она позволит обеспечить модернизацию образовательного процесса, внедрить в педагогическую практику технологии электронного обучения, модели смешанного обучения, автоматизирует процессы управления качеством образования, формирование у студентов навыков обучения в цифровом мире, умению создавать цифровые проекты для своей профессии, присутствие в образовательной организации в сети Интернет.

Выводы по главе 1

В настоящее время приняты к исполнению приоритетные проекты в области образования:

– приоритетный проект «Создание современной образовательной среды для школьников», в рамках которого правительство РФ стремится предоставить максимальную доступность обучающимся к качественному общему образованию;

– приоритетный проект «Цифровая школа», нацеленный на обеспечение к 2024 году всех общеобразовательных учреждений современной и безопасной цифровой образовательной средой, гарантирующей достижение необходимого уровня информатизации образования;

– приоритетный проект «Современная цифровая образовательная среда в Российской Федерации», предоставляющий возможность гражданам Российской Федерации получить необходимое им качественное образование с любой точки страны посредством дистанционного онлайн-обучения.

Реализация данных проектов предполагает создание цифровой образовательной среды в образовательных организациях.

Цифровая среда профессиональной образовательной организации – это открытая совокупность информационных систем, предназначенных для обеспечения основных задач учебно-воспитательного процесса.

Создание ЦОС и применение цифровых технологий обучения является эффективным, как для студентов и обучающихся, так и для преподавателей. Однако в процессе организации и функционирования ЦОС могут возникать различные риски, одним из которых является обеспечение информационной безопасности данной среды.

Информационная безопасность выражается в защищенности, гарантии сохранности состояния человека, общества, ресурсов, условий и т.д., одним словом, среды, в которой живёт, действует и развивается личность.

Современные образовательные организации широко используют в своей деятельности информационные технологии для ведения журналов, контроля успеваемости, административно-хозяйственной деятельности и т.п. К сожалению, информационные системы, используемые в ПОО, в большинстве своем, не отвечают даже минимальным требованиям, предъявляемым к безопасным системам. Подавляющее большинство информационных систем не проходят какой-либо сертификации, стандартизации, создаются низко квалифицированными разработчиками, очень часто на основе устаревших решений.

Именно поэтому становится актуальной разработка методических рекомендаций по совершенствованию системы обеспечения информационной безопасности в условиях функционирования цифровой образовательной среды.

ГЛАВА 2. АНАЛИЗ ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ГБПОУ «МИАССКИЙ ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ» В УСЛОВИЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1 Анализ модели цифровой образовательной среды ГБПОУ «Миасский педагогический колледж»

Изучив нормативно-правовые основы организации и функционирования цифровой образовательной среды в условиях обеспечения информационной безопасности, рассмотрев особенности внедрения Целевой модели цифровой образовательной среды, а также описав характеристику цифровой образовательной среды профессиональной образовательной организации в условиях обеспечения информационной безопасности, необходимо рассмотреть особенности функционирования цифровой среды в условиях обеспечения информационной безопасности конкретной профессиональной образовательной организации. Примером для рассмотрения, изучения и анализа опыта организации и функционирования ЦОС является ГБПОУ «Миасский педагогический колледж».

Исходя из экономической целесообразности, а также во исполнение указа президента РФ «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» от 7 мая 2018 г. № 204, можно сделать вывод о том, что в основу функционирования цифровой среды профессиональной образовательной организации следует положить работу со свободно-распространяемым и отечественным программным обеспечением. На основе требований федеральных государственных образовательных стандартов СПО и учета специфики работы профессиональных образовательных организаций рассмотрим основные компоненты ЦОС, которые представлены в таблице 1.

Таблица 1 – Основные компоненты цифровой образовательной среды

№ п/п	Основные компоненты	Удовлетворение требованиям ФГОС
1.	Официальный сайт колледжа	Обеспечивает информационно-методическую поддержку образовательного процесса.
2.	Электронная почта	Обеспечивает информационно-методическую поддержку образовательного процесса.
3.	Электронный журнал	Обеспечивает планирование образовательного процесса и его ресурсного обеспечения, мониторинг и фиксацию хода и результатов образовательного процесса.
4.	Электронный календарь	Обеспечивает планирование образовательного процесса и его ресурсного обеспечения.
5.	Система электронного документооборота	Обеспечивает современные процедуры создания, поиска, сбора, анализа, обработки, хранения и представления информации.
5.	Система дистанционного обучения для студентов	Обеспечивает дистанционное взаимодействие всех участников образовательного процесса (обучающихся, их родителей (законных представителей), педагогических работников, органов управления в сфере образования, общественности), в том числе, в рамках дистанционного образования.
6.	Корпоративный портал	Обеспечивает формирование ИКТ-компетенции педагогов образовательной организации.
7.	Система поддержки пользователей компьютерной техники	Обеспечивает условия для практического применения компьютерной техники участниками образовательного процесса.

Проанализировав цифровую образовательную среду ГБПОУ «Миасский педагогический колледж», можно сделать вывод о том, что она включает лишь некоторые компоненты ЦОС, такие как:

- официальный сайт колледжа (<http://miasspk.ru/>);
- электронная почта (не является корпоративной);
- электронный журнал (Сетевой город «Электронный журнал»
Модуль ПОО: <https://poo.edu-74.ru/>);
- электронный календарь.

Таким образом, в период дистанционного обучения, приходилось привлекать различные ресурсы для упрощения электронного документа оборота, организации дистанционного обучения и поддержки пользователей компьютерной техники.

Из вышесказанного следует, что ЦОС ГБПОУ «Миасский педагогический колледж» позволяет осуществлять в электронной (цифровой) форме следующие лишь следующие виды деятельности:

- информационно-методическую поддержку образовательного процесса;
- планирование образовательного процесса и его ресурсного обеспечения;
- мониторинг и фиксацию хода и результатов образовательного процесса.

Тогда как основные виды деятельности, такие как:

- современные процедуры создания, поиска, сбора, анализа, обработки, хранения и представления информации;
- дистанционное взаимодействие всех участников образовательного процесса (обучающихся, их родителей/законных представителей, педагогических работников, органов управления в сфере образования, общественности), в том числе в рамках дистанционного образования;
- дистанционное взаимодействие образовательного учреждения с другими организациями социальной сферы: учреждениями дополнительного образования детей, учреждениями культуры, здравоохранения, спорта, досуга, службами занятости населения, обеспечения безопасности жизнедеятельности

требуют привлечения дополнительных ресурсов, которые не относятся к образовательным и располагаются на удаленных серверах, например, использование социальной сети ВКонтакте для взаимодействия между всеми участниками образовательного процесса, конференции Zoom для организации видеоконференций со студентами и педагогами, GoogleClass для создания курсов, а также назначения и проверки заданий и др.

Таким образом, цифровая образовательная среда ГБПОУ «Миасский педагогический колледж» требует внедрения всех компонентов ЦОС, а также использование свободно-распространяемого и отечественного программного обеспечения.

2.2 Анализ цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» по реализации мер информационной безопасности

Анализ цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» по реализации мер информационной безопасности был осуществлен в несколько этапов:

1) Анализ системы защиты информационной системы колледжа в целом.

2) Анализ системы обеспечения информационной безопасности студентов.

3) Анализ осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в цифровой образовательной среде.

Для анализа системы защиты информационной системы было проведен анализ реализованных мер комплексной защиты колледжа с перечнем мер, предложенных «Лабораторией Касперского» для реализации комплексной программно-технической системы защиты информационных систем компаний и организаций. Проведенный анализ (таблица 2) позволяет сделать следующие выводы:

1. Из 17 мер по защите информационных систем в полном объеме реализована лишь часть; 6 – реализовано частично, а 5 мер – в системе защиты не реализованы.

2. Отсутствует политики и меры безопасности для «мобильных» устройств и ноутбуков, а использование таких гаджетов сотрудниками ежегодно растет.

3. Шифрование дисков, внешних устройств, используемых сотрудниками реализовано частично или не реализовано совсем.

Таблица 2 – Анализ системы защиты информационной системы колледжа

№	Наименование элемента защиты информационной системы (Перечень «Лаборатории Касперского»)	Реализация в колледже
1	Защита от вредоносного ПО	Реализовано в полном объеме
2	Управление обновлением ПО	Реализовано в полном объеме
3	Разграничение доступа к ИТ ресурсам	Реализовано в полном объеме
4	Сетевая структура (выделение критически важных подсетей)	Реализовано в полном объеме
5	Контроль использования внешних устройств	Реализовано в частичном объеме
6	Специальная политика безопасности для внешних устройств	Реализовано в частичном объеме
7	Специальная политика безопасности для съемных носителей	Реализовано в частичном объеме
8	Шифрование переписки	Реализовано в полном объеме
9	Шифрование файлов и папок	Реализовано в полном объеме
10	Контроль программ	Реализовано в полном объеме
11	Антивирусное ПО для мобильных устройств	Отсутствует
12	Специальная политика безопасности для ноутбуков	Отсутствует
13	Полное шифрование диска	Реализовано в частичном объеме (сервер ИС, СУБД)
14	Шифрование данных на съемных носителях	Отсутствует
15	Аудит ИТ безопасности независимыми компаниями	Реализовано в частичном объеме (проверки ФАПСИ по реализации защиты конфиденциальной информации о обучающихся)
16	Специальная политика безопасности для смартфонов / планшетов	Отсутствует
17	Системы управления мобильными устройствами	Отсутствует

Поскольку в ГБПОУ «Миасский педагогический колледж» на 1-2 курсах обучаются лица, не достигшие возраста 18 лет, необходимо провести анализ системы обеспечения информационной безопасности студентов. На основании данного анализа построена модель комплексной информационной безопасности студентов, представленная на рисунке 2.



Рисунок 2 – Модель обеспечения информационной безопасности студентов

Целью и результатом реализации данной модели является формирование информационно-безопасной личности выпускника. Объектом информационной безопасности является личная информационная среда студента.

На рисунке 2 представлены внутренние и внешние угрозы информационной безопасности несовершеннолетних студентов –

совокупность факторов и условий, возникающих в процессе взаимодействия объекта безопасности с другими объектами (субъектами). Информационные опасности современных школьников – негативное проявление перехода к информационному обществу, формирующееся под воздействием вышеуказанных информационных угроз и рисков, которым современный обучающийся должен уметь противостоять, организовывая свою образовательную деятельность и др.

Не менее важным вопросом является определение субъектов информационной безопасности, то есть тех, кто влияет на информационную безопасность студентов и несет ответственность за ее обеспечение. В данной модели определены следующие субъекты: государство, общество, открытые информационные ресурсы (СМИ, Интернет), родители, близкие и родные, сверстники и педагоги. Данные субъекты могут быть источниками как внешних, так и внутренних угроз.

Рассматривая внешние и внутренние угрозы более подробно. Необходимо отметить, что на личность несовершеннолетнего в современном информационном обществе воздействует мощный информационный поток, представленный в виде всей информации, которую он получает. И если информация, предлагаемая родными и педагогами чаще является трансформированной под возрастные и психофизиологические особенности обучающегося, то информация получаемая несовершеннолетними студентами из внешней среды (телевидение, интернет, печатная пресса, фото и видео, информационные службы) предлагается им в первоначальном виде, и может негативно влиять на него в большей или меньшей степени в зависимости от личностных характеристик. Наиболее явные внешние и внутренние угрозы представлены на рисунке 2.

Обеспечение информационной безопасности несовершеннолетних студентов представлено: правовым обеспечением информационной безопасности, нравственным и этическим контролем, защитой психики и здоровья, техническим и программным обеспечением ИБ, воспитательными

и организационными мерами по обеспечению ИБ, формированием информационной культуры учащихся, образованием в области информационной безопасности.

Данные мероприятия реализуются полностью или частично в ГБПОУ «Миасский педагогический колледж». Рассмотрим их более подробно.

1. Правовое обеспечение информационной безопасности – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту личной информационной среды несовершеннолетнего на законодательной и правовой основе для реализации единой государственной политики в сфере защиты детей от информации, причиняющей вред их здоровью и развитию. Данные мероприятия реализуются в полном объеме. На сайте колледжа в разделе «Информационная безопасность» представлены актуальные нормативные документы, доступные для просмотра и скачивания:

- Письмо Минобрнауки России от 14.05.2018 № 08-1184 «О направлении информации» вместе с «Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении использовании сети «Интернет»).
- Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.07.2018) «О защите детей от информации, причиняющей вред их здоровью и развитию».
- Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

- Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) «О персональных данных»

2. Нравственный и этический контроль подразумевает соблюдение обучающимися при осуществлении информационной деятельности норм и правил поведения в обществе, а также сетевой культуры и этики, которые складываются по мере распространения информационных технологий в современном информационном обществе.

3. Защита психики и здоровья несовершеннолетнего – меры направлены на актуализацию потребности студентов в хорошем здоровье, физическом благополучии, как средств достижения жизненно важных ценностей, снижение и профилактика компьютерной и Интернет-зависимости среди обучающихся, педагогическая и психологическая помощь в вопросах уменьшения информационных опасностей в жизнедеятельности.

Мероприятия по осуществлению нравственного и эстетического контроля, а также по защите психики и здоровья несовершеннолетнего реализуется частично, так на сайте колледжа во вкладке «Информационная безопасность» в разделе «Студентам» располагаются:

- Методические рекомендации по ограничению в образовательной организации доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования
- Памятка для обучающихся об информационной безопасности детей.

С данными документами могут ознакомиться все желающие, однако не проводятся мероприятия, направленные на акцентирование внимание на них, а также не организуется работа по профилактике компьютерной и Интернет-зависимости среди обучающихся.

4. Воспитательные меры по обеспечению ИБ – меры направленные на формирование культуры безопасности, ответственности за производимые

действия в информационном пространстве, меры воспитания и укрепления духовно-нравственных ценностей, патриотизма. Данная деятельность реализуется частично, поскольку план воспитательной работы на год включает лишь два общеколледжных мероприятия, направленных на формирование культуры безопасности и т. д.

5. Техническое и программное обеспечение ИБ – это использование различных технических и программных средств, препятствующих нанесению материального или морального ущерба личной информации, программы родительского контроля, технические средств защиты информации.

На всех компьютерах колледжа с присвоением разных профилей фильтрации установлен контент-фильтр SkyDNS. SkyDNS – это программный продукт, позволяющий осуществлять высокоскоростную фильтрацию трафика в сети Интернет без ограничений по объему и полосе пропускания трафика. Контент-фильтр позволяет управлять доступом к онлайн-ресурсам, избавляет от ненужной и вредной информации в Сети. Реализация возможностей SkyDNS в ГБПОУ «Миасский педагогический колледж» представлена в таблице 3.

Таблица 3 – Реализация возможностей контент-фильтрации SkyDNS

Контентная фильтрация	Реализация в колледже
Реализация основных возможностей	
Стандартный DNS-фильтр	Реализовано (собственная база, включающая более 9 млн. доменов, распределенных на 58 категорий)
Фильтрация протоколов сайтов	Реализовано (HTTP и HTTPS)
Наличие черного и белого списков	Реализовано (более 200 записей)
Режим работы только по белому списку	да
Явная блокировка сайтов, запрещенных законодательством РФ (экстремизм и т.д.)	Реализовано (фильтрация по спискам Министерства юстиции РФ, единому реестру запрещенных на территории РФ сайтов).
Безопасный поиск с защитой от экстремизма, порнографии, наркотиков и другой запрещенной законодательством РФ информации	Реализовано (встроенный поиск с принудительным перенаправлением с других поисковых систем)
Блокировка неизвестных контент-фильтру сайтов	да
Фильтрация графических баннеров, всплывающих окон и контекстной рекламы	да

Продолжение таблицы 3

Контентная фильтрация	Реализация в колледже
Реализация основных возможностей	
Присвоение разных профилей фильтрации для разных компьютеров	да
Присвоение разных профилей фильтрации разным пользователям в рамках одного компьютера	да
Обеспечение безопасности	
Блокировка анонимайзеров и прокси	да
Блокировка фишинговых и вирусных сайтов	да
Защита от ботнет сетей	да
Уведомление администратора о зараженных компьютерах, попавших в ботнет	Реализовано (по электронной почте с блокировкой доступа зараженных компьютеров к управляющему серверу ботнета)

Из данных таблицы 3 видно, что в колледже используются программные продукты российской компании СкайДНС для обеспечения контентной фильтрации интернета и безопасности пользователей от таких угроз как ботнет-сети, фишинговые, мошеннические и вредоносные интернет-ресурсы. Данные мероприятия реализуются в полном объеме.

6. Образование в области информационной безопасности – реализация образовательных модулей в курсе общеобразовательных и общепрофессиональных дисциплин (ОБЖ, безопасность жизнедеятельности и др.), организация дополнительного образования обучающихся по информационной безопасности, повышение квалификации педагогического состава, проведение тематических родительских собраний и встреч с интересными людьми.

Работа в данном направлении осуществляется частично, так, например, в курсы ОБЖ и безопасность жизнедеятельности включены разделы, посвящённые информационной и кибербезопасности. Однако несмотря на то, что на базе колледжа реализуются программы дополнительного образования различной направленности, отсутствуют программы по кибербезопасности и кибергигиене. Кроме того, не осуществляется повышение квалификации

педагогического коллектива по данному направлению и проведение тематических родительских собраний и встреч с интересными людьми.

7. Формирование информационной культуры студентов – через образовательную и воспитательную среду колледжа, которая определяется как компонент базовой культуры личности и характеристики человека, позволяющей ему эффективно выполнять все виды работы с информацией, понимать природу информационных процессов и осуществлять информационную рефлексию без ущерба для себя и окружающих. Данные мероприятия реализуются частично, в колледже имеется стенд «Информационная культура на современном этапе развития общества», на различных образовательных дисциплинах делается акцент на вопросы, связанные с особенностями пребывания в информационном обществе, организуется внеклассная работа. Однако, для усиления эффективности данных мероприятий требуется более тщательная проработка и планирование.

Анализ осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в цифровой образовательной среде представлен на основании двухлетнего наблюдения за сотрудниками профессиональной образовательной организации.

По результатам, наблюдения и бесед с сотрудниками ГБПОУ «Миасский педагогический колледж», были выявленные следующие типы технического поведения сотрудников, которые создают уязвимости в комплексной системе защиты цифровой образовательной среды, среди них: техническая неосмотрительность, халатность и безграмотность. Рассмотрим их более подробно.

1. Техническая неосмотрительность. Пользователь, может не завершив сеанс работы с АРМ, покинуть рабочее место;
2. Техническая халатность. Пользователь оставляет сведения личной идентификации в информационной системе колледжа в доступном месте (монитор, клавиатура и т.д.); не задумываясь о безопасности

открывает все ссылки и файлы, указанные в электронных письмах, на страницах сайтов;

3. Техническая безграмотность. Пользователь не знает основных правил информационной безопасности, например, методов определения типа документов по расширению файлов.

Таким образом, результаты проведенного анализа защиты информационной системы, системы обеспечения информационной безопасности студентов и осведомленности, а также выполнения сотрудниками организации основных принципов и правил защиты при работе в цифровой образовательной среде, явились основанием для разработки рекомендаций для обеспечения информационной безопасности в условиях функционирования цифровой образовательной среды ГБПОУ «Миасский педагогический колледж».

Выводы по главе 2

Теоретические изыскания, проведенные в первой главе магистерской диссертации, позволили перейти к выполнению первой группы практических задач исследования, а именно, анализу цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» в условиях обеспечения информационной безопасности, которые были реализованы в несколько этапов.

1) Анализ модели цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» позволил сделать следующие выводы:

– цифровая среда ГБПОУ «Миасский педагогический колледж» включает лишь некоторые компоненты ЦОС, такие как: официальный сайт колледжа, электронная почта, которая не является корпоративной, электронный журнал, электронный календарь и не включает систему электронного документооборота, систему дистанционного обучения, корпоративный портал и систему поддержки пользователей компьютерной техники;

– основные виды деятельности, реализуемые в ЦОС: дистанционное взаимодействие всех участников образовательного процесса, дистанционное взаимодействие образовательного учреждения с другими организациями социальной сферы требуют привлечения дополнительных ресурсов, которые не всегда относятся к образовательным и располагаются на удаленных серверах.

2) Анализ цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» по реализации мер информационной безопасности был осуществлен в несколько этапов:

– анализ системы защиты информационной системы колледжа в целом. Для анализа системы защиты информационной системы было проведено анализ реализованных мер комплексной защиты колледжа с перечнем мер, предложенных «Лабораторией Касперского» для реализации

комплексной программно-технической системы защиты информационных систем компаний и организаций. Проведенный анализ позволяет сделать следующие выводы: из 17 мер по защите информационных систем в полном объеме реализована лишь часть (6 – реализовано частично, а 5 мер – в системе защиты не реализованы); отсутствует политики и меры безопасности для «мобильных» устройств и ноутбуков, а использование таких гаджетов сотрудниками ежегодно растет; шифрование дисков, внешних устройств, используемых сотрудниками реализовано частично или не реализовано совсем.

– анализ системы обеспечения информационной безопасности студентов. На основании данного анализа построена модель обеспечения информационной безопасности студентов, которая включает в себя следующие основные компоненты: объект информационной безопасности – личная информационная среда студента, субъекты информационной безопасности, внутренние и внешние угрозы, а также мероприятия по обеспечению информационной безопасности, 2 из которых реализуются в полном объеме (правовое обеспечение информационной безопасности и техническое и программное обеспечение ИБ) и 5 частично (нравственный и эстетический контроль, защита психики и здоровья несовершеннолетнего, воспитательные меры по обеспечению ИБ, образование в области ИБ, формирование информационной культуры студентов).

– анализ осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в цифровой образовательной среде. По результатам, двухлетнего наблюдения за профессиональной деятельностью сотрудников колледжа в области информационной безопасности, а также личных бесед, были выявленные следующие типы технического поведения сотрудников, которые создают уязвимости в комплексной системе защиты информационной системы: технические неосмотрительность, халатность и безграмотность.

Данные результаты анализа цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» в условиях обеспечения информационной безопасности позволяют перейти к выполнению второй группы практических задач работы, а именно планированию и реализации мероприятий по совершенствованию системы обеспечения информационной безопасности в условиях функционирования цифровой образовательной среды колледжа.

ГЛАВА 3. СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ

3.1 Разработка методических рекомендаций по совершенствованию системы обеспечения информационной безопасности функционирования цифровой образовательной среды

Процесс разработки методических рекомендаций по совершенствованию системы обеспечения информационной безопасности функционирования цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» проходил в несколько этапов:

1) Анализ модели цифровой образовательной среды ГБПОУ «Миасский педагогический колледж», реализация данного этапа описана в п.п. 2.1.

2) Анализ цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» по реализации мер информационной безопасности. Описание данного этапа представлено в п.п. 2.2.

3) Составление методических рекомендаций по совершенствованию системы обеспечения информационной безопасности цифровой образовательной среды ГБПОУ «Миасский педагогический колледж». Основные пункты рекомендаций представлены в таблице 4. Все методические рекомендации, как единый документ представлены в Приложении 1.

Методические рекомендации – это методическое издание, содержащее комплекс кратких и четко сформулированных предложений по внедрению в практику эффективных методов организации образовательного процесса; разрабатываются на основе изучения и обобщения опыта образовательных организаций, преподавателей, проведенных исследований.

Структурно методические рекомендации по совершенствованию системы обеспечения информационной безопасности в условиях

функционирования цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» состоит из следующих элементов:

- титульный лист;
- сведения об авторе (авторах);
- пояснительная записка;
- аннотация;
- введение;
- основная часть;
- заключение;
- библиографический список;
- приложения.

Рассмотрим требования, предъявляемые к оформлению текста методических рекомендаций.

– Все страницы текста должны соответствовать единому формату А4 или А5. Объём методического издания должен превышать 15 листов.

– Текст следует размещать на одной стороне листа бумаги с соблюдением следующих размеров полей: формат А4 - левое - 3,0 см, правое - 1,5 см, верхнее - 2,0 см, нижнее - 2,0 см в текстовом редакторе Word шрифтом №14 Times New Roman, межстрочным интервалом 1,15 или 1,5, выравнивание по ширине страницы.

– Нумерация страниц: страницы текста нумеруют арабскими цифрами, соблюдая сквозную нумерацию по всему тексту; титульный лист, так же, как и оглавление, включаются в общую нумерацию страниц текста. Однако номер страницы не проставляется ни на титульном листе, ни на оглавлении.

– Главы, параграфы, пункты, подпункты текста нумеруются арабскими цифрами с точкой, например, 1., 1.1., 1.1.1. и т.д.

– Пояснительная записка, главы основной части, заключение, список литературы, вспомогательные указатели и приложения должны

начинаться с новой страницы и иметь заголовки, напечатанный прописными буквами. Параграфы, пункты и подпункты располагаются по порядку друг за другом.

– Заголовки структурных элементов текста следует располагать в середине строки без точки в конце, не подчеркивая. Переносы слов не допускаются. Расстояние между заголовками и текстом должно быть не менее 2-3 интервалов. Шрифты заголовков структурных элементов различного уровня (главы, параграфы, пункты, подпункты) должны быть однотипными.

– Оформление приложений. В случаях, когда графики, таблицы и другой материал слишком объёмны, также неуместны в тексте, но несут дополнительную смысловую информацию, их необходимо разместить в приложениях.

4) Экспертиза методических рекомендаций

Перед внедрением любых новшеств в систему обеспечения информационной безопасности функционирования цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» любые нововведения проходят экспертную оценку или процесс согласования. Экспертами выступили члены администрации и специалисты по информатизации, ответственные за различные аспекты обеспечения информационной безопасности колледжа.

Пример бланка оценочного листа для проведения экспертизы представлен в Приложении 2.

Результаты экспертной оценки представлены в таблице 4.

Таблица 4 – Результаты экспертной оценки

Эксперт	Оценки по разделам требований (5 балльная шкала)			Ср. итоговая оценка
	Мероприятия по проектированию модели цифровой образовательной среды профессиональной образовательной организации	Меры по совершенствованию осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в ЦОС	Меры по обеспечению информационной безопасности студентов в процессе функционирования цифровой образовательной среды	
К.Н.В.	5	4	5	4,5
Н.Н.В.	4	5	4	4,5
К.Ю.В.	4	4	5	4,3
Ср. итоговая оценка	4,3	4,3	4,7	4,4

Графические результаты представлены в виде диаграммы на рисунке 3.

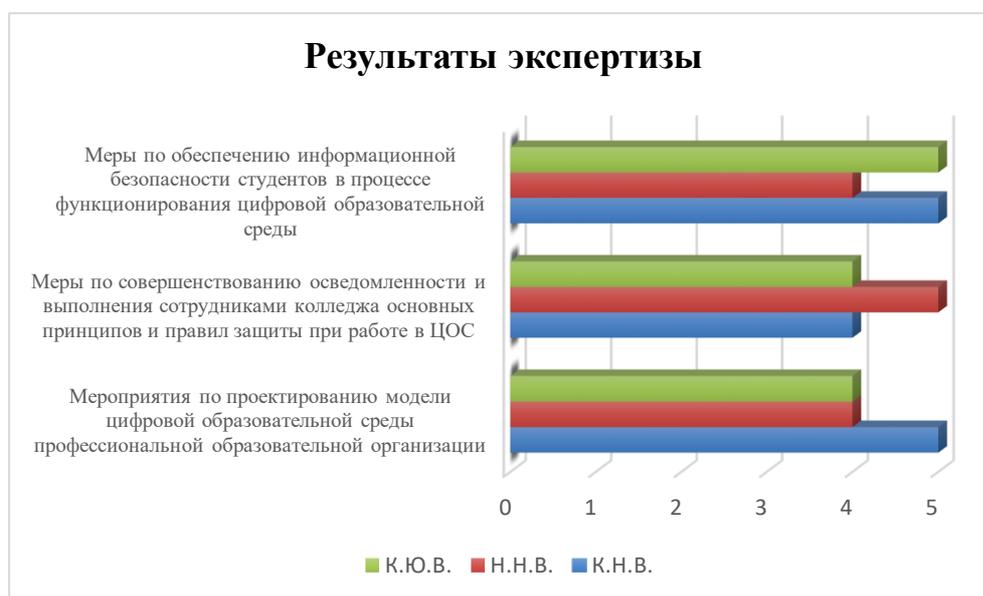


Рисунок 3 – Результаты экспертной оценки методических рекомендаций по совершенствованию системы обеспечения информационной безопасности в условиях функционирования цифровой образовательной среды ГБПОУ «Миасский педагогический колледж»

Все эксперты поставили высокие оценки разработанным методическим рекомендациям по совершенствованию системы обеспечения

информационной безопасности функционирования цифровой образовательной среды, рекомендовали их к внедрению.

5) Представление готовых методических рекомендаций к реализации. На основании результатов экспертизы, членами администрации и специалистами по информатизации были приняты следующие решения:

– включить отдельные меры по проектированию модели цифровой образовательной среды профессиональной образовательной организации, а также меры по совершенствованию системы защиты информации в план работы на 2019-2020 учебный год.

– отдельные меры по обеспечению информационной безопасности студентов в условиях функционирования цифровой образовательной среды и меры по совершенствованию осведомленности и выполнения сотрудниками института основных принципов и правил защиты при работе в ЦОС в план работы на 2020-2021 год.

3.2 Анализ результатов реализации методических рекомендаций по совершенствованию системы обеспечения информационной безопасности функционирования цифровой образовательной среды

В параграфе 3.1. было сказано, что в 5 пункте процесса разработки методических рекомендаций по совершенствованию системы обеспечения информационной безопасности функционирования цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» членами администрации и специалистами по информатизации на основании результатов экспертизы рекомендаций были приняты следующие решения:

– отдельные меры по проектированию модели цифровой образовательной среды профессиональной образовательной организации, а также меры по совершенствованию системы защиты информации включены в план работы на 2019-2020 учебный год;

– отдельные меры по обеспечению информационной безопасности студентов функционирования цифровой образовательной среды и меры по совершенствованию осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в ЦОС включены в план работы на 2020-2021 год.

Меры по проектированию модели цифровой образовательной среды профессиональной образовательной организации реализованы в период на 2019-2020 учебный год:

1. Разработана модель цифровой образовательной среды ГБПОУ «Миасский педагогический колледж», представленная на рисунке 4.

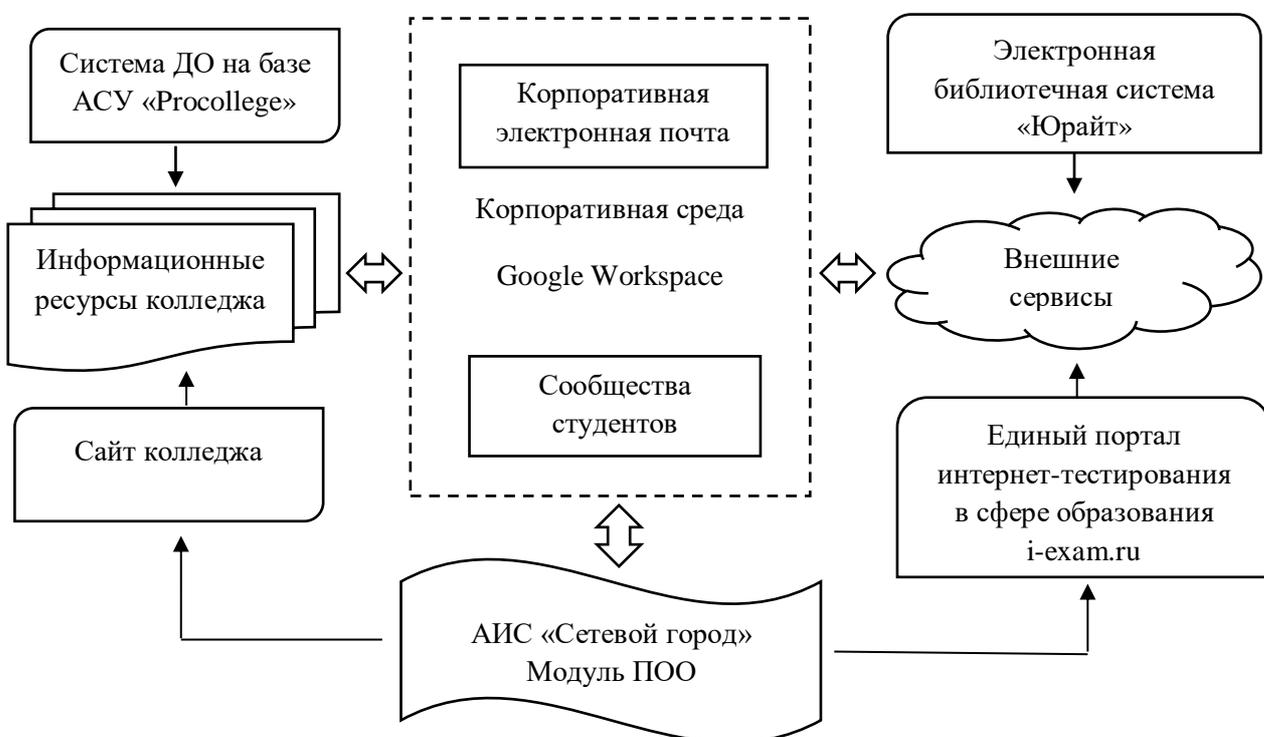


Рисунок 4 – Модель цифровой образовательной среды ГБПОУ «Миасский педагогический колледж»

Данные о реализованных мероприятиях по проектированию цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» представлены в таблице 5.

Таблица 5 – Реализация мероприятий по проектированию цифровой образовательной среды профессиональной ГБПОУ «Миасский педагогический колледж»

№ п/п	Компонент ЦОС	Результат выполнения
1.	Корпоративная электронная почта	Реализовано в полном объеме с использованием сервиса Google Workspace (пакет для учебных заведений бесплатен)
2.	Виртуальные чат-комнаты: – Коллектив – Администрация – Экспериментальная площадка – Руководители МО – Служба АХР – Классные руководители – Служба сопровождения	Реализовано частично, с помощью АСУ «ProCollege» созданы чаты для администрации и педагогического коллектива
3.	Система видеоконференцсвязи (https://bigbluebutton.ru/ - бесплатная вебинарная комната на своем сервере)	Реализовано в полном объеме, установлена на сервер колледжа для проведения онлайн-занятий, консультаций и видеоконференций.
4.	Учебные календари в АИС «Сетевой город» Модуль ПОО (https://poo.edu-74.ru/plan/#/calendars)	Ведется работа по реализации, поскольку АИС только вводится в эксплуатацию.
5.	Система электронного документооборота, встроенная в АСУ «ProCollege»	Реализовано в полном объеме.
5.	Система дистанционного обучения для студентов на базе АСУ «ProCollege»	Ведется работа по реализации: – обучение педагогического коллектива созданию курсов в АСУ «ProCollege»; – разработка и наполнение курсов дистанционного обучения.
6.	Электронный журнал в АИС «Сетевой город» Модуль ПОО (https://poo.edu-74.ru)	Ведется работа по реализации, поскольку АИС только вводится в эксплуатацию.
7.	Система поддержки пользователей компьютерной техники: – техподдержка АСУ «ProCollege»; – техподдержка АИС «Сетевой город» Модуль ПОО; – консультации специалиста по ИБ и системного администратора.	Реализовано в полном объеме, оказывается консультативная помощь всем участникам, работающих в цифровой образовательной среде.

Продолжение таблицы 5

8.	Официальный сайт ГБПОУ «Миасский педагогический колледж» (http://miasspk.ru/)	Реализовано в полном объеме, пополняется раздел «Информационная безопасность» в соответствии с актуальными тенденциями развития образования.
9.	Электронная библиотечная система «Юрайт» (https://urait.ru/)	Реализовано частично. Электронная библиотечная система внедрена в практику образовательного процесса, однако только часть педагогов прошли курсы повышения квалификации и используют данную систему.
10.	Система оценки / мониторинга качества образования (https://i-exam.ru/)	Ведется работа по ознакомлению педагогического коллектива и внедрению системы оценки.

2. Для анализа системы защиты информационной системы было проведен анализ реализованных мер комплексной защиты колледжа с перечнем мер, предложенных «Лабораторией Касперского» для реализации комплексной программно-технической системы защиты информационных систем компаний и организаций после внедрения мер по совершенствованию системы защиты информации. Результаты анализа представлены в таблице 6.

Проведенный анализ позволяет сделать вывод о том, что:

1. Из 17 мер по защите информационных систем в полном объеме реализована часть; 2 – реализовано частично, а 3 меры – в системе защиты не реализованы.

2. Отсутствует политики и меры безопасности для «мобильных» устройств, а использование таких гаджетов сотрудниками ежегодно растет.

Таблица 6 – Реализация мероприятий по совершенствованию системы защиты информации

№	Наименование элемента защиты информационной системы (Перечень «Лаборатории Касперского»)	Реализация в колледже
1	Защита от вредоносного ПО	Реализовано в полном объеме
2	Управление обновлением ПО	Реализовано в полном объеме
3	Разграничение доступа к ИТ ресурсам	Реализовано в полном объеме
4	Сетевая структура (выделение критически важных подсетей)	Реализовано в полном объеме

Продолжение таблицы 6

5	Контроль использования внешних устройств	Реализовано в частичном объеме
6	Специальная политика безопасности для внешних устройств	Реализовано в полном объеме. Администратором создан профиль политики безопасности для внешних устройств.
7	Специальная политика безопасности для съемных носителей	Реализовано в полном объеме. Администратором создан профиль политики безопасности для съемных носителей.
8	Шифрование переписки	Реализовано в полном объеме
9	Шифрование файлов и папок	Реализовано в полном объеме
10	Контроль программ	Реализовано в полном объеме
11	Антивирусное ПО для мобильных устройств	Отсутствует
12	Специальная политика безопасности для ноутбуков	Реализовано в полном объеме. Администратором в дереве консоли выбрана группа администрирования, для политики которой нужно создан профиль политики безопасности для ноутбуков.
13	Полное шифрование диска	Реализовано в полном объеме. В политике администратор создает правило по умолчанию для шифрования всех жестких дисков. После применения политики программа выполняет шифрование жестких дисков посекторно. Программа шифрует все логические разделы жесткого диска.
14	Шифрование данных на съемных носителях	Реализовано в полном объеме. В политике администратором создано правило шифрования по умолчанию, которое применяется ко всем съемным носителям. Программа шифрует и расшифровывает файлы после применения политики согласно приоритетам
15	Аудит ИТ безопасности независимыми компаниями	Реализовано в частичном объеме (проверки ФАПСИ по реализации защиты конфиденциальной информации об обучающихся)
16	Специальная политика безопасности для смартфонов / планшетов	Отсутствует
17	Системы управления мобильными устройствами	Отсутствует

Мероприятия по совершенствованию системы защиты информации и меры по совершенствованию осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в ЦОС включены в план работы на 2020-2021 год, поэтому ведется работа по их реализации.

В план работы по совершенствованию системы информационной безопасности колледжа включены следующие мероприятия по обеспечению информационной безопасности студентов в условиях функционирования цифровой образовательной среды:

- обновление нормативно-правовых документов по обеспечению информационной безопасности на сайте колледжа в разделе «Информационная безопасность»;

- в план общеколледжной воспитательной работы включены мероприятия по осуществлению нравственного и эстетического контроля, а также по защите психики и здоровья несовершеннолетнего, такие как Всероссийская добровольная просветительская интернет-акция «Безопасность детей в сети Интернет», Федеральный проект «Цифровой Диктант», Всероссийской образовательной акции по информационным технологиям «ИТ - диктант» и др.;

- в план воспитательной работы учебных групп 1-2 курса включены мероприятия по обеспечению информационной безопасности: серия медиауроков по теме: «Личная информационная безопасность в сети Интернет», участие в акции «Урок НТИ» и др.;

- мероприятия, включающие техническое и программное обеспечение ИБ: использование «Лаборатории Касперского» и контент-фильтрации SkyDNS;

- мероприятия в области образования по ИБ: включение разделов, посвящённых информационной и кибербезопасности в учебные дисциплины ОБЖ и безопасность жизнедеятельности, информатика, информатика и ИКТ в профессиональной деятельности; в рамках сетевого взаимодействия с

учреждениями дополнительного образования организована реализация дополнительной общеобразовательной, общеразвивающей программы «Цифровая гигиена и работа с большими данными», охват студентов: две учебные группы первого курса;

– мероприятия, направленные на формирование информационной культуры студентов, реализуются через размещение и изучение содержимого стенда, посвященного информационной культуре на современном этапе развития общества, а также осуществление вышеописанной работы по образованию и воспитанию в области информационной безопасности.

Мероприятия по выполнению сотрудниками колледжа основных принципов и правил защиты при работе в ЦОС включают следующие аспекты:

– разработана программа повышения квалификации сотрудников колледжа «Обеспечение информационной безопасности функционирования цифровой образовательной среды профессиональной образовательной организации» (Приложение 3);

– разработана памятка для педагогических работников по обеспечению информационной безопасности обучающихся в ГБПОУ «Миасский педагогический колледж» (Приложение 4).

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

Выводы по главе 3

Проанализировав во второй главе цифровую образовательную среду ГБПОУ «Миасский педагогический 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 цифровой образовательной среды колледжа.

Структурно методические рекомендации по совершенствованию системы обеспечения информационной безопасности функционирования ЦОС состоят из следующих элементов: титульный лист; оглавление; пояснительная записка; особенности проектирования и функционирования цифровой образовательной среды в информационном пространстве организаций среднего профессионального образования; мероприятия по проектированию модели цифровой образовательной среды профессиональной образовательной организации; меры по совершенствованию осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в цифровой образовательной среде; меры по обеспечению информационной безопасности студентов в условиях функционирования цифровой образовательной среды; цифровые образовательные технологии в среднем профессиональном образовании; заключение; библиографический список; приложение.

Методические рекомендации по совершенствованию системы обеспечения информационной безопасности функционирования цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» представлены в Приложении 1.

Перед внедрением любых новшеств в систему информационной безопасности 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 цифровой образовательной среды ГБПОУ «Миасский педагогический колледж», рекомендовали их к внедрению.

На основании результатов экспертизы, были приняты следующие решения:

– отдельные меры по проектированию модели цифровой образовательной среды профессиональной образовательной организации, а также меры по совершенствованию системы защиты информации включены в план работы на 2019-2020 учебный год.

– отдельные меры по обеспечению информационной безопасности студентов в процессе функционирования цифровой образовательной среды и меры по совершенствованию осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в ЦОС включены в план работы на 2020-2021 год.

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

ЗАКЛЮЧЕНИЕ

Подводя итоги проведенному исследованию, отметим, что поставленные в задачи решены и положения гипотезы подтверждены.

1) Изучены законодательные акты и нормативно-правовые документы в области организации и функционирования цифровой образовательной среды профессиональной образовательной организации, на основании чего сделаны следующие выводы: в настоящее время приняты к исполнению приоритетные проекты в области образования:

– приоритетный проект «Создание современной образовательной среды для школьников», в рамках которого правительство РФ стремится предоставить максимальную доступность обучающимся к качественному общему образованию;

– приоритетный проект «Цифровая школа», нацеленный на обеспечение к 2024 году всех общеобразовательных учреждений современной и безопасной цифровой образовательной средой, гарантирующей достижение необходимого уровня информатизации образования;

– приоритетный проект «Современная цифровая образовательная среда в Российской Федерации», предоставляющий возможность гражданам Российской Федерации получить необходимое им качественное образование с любой точки страны посредством дистанционного онлайн-обучения.

2) Описана целевая модель цифровой образовательной среды. дана характеристика ЦОС профессиональной образовательной организации в условиях обеспечения информационной безопасности.

В соответствии с методическими рекомендациями по вопросам внедрения Целевой модели цифровой образовательной среды в субъектах Российской Федерации, внедрение целевой модели ЦОС осуществляется в образовательных организациях, осуществляющих деятельность в сфере общего образования, среднего профессионального образования и

соответствующего дополнительного профессионального образования, профессионального обучения, дополнительного образования детей и взрослых, воспитания в рамках полномочий Минпросвещения России.

3) Представлена характеристика ЦОС профессиональной образовательной организации в условиях обеспечения информационной безопасности.

Создание ЦОС и применение цифровых технологий обучения является эффективным, как для студентов и обучающихся, так и для преподавателей. Однако в процессе организации и функционирования ЦОС могут возникать различные риски, одним из которых является обеспечение информационной безопасности данной среды.

Информационная безопасность выражается в защищенности, гарантии сохранности состояния человека, общества, ресурсов, условий и т.д., одним словом, среды, в которой живёт, действует и развивается личность.

4) Проанализирована модель цифровой образовательной среды профессиональной образовательной организации (на примере базы исследования) в условиях обеспечения информационной безопасности.

Анализ модели цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» позволил сделать следующие выводы:

– цифровая среда ГБПОУ «Миасский педагогический колледж» включает лишь некоторые компоненты ЦОС, такие как: официальный сайт колледжа, электронная почта, которая не является корпоративной, электронный журнал, электронный календарь и не включает систему электронного документооборота, систему дистанционного обучения, корпоративный портал и систему поддержки пользователей компьютерной техники;

– основные виды деятельности, реализуемые в ЦОС: дистанционное взаимодействие всех участников образовательного процесса, дистанционное взаимодействие образовательного учреждения с другими организациями социальной сферы требуют привлечения дополнительных

ресурсов, которые не всегда относятся к образовательным и располагаются на удаленных серверах.

Анализ цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» по реализации мер информационной безопасности был осуществлен в несколько этапов:

– анализ системы защиты информационной системы колледжа в целом. Для анализа системы защиты информационной системы было проведено анализ реализованных мер комплексной защиты колледжа с перечнем мер, предложенных «Лабораторией Касперского» для реализации комплексной программно-технической системы защиты информационных систем компаний и организаций. Проведенный анализ позволяет сделать следующие выводы: из 17 мер по защите информационных систем в полном объеме реализована лишь часть (6 – реализовано частично, а 5 мер – в системе защиты не реализованы); отсутствует политики и меры безопасности для «мобильных» устройств и ноутбуков, а использование таких гаджетов сотрудниками ежегодно растет; шифрование дисков, внешних устройств, используемых сотрудниками реализовано частично или не реализовано совсем.

– анализ системы обеспечения информационной безопасности студентов. На основании данного анализа построена модель обеспечения информационной безопасности студентов, которая включает в себя следующие основные компоненты: объект информационной безопасности – личная информационная среда студента, субъекты информационной безопасности, внутренние и внешние угрозы, а также мероприятия по обеспечению информационной безопасности, 2 из которых реализуются в полном объеме (правовое обеспечение информационной безопасности и техническое и программное обеспечение ИБ) и 5 частично (нравственный и эстетический контроль, защита психики и здоровья несовершеннолетнего, воспитательные меры по обеспечению ИБ, образование в области ИБ, формирование информационной культуры студентов).

– анализ осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в цифровой образовательной среде. По результатам, двухлетнего наблюдения за профессиональной деятельностью сотрудников колледжа в области информационной безопасности, а также личных бесед, были выявленные следующие типы технического поведения сотрудников, которые создают уязвимости в комплексной системе защиты информационной системы: технические неосмотрительность, халатность и безграмотность.

5) Разработаны и апробированы методические рекомендации по совершенствованию системы обеспечения информационной безопасности функционирования цифровой среды профессиональной образовательной организации (на примере базы практики).

Структурно методические рекомендации по совершенствованию системы обеспечения информационной безопасности функционирования ЦОС состоят из следующих элементов: титульный лист; оглавление; пояснительная записка; особенности проектирования и функционирования цифровой образовательной среды в информационном пространстве организаций среднего профессионального образования; мероприятия по проектированию модели цифровой образовательной среды профессиональной образовательной организации; меры по совершенствованию осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в цифровой образовательной среде; меры по обеспечению информационной безопасности студентов в условиях функционирования цифровой образовательной среды; цифровые образовательные технологии в среднем профессиональном образовании; заключение; библиографический список; глоссарий; приложения.

Перед внедрением любых новшеств в систему информационной безопасности любые нововведения проходят экспертную оценку или процесс

согласования. Экспертами методических рекомендаций выступили члены администрации и специалисты по информатизации, ответственные за различные аспекты обеспечения информационной безопасности колледжа.

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

На основании результатов экспертизы, были приняты следующие решения:

– отдельные меры по проектированию модели цифровой образовательной среды профессиональной образовательной организации, а также меры по совершенствованию системы защиты информации включены в план работы на 2019-2020 учебный год.

– отдельные меры по обеспечению информационной безопасности студентов функционирования цифровой образовательной среды и меры по совершенствованию осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в ЦОС включены в план работы на 2020-2021 год.

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

На основании анализа данных всех этапов выполнения магистерской диссертации можно сделать вывод об успешности выполнения всех задач выпускной квалификационной работы и достижения поставленной цели.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аксюхин, А.А. Информационные технологии в образовании и науке / Аксюхин А.А., Вицен А.А., Мекшенева Ж.В. // Современные наукоемкие технологии, 2019. № 11. С. 50–52.
2. Андреев А.А. Некоторые проблемы педагогики в современных информационно-образовательных средах // Инновации в образовании, 2014. – №6. С. – 98 – 113.
3. Андриюхина Л.М., Садовникова Н.О., Уткина С.Н., Мирзаахмедов А.М. Цифровизация профессионального образования: перспективы и незримые барьеры [Электронный ресурс] // Образование и наука. – 2020; 22(3): 116-147. Режим доступа: <https://doi.org/10.17853/1994-5639-2020-3-116-147> (дата обращения: 18.09.2020)
4. Афолина, Е. С. Модель обеспечения информационной безопасности школьников при создании единого информационного пространства школы [Текст] / Е. С. Афолина. // Молодой ученый. – 2015. – № 6.4 (86.4). – С. 68-71.
5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: утв. Федеральной службой по техническому и экспортному контролю 15 февраля 2008 г //СПС Консультант Плюс.
6. Баймакова, И.А. Обеспечение защиты персональных данных. Методическое пособие / И.А. Баймакова, А.В. Новиков, А.И. Рогачев – М.: 1С -Публишинг, 2014. – 214 с.
7. Безопасное использование сайтов в сети Интернет в образовательном процессе в целях обучения и воспитания обучающихся в образовательной организации [Электронный ресурс]: Портал «Единыйурок.рф» // Режим доступа: <https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/kartochka-programmy/item/603-formirovanie-i->

razvitiipedagogicheskoi-ikt-kompetentnosti-v-sootvetstvii-s-trebovaniyami-fgos-i-professionalnogo standarta (дата обращения: 11.12.2020).

8. Безопасность детей в интернете: международный опыт и вызовы для России / Под ред. С. А. Грина. – М.: Центр изучения интернета и общества, Российская экономическая школа, 2012.

9. Белов, Е.Б. Основы информационной безопасности [Текст]. Учебное пособие для вузов / Е.Б.Белов, В.П.Лось, Р.В.Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2016. – 544 с.

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

11. Богатырева, Ю. И. Безопасный Интернет для школьников, родителей и учителей / Ю.И. Богатырева, А.Н. Привалов, Л.В. Пятницкая // Преподавание информационных технологий в Российской Федерации: материалы Одиннадцатой открытой Всероссийской конференции (17-17 мая 2013 г.). – Воронеж: Воронежский государственный университет, 2013. – 332 с. – С. 319-320.

12. Богатырева, Ю.И. Анализ проблем информационной безопасности личности обучающихся / Новые информационные технологии в образовании: материалы VI междунар. научно-практической конференции, Екатеринбург, 12-15 марта 2013 г. //ФГАОУ ВПО «Рос. гос. проф.-пед. ун-т», Екатеринбург, 2013. – 390 с. – с. 313-316.

13. Богатырева, Ю.И. Информационная безопасность школьников в образовательной среде: теория и практика высшей школы. Тула: ТулГУ, 2013. – 160 с.

14. Богатырева, Ю.И. Компетентность педагогов в области информационной безопасности: проблема и пути решения / Ю.И. Богатырева, А.Н. Привалов // Известия Российской академии образования – 2013, № 2 (26) – 148 с. - С. 96-106.

15. Богатырева, Ю.И. Модель обеспечения информационной безопасности школьников при создании инфобезопасной среды

образовательного учреждения / Ю.И. Богатырева // Известия Тульского государственного университета. Гуманитарные науки. Вып. 3. Ч. 2. Тула: изд-во ТулГУ, 2013. – 343 с. – С. 14-25.

16. Богатырева, Ю.И. Организация безопасного информационного пространства школьников в Интернете: методические рекомендации для бакалавров и магистров направления 050100 Педагогическое образование, учителей, учащихся и их родителей / Ю.И. Богатырева, А.Н. Привалов, С.В. Пазухина. Тула: Изд-во ТулГУ, 2013. – 96 с.

17. Богатырева, Ю.И. Подходы к разработке методической системы формирования компетентности в области информационной безопасности учителей информатики / Ю.И. Богатырева, А.Н. Привалов // Информатика и образование. 2012. Выпуск 10. - С. 77- 80.

18. Ваграменко, Я.А. Информатизация образования: итоги и направления дальнейшей работы // Педагогическая информатика. 2017. - №1. -С. 41 -51.

19. 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.

20. Гершунский, Б.С. Компьютеризация в сфере образования: проблемы и перспективы./ Б.С. Гершунский - М.: Педагогика, 2017. - 264 с.

21. Главный тренд российского образования – цифровизация. [Электронный ресурс] // Режим доступа: <http://www.ug.ru/article/1029/> (дата обращения: 30.09.2020).

22. Гнатышина, Е.А. Магистерская диссертация: рекомендации по подготовке и защите: учебно-методическое пособие/ Е.А. Гнатышина, В.А. Белевитин, И.Г. Черновол.- Челябинск: ЧГПУ, 2016. – 158с.

23. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Электронный ресурс]. – Введ. 2006–12–27. //СПС Консультант Плюс.

24. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения [Электронный ресурс]. – Введ. 2000–06–30. //СПС Консультант Плюс.

25. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью [Электронный ресурс]. – Введ. 2007–01–01. //СПС Консультант Плюс.

26. Григорьев, С.Г. Информатизация образования. Фундаментальные основы. / С.Г. Григорьев, В.В. Гриншкун. - Москва, 2013.- 231 с.

27. Евдокимова, Т.Г. Инновационный менеджмент [Текст] / Т.Г. Евдокимова, Г. А. Маховикова, Н.Ф. Ефимова. - СПб.: «Вектор», 2005. - 285с.

28. Елжанова, Р.К. Инновационные процессы в образовании [Текст] / Р.К. Елжанова, Э.Р. Давлетгильдинов // Проблемы современной экономики: материалы IV Международной научной конференции (г. Челябинск, февраль, 2015 г.).- Челябинск: Два комсомольца, 2015. – с.1-3.

29. Завьялова, Н.Б. Методология разработки интегрированной информационной образовательной среды / Н.Б. Завьялова, Л.П. Дьяконова // Материалы: XI конференция-выставка «Информационные технологии в образовании». – М.: МИФИ, 2011. – 200 с.

30. Захарова, И.Г. Информационные технологии в образовании: учеб. пособие для студ. высш. пед. учеб. заведений / И.Г. Захарова. – М: ИЦ «Академия», 2015. -192 с.

31. Защита детей в Интернете [Электронный ресурс]: Сайт Лаборатории Касперского // Режим доступа: <https://www.kaspersky.ru/resource-center/preemptive-safety/kids-online-safety> (дата обращения: 11.12.2019)

32. Зубаиров, А.Ф. Создание единой информационной среды для оказания муниципальных услуг в сфере образования в электронном виде / А.Ф. Зубаиров // Научно-методическое обеспечение оценки качества

образования. Научно-методический журнал. – Челябинск, 2017 №1(2). С. 105-109.

33. Ильин, А.С. Анализ состояния защищенности персональных данных при их обработке в учреждениях системы образования Челябинской области в 2016 году / А.С. Ильин, Д.С. Ильина // Научно-методическое обеспечение оценки качества образования. Научно-методический журнал. – Челябинск, 2017 №1(2). С. 89-94.

34. Ильин, А.С. Обеспечение безопасности информации в образовательной организации в современных условиях / А.С. Ильин, Д.С. Ильина // Научно-методическое обеспечение оценки качества образования – 2016 –№ 1 – 48-51.

35. Информатизация образования. [Электронный ресурс] // Российская педагогическая энциклопедия. Режим доступа: <https://pedagogicheskaya.academic.ru/1241/> (дата обращения: 15.03.2020).

36. Информационный сервис для профессионального образовательного сообщества «Агрегатор новостей образования» [Электронный ресурс] // Режим доступа: https://akvobr.ru/cifrovaya_obrazovatel'naya_sreda_ehto.html (дата обращения: 15.04.2020).

37. Кашина, Е.А. Прогнозирование структуры интегрированного курса информатики: дис. канд. пед. наук / Е.А. Кашина. Екатеринбург, 2017. 187 с.

38. Концепция создания и развития информационно-образовательной среды Открытого Образования системы образования РФ [электронный ресурс] / Концепции информационно-образовательной среды. — Саратов, 2012. – Режим доступа: <http://do.sgu.ru/conc.html>. (дата обращения 27.02.20)

39. Красильникова, В.А. Информатизация образования: понятийный аппарат / В.А. Красильникова // Информатика и образования, № 4, 2013. - С. 21 – 27.

40. Кречетников, К.Г. Методология проектирования, оценки качества и применения информационных технологий обучения / К.Г. Кречетников. – М.: Госкоорцентр, 2016 – 216 с.

41. Крысин, Л.П. Толковый словарь иноязычных слов / Л.П. Крысин. – М.:Инфокнига, 2015.-564с.

42. Кузнецов, Э.И. Общеобразовательные и профессионально-прикладные аспекты изучения информатики и вычислительной техники в педагогическом институте: автореф. дис. . д-ра пед. наук. М., 2015.

43. Курова, Н.Н. Информационная среда образовательного учреждения как управленческий ресурс современного руководителя школы [электронный ресурс] / Н.Н. Курова // Конференция «Информационные технологии в образовании». – М., 2012. – Режим доступа: <http://www.ito.su/main.php?pid=26>(дата обращения 27.02.20)

44. Кязимов К. Г. Цифровая образовательная среда как условие для применения цифровых образовательных технологий в УПО // Профессиональное образование в современном мире. 2020. Т. 10, № 1. С. 3556–3565. doi: 10.15372/PEMW20200118

45. Лобачев, С.Л. Региональная информационно-образовательная среда - основа федеральной среды системы открытого образования // Телематика-2016. -СПб.: СПб ГТУ, 2016 - 98с.

46. Лобачев, С.Л. Универсальная инструментальная информационно-образовательная среда системы открытого образования Российской Федерации / С.Л. Лобачев, А.А. Поляков. М.: ИЦПКПС, 2015. - 40 с.

47. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст]. Учеб. пособие для вузов / А.А. Малюк. – М.: Горячая линия-Телеком, 2014. – 280 с.

48. Меняйся или уходи. Цифровое образование бросает вызов преподавателям вузов. [Электронный ресурс] // Режим доступа: <http://www.poisknews.ru/theme/edu/31969/> (дата обращения: 30.09.2020).

49. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: утв. Федеральной службой по техническому и экспортному контролю 14 февраля 2008 г //СПС Консультант Плюс.

50. Михалева, Г.В. Современная британская стратегия информационной безопасности детей и молодежи [Электронный ресурс] // Вестник ЧелГУ. 2013. №22 (313). URL: <https://cyberleninka.ru/article/n/sovremennaya-britanskaya-strategiya-informatsionnoybezopasnosti-detey-i-molodezhi> (дата обращения: 12.05.2020).

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

52. Новиков, А.М. Организация опытно-экспериментальной работы на базе образовательного учреждения [Текст] /А.М. Новиков// Дополнительное образование. – 2012. – № 4. С.51 – 53.

53. О персональных данных [Электронный ресурс]: Федеральный закон №152-ФЗ: [принят Гос. Думой 8 июля 2006 г.: одобр. Советом Федерации 14 июля 2006 года]// СПС Консультант Плюс.

54. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федер. закон: [принят Гос. Думой 8 июля 2006 г.: одобр. Советом Федерации 14 июля 2006 г.] //СПС Консультант Плюс.

55. Об образовании в Российской Федерации (ред. от 29.07.2019) [Электронный ресурс]: федер. закон: [принят Гос. Думой 21.12. 2012 г.] //СПС Консультант Плюс.

56. Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: постановление Правительства РФ от 17 ноября 2007 г. N 781. //СПС Консультант Плюс.

57. Об утверждении Целевой модели цифровой образовательной среды: [приказ Министерства просвещения РФ от 02.12.2019 № 649, зарегистрирован в Минюсте РФ 24.12.2019, регистрационный № 56962] [Электронный ресурс] // Правовая база Гарант. — 2020. — URL: <https://www.garant.ru/> (дата обращения: 20.03.2020).

58. Образовательные экосистемы для общественной трансформации. Доклад Global Education Futures [Электронный ресурс] / П. Лукша, Дж. Кубиста, А. Ласло // Образование для сложного общества. – С. 77. Режим доступа:
<https://drive.google.com/file/d/0B9ZvF6mQ5FMbSTFKVmhodU5rNTNiTXpUZ2QwZktiR0pzSmJR/view> (дата обращения: 18.09.2020)

59. Общая повестка дня России и АСЕАН в киберпространстве: противодействие глобальным угрозам, укрепление кибербезопасности и развитие сотрудничества // Индекс безопасности № 4 (111), том 20 – С. 77-92 [электронный ресурс] <http://www.pircenter.org/media/content/files/18/14219241510.pdf>. (Дата обращения 10.10.2018)

60. Петрова, Н. П. Цифровизация и цифровые технологии в образовании / Н. П. Петрова, Г. А. Бондарева // Мир науки, культуры, образования. – 2019. – № 5 (78). – С. 353–355.

61. Пимонов, В.А. Основные проблемы обеспечения информационной безопасности субъектов образовательного процесса [Электронный ресурс] // Психология и право. 2011. № 4. Режим доступа: <http://psyjournals.ru/psyandlaw/2011/n4/49302.shtml> (дата обращения: 26.07.2019).

62. Письмо Минпросвещения России от 07.06.2019 N 04-474 «О методических рекомендациях» (вместе с «Методическими рекомендациями по ограничению в образовательных организациях доступа, обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования») [Электронный ресурс] // Режим

доступа: http://www.consultant.ru/document/cons_doc_LAW_328805/ (дата обращения: 26.07.2019).

63. Полат Е.С. Новые педагогические и информационные технологии в системе образования [Текст] / Полат Е.С.– М.: Академия, 2016. – 272 с.

64. Полат Е.С., Новые педагогические и информационные технологии в системе образования /Е.С. Полат, М.Ю. Бухаркина и др. - М.: ИД «Академия», 2012. – 272с.

65. Полат, Е.С. Современные педагогические и информационные технологии в системе образования: учебное пособие для студентов высших учебных заведений [Текст] / Е.С. Полат, М.Ю.Бухаркина. – 3-е изд., стер. – М.:Издательский центр «Академия», 2015 г. – 368 с.

66. Практическая психология безопасности. Управление персональными данными в интернете: учеб.-метод. пособие для работников системы общего образования / Солдатова Г.У., Приезжева А.А., Олькина О.И., Шляпников В.Н. – М.: Генезис, 2017. 224 с.

67. Привалов, А.Н., Богатырева Ю.И. Основные угрозы информационной безопасности субъектов образовательного процесса // Известия ТулГУ. Гуманитарные науки. 2012. №3. - Режим доступа: <https://cyberleninka.ru/article/n/osnovnyye-ugrozy-informatsionnoy-bezopasnosti-subektov-obrazovatel'nogo-protsesssa> (дата обращения: 12.01.2019)

68. Приоритетный проект в области образования «Современная цифровая образовательная среда в Российской Федерации». [Электронный ресурс] // URL: <http://neorusedu.ru/about/> (дата обращения: 30.09.2020).

69. Распоряжение Правительства РФ от 28.07.2017 N 1632-р «Об утверждении программы Цифровая экономика Российской Федерации» [Электронный ресурс] // Режим доступа: [base.garant.ru/71 734 878](http://base.garant.ru/71734878) (дата обращения: 12.08.2020)

70. Роберт, И.В. Информатизация образования (педагогико-эргономический аспект). / И.В. Роберт - М.: РАО, 2012. – 216с.

71. Роберт, И.В. Информационные и коммуникационные технологии в образовании. Учебное пособие / И.В. Роберт, С.В. Панюкова, А.А. Кузнецов, А.Ю. Кравцова. – М.: Дрофа, 2015. – 320 с.

72. Роберт, И.В. Информационные технологии в науке и образовании: учеб.-метод. пособие. / И.В. Роберт - М.: РАО, 2014. – 118с.

73. Роберт, И.В. Основные направления научных исследований в области информатизации профессионального образования / И.В. Роберт, В.А. Поляков. – М.: «Образование и Информатика», 2014 – 96с.

74. 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.

75. Самарханова, Э.К. Основные направления и принципы развития информатизации образовательного учреждения. Журнал «Наука и школа» 2010, [Электронный ресурс] – Режим доступа: <https://cyberleninka.ru/article/n/osnovnyie-napravleniya-i-printsipy-razvitiya-informatizatsii-obrazovatel'nogo-uchrezhdeniya>. (дата обращения: 13.05.2020).

76. Сичинский, Е. П. О системе непрерывного повышения квалификации работников среднего профессионального образования Челябинской области / Е. П. Сичинский, И. Р. Сташкевич, З. А. Федосеева // Современная наука: актуальные проблемы теории и практики. – 2018. – № 8. – С. 72-75.

77. Современный энциклопедический словарь /под ред. А.М. Прохорова. - М.: Просвещение, 2015 -1112с.

78. Сташкевич, И. Р. Информатизация как стратегический фактор развития профессионального образования / И. Р. Сташкевич // Инновационное развитие профессионального образования. – 2016. – № 4 (12). – С. 25-28.

79. Сташкевич, И. Р. Информационно-образовательная среда профессиональной образовательной организации – смена образовательной

парадигмы / И. Р. Сташкевич // Профессиональное образование и рынок труда. – 2014. – № 9 (13). – С. 26-28.

80. Стратегия развития информационного общества в РФ на 2017–2030 годы [Электронный ресурс]. Режим доступа: docs.cntd.ru/document/420397755 (дата обращения: 12.08.2020)

81. Стратегия развития информационного общества на 2017 – 2030 годы (утв. Указом Президента РФ от 9 мая 2017 г. N 203) [Электронный ресурс] // Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_216363/e91cc5f89aaced60e19c6c6554fc03432f4ee971/ (дата обращения: 11.06.2020)

82. Тайлаков У. Н. Единое информационно-образовательное пространство школы как фактор повышения качества образовательных процессов [Текст] / У. Н. Тайлаков // Молодой ученый. – 2013. – №5. – С. 768-772.

83. Федеральный закон от 29.12.2010 №436-ФЗ (ред. от 18.12.2018) «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс] // Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 11.06.2020)

84. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности [Текст]/ А.Ф. Чипига. – М.:ГелиосАРМ, 2017. –336с.

85. Шпагина, Е.М. Информационная безопасность в контексте защиты прав детей в Российской Федерации [Электронный ресурс] // Психология и право. 2016. Том 6. № 4. С. 86–94. doi:10.17759/psylaw.2016060409 O'Neill B., Staksrud E. Final recommendations for policy. London: EU Kids Online, LSE, 2014. p.42. Режим доступа: <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/D64Policy.pdf>. (дата обращения: 24.11.2019 г.)

86. Шубинский, М.И. Информационная безопасность для работников бюджетной сферы: учеб. пособие / НИУ ИТМО. - СПб., 2012.

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

ПРИЛОЖЕНИЕ 1

Методические рекомендации по совершенствованию системы обеспечения информационной безопасности функционирования цифровой образовательной среды профессиональной образовательной организации

Методические рекомендации по совершенствованию системы обеспечения информационной безопасности функционирования цифровой образовательной среды. – Челябинск: ФГБОУ ВО «ЮУрГГПУ», 2021. – 51 с.

Составители:

М.В. Бугаевская М.В., магистрант ФГБОУ ВО «ЮУрГГПУ»

В данных методических рекомендациях представлены материалы, отражающие теоретические положения и практические рекомендации по организации и функционированию современной цифровой образовательной среды в профессиональных образовательных организациях среднего профессионального образования.

Представленная теория и практика является системным комплексным решением цифровизации всех процессов профессиональной образовательной организации, фактического создания сетевого виртуального пространства для взаимодействия участников образовательного процесса в условиях обеспечения информационной безопасности.

Материалы сборника предназначены для администрации, преподавателей, мастеров производственного обучения и обучающихся профессиональных образовательных организаций среднего профессионального образования.

ОГЛАВЛЕНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА	95
1. Особенности проектирования и функционирования цифровой образовательной среды в информационном пространстве организаций среднего профессионального образования.....	96
2. Мероприятия по проектированию модели цифровой образовательной среды профессиональной образовательной организации	106
3. Меры по совершенствованию осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в цифровой образовательной среде.....	109
4. Меры по обеспечению информационной безопасности студентов в условиях функционирования цифровой образовательной среды	113
5. Цифровые образовательные технологии в среднем профессиональном образовании.....	122
ЗАКЛЮЧЕНИЕ	139
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	141
ПРИЛОЖЕНИЕ 1 Глоссарий.....	144

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Главная цель издания методических рекомендаций по совершенствованию системы обеспечения информационной безопасности функционирования цифровой образовательной среды заключается в оказании помощи администрации профессиональной образовательной организации, педагогическим работникам и студентам в развитии компетенций, направленных на эффективное взаимодействие в цифровой образовательной среде в условиях обеспечения информационной безопасности.

Предлагаемые методические рекомендации представляют собой синтез многочисленных литературных источников, посвященных вопросам обеспечения информационной безопасности в условиях функционирования ЦОС, а также опыта работы в данном направлении.

Изложенный теоретический материал с разной степенью полноты охватывает всё необходимое для организации и функционирования ЦОС профессиональной образовательной организации (ПОО) в условиях обеспечения информационной безопасности.

Особое внимание уделяется проектированию модели ЦОС, развитию профессиональных компетенций педагога ПОО, использованию современных цифровых технологий в образовательном процессе, а также представлена модель обеспечения информационной безопасности студентов в условиях функционирования цифровой образовательной среды.

Методические рекомендации содержат список основных терминов (гlossарий), которые необходимы для изучения данной проблемы, а также библиографический список.

1. Особенности проектирования и функционирования цифровой образовательной среды в информационном пространстве организаций среднего профессионального образования

Проектирование цифровой образовательной среды в профессиональной образовательной организации (далее – ПОО) – насущная необходимость, поскольку ПОО несет особую миссию, которая заключается в подготовке всесторонне развитого выпускника, обладающего необходимым набором компетенций и компетентностей, готового к работе или продолжению образования в высокоразвитом информационном обществе.

Цифровая образовательная среда ПОО (далее – ЦОС) предполагает набор ИКТ-инструментов, использование которых должно носить системный порядок и удовлетворять требованиям ФГОС к формированию условий реализации основной образовательной программы профессионального и среднего общего образования, способствует овладению обучающимися планируемых личностных, метапредметных, предметных результатов обучения, а также способствует развитию общих и профессиональных компетенций [3].

Кроме того, цифровая образовательная среда ПОО должна стать единым пространством коммуникации для всех участников образовательных отношений, действенным инструментом управления качеством реализации образовательных программ, работой педагогического коллектива.

Таким образом, цифровая образовательная среда профессиональной образовательной организации (ЦОС ПОО) – это управляемая и динамично развивающаяся с учетом современных тенденций модернизации образования система эффективного и комфортного предоставления информационных и коммуникационных услуг, цифровых инструментов объектам процесса обучения.

Согласно требованиям федеральных государственных образовательных стандартов к условиям реализации образовательной программы, ЦОС ПОО включает в себя:

- эффективное управление ПОО с использованием современных цифровых инструментов, современных механизмов финансирования;
- информационно-библиотечные центры с рабочими зонами, оборудованными читальными залами и книгохранилищами, обеспечивающими сохранность книжного фонда, медиатекой;
- размещение продуктов познавательной, учебно-исследовательской и проектной деятельности обучающихся в информационно-образовательной среде ПОО;
- проектирование и организацию индивидуальной и групповой деятельности, организацию своего времени с использованием ИКТ;
- планирование учебного процесса, фиксирование его реализации в целом и отдельных этапов (выступлений, дискуссий, экспериментов);
- обеспечение доступа в библиотеке к информационным ресурсам сети Интернет, учебной и художественной литературе, коллекциям медиаресурсов на электронных носителях, к множительной технике для тиражирования учебных и методических тексто-графических и аудио-видеоматериалов, результатов творческой, научно-исследовательской и проектной деятельности обучающихся;
- планирование учебного процесса, фиксацию его динамики, промежуточных и итоговых результатов [1].

Исходя из этого ЦОС ПОО – это комплекс информационных образовательных ресурсов, в том числе цифровые образовательные ресурсы, совокупность технологических средств информационных и коммуникационных технологий: компьютеры, иное ИКТ-оборудование, коммуникационные каналы, систему современных педагогических технологий, обеспечивающих обучение в современной информационно-образовательной среде.

Основными структурными компонентам ЦОС ПОО в соответствии с требованиями ФГОС являются:

- техническое обеспечение;
- программные инструменты;
- обеспечение технической, методической и организационной поддержки;
- отображение образовательного процесса в информационной среде;
- компоненты на бумажных носителях;
- компоненты на флеш-картах.

ЦОС ПОО должна обеспечить решение следующих задач:

- информационно-методическую поддержку образовательного процесса;
- планирование образовательного процесса и его ресурсного обеспечения;
- мониторинг и фиксацию хода и результатов образовательного процесса;
- современные процедуры создания, поиска, сбора, анализа, обработки, хранения и представления информации;
- дистанционное взаимодействие всех участников образовательного процесса (обучающихся, их родителей (законных представителей), педагогических работников, органов управления в сфере образования, общественности, базовые предприятия), в том числе в рамках дистанционного образования;
- дистанционное взаимодействие ПОО с другими организациями социальной сферы: учреждениями дополнительного образования детей, учреждениями культуры, здравоохранения, спорта, досуга, службами занятости населения, обеспечения безопасности жизнедеятельности [5].

Формирование ЦОС в каждой ПОО – процесс уникальный и должен учитывать множество факторов. При формировании ЦОС в ПОО следует принять во внимание ряд ключевых аспектов:

- уровень сформированности ИКТ-компетенции педагогов ПОО;
- возможности внедрения информационных и коммуникационных технологий в практику преподавания всех учебных дисциплин, междисциплинарных курсов, учебной и производственной практики;
- возможности внедрения информационных и коммуникационных технологий в деятельность воспитательной службы ПОО и служб сопровождения;
- обеспеченность ПОО необходимым оборудованием;
- условия для практического применения компьютерной техники и иных цифровых инструментов всеми участниками образовательных отношений;
- возможность открытого доступа к информационным каналам локальной внутренней сети, глобальной сети Интернет и к ресурсам медиатек;
- непрерывность развития технической инфраструктуры цифровой образовательной среды [12].

В процессе формирования цифровой образовательной среды ПОО можно выделить несколько этапов:

1. Организационный этап:

- Производится оценка соответствия имеющейся материально-технической базы требованиям ФГОС.
- Планирование пополнения материально-технической базы.
- Планирование обучения коллектива ПОО.
- Анализ уровня ИКТ-компетентности педагогов.
- Разработка локальных актов.
- Выбор программного обеспечения для формирования ЦОС наиболее подходящего для данных условий.

2. Этап формирования ЦОС:

- Создание службы методического и технического сопровождения ЦОС.

- Формирование материально-технической базы.
- Обучение персонала.
- Формирование единого информационного пространства в ПОО.
- Обеспечение информационной безопасности в ЦОС ПОО.
- Привлечение родителей и обучающихся к работе с отдельными компонентами ЦОС ПОО.

3. Аналитический этап:

- Оценка соответствия сформированной ЦОС требованиям ФГОС.
- Внесение изменений в функционирование ЦОС.

При выборе программного обеспечения для формирования ЦОС ПОО и разработке локальных актов, регламентирующих ее работу, необходимо руководствоваться нормативно правовыми актами Правительства РФ и Министерства просвещения РФ, принятым по данному вопросу.

Исходя из экономической целесообразности, а также во исполнение Указа Президента РФ «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» от 7 мая 2018 г. № 204, можно сделать вывод о том, что в основу функционирования цифровой образовательной среды ПОО следует положить работу со свободно-распространяемым и отечественным программным обеспечением.

На основе требований федеральных государственных образовательных стандартов и учета специфики работы ПОО можно выделить основные компоненты ЦОС, представленные в таблице 1.

Таблица 1 – Основные компоненты цифровой образовательной среды профессиональной образовательной организации в соответствии с требованиями ФГОС

№ п/п	Основные компоненты	Удовлетворение требованиям ФГОС
1.	Официальный сайт колледжа	Обеспечивает информационно-методическую поддержку образовательного процесса.
2.	Электронная почта	Обеспечивает информационно-методическую поддержку образовательного процесса.
3.	Электронный журнал	Обеспечивает планирование образовательного процесса и

		его ресурсного обеспечения, мониторинг и фиксацию хода и результатов образовательного процесса.
4.	Электронный календарь	Обеспечивает планирование образовательного процесса и его ресурсного обеспечения.
5.	Система электронного документооборота	Обеспечивает современные процедуры создания, поиска, сбора, анализа, обработки, хранения и представления информации.
5.	Система дистанционного обучения для студентов	Обеспечивает дистанционное взаимодействие всех участников образовательного процесса (обучающихся, их родителей (законных представителей), педагогических работников, органов управления в сфере образования, общественности), в том числе, в рамках дистанционного образования.
6.	Корпоративный портал	Обеспечивает формирование ИКТ-компетенции педагогов образовательной организации.
7.	Система поддержки пользователей компьютерной техники	Обеспечивает условия для практического применения компьютерной техники участниками образовательного процесса.

Важным критерием при формировании ЦОС является доступ ко всем сервисам через браузер и мультиплатформенность используемых инструментов, что обеспечивает гибкость настройки, мобильность и удобство в работы для всех участников образовательного процесса.

Формирование цифровой образовательной среды образовательной организации позволит обеспечить модернизацию образовательного процесса, внедрить в педагогическую практику технологии электронного обучения, модели смешанного обучения, автоматизирует процессы управления качеством образования, формирование у студентов навыков обучения в цифровом мире, умению создавать цифровые проекты для своей будущей профессии, присутствие в образовательной организации в сети Интернет [17].

Рассмотрим особенности создания цифровой образовательной среды в профессиональной образовательной организации среднего профессионального образования на примере технологии функционирования автоматизированной системы управления (далее – АСУ) «ProCollege».

Процесс создания цифровой образовательной среды можно начать с внедрения АСУ «ProCollege», являющейся «сердцем» всей цифровой

образовательной среды. АСУ «ProCollege» предназначена для управления образовательным процессом по всем реализуемым профессиональной образовательной организацией СПО образовательным программам и всем формам обучения. Разработанная система выполняет задачи по автоматизации деятельности каждого структурного подразделения и всех процессов профессиональной образовательной организации (далее – ПОО). На основании базы данных АСУ формируются отчетные документы, ведется мониторинг образовательной деятельности ПОО.

АСУ «ProCollege» включает в себя несколько модулей. Модули обеспечивают все уровни управления развитием образовательного учреждения на основе сбора и обработки административной и педагогической информации с использованием различных баз данных, а именно:

1. Сопровождение приемной кампании в соответствии с требованиями законодательства РФ;
2. Автоматический сбор и распределение документации отчетного характера;
3. Учет и управление кадрами, сбор и хранение актуальных сведений о сотрудниках;
4. Формирование актуального расписания занятий;
5. Планирование и администрирование образовательного процесса, в т.ч. планирование и своевременный учет учебной нагрузки, мониторинг выполнения учебных планов;
6. Информационное сопровождение деятельности структурных подразделений (учебной части, учебных отделений и др.);
7. Формирование личных дел обучающихся;
8. Хранение статистических данных о результатах обучения; учебных планах и др.;
9. Ввод дополнительных информационных полей по желанию администрации и т. д.

Кроме того, разработан модуль планирования и учета тарификации преподавателей; модуль формирования сводной ведомости по результатам освоения образовательной программы и печати дипломов об образовании; автоматизировано формирование календарного учебного графика; усовершенствованы модули, обеспечивающие электронный документооборот, формирование приказной документации, введены новые формы внутренней отчетности и форма отчета «СПО -1».

Необходимо отметить, что система реализует один из самых, по мнению исследователей, значимых факторов успешной информатизации образовательной деятельности – централизацию информационных запросов различного уровня.

Как правило, все сведения, необходимые для составления ответа на любой информационный запрос, в том числе из сторонней организации, предусмотрены структурой баз данных, однако даже в тех организациях, где эти сведения были введены, отчеты часто формируются и заполняются «вручную». Это объясняется тем, что для автоматического формирования отчета должна быть запрограммирована конкретная заданная запрашивающей организацией форма обработки и вывода данных. Разработчики системы предусмотрели формы отчетности, принятые на уровне Челябинской области.

АСУ «ProCollege» интегрирована с MS MOODLE. Наполнение и корректировка образовательного контента с внедрением новых инструментов, формирование новых и модернизация разработанных в 2011-2012 уч.г. модулей происходит непрерывно, отвечая изменениям в региональной системе профессионального образования, запросам и потребностям образовательной организации, и соответствует требованиям настоящего этапа развития системы среднего профессионального образования.

Эффективное взаимодействие пользователей системы реализуется за счет коммуникативного сервиса: чат, форум. Сервисное обслуживание

пользователей реализовано посредством системы поддержки (горячей линии).

Информационная система включается в цифровую образовательную среду, которая требует модернизации рабочих мест преподавателей, мастеров производственного обучения, тьюторов, оснащения ноутбуками, интерактивными досками, мультимедийными проекторами. Высокотехнологичным оборудованием на базе компьютерной техники и стабильным выходом в сеть Интернет должны быть оборудованы не только кабинеты, но и мастерские и учебно-производственные полигоны. Должна быть создана библиотека электронных ресурсов на определенное количество посадочных мест, позволяющая обучающимся работать с информационными электронными ресурсами не только ПОО, но и ресурсами электронных библиотек, ресурсами всемирной сети Интернет, специализированным программным обеспечением.

Важной составляющей цифровой образовательной среды являются специализированные сервисные структуры: базовые кафедры и ресурсные информационно-методические центры. Базовые кафедры – это структурные подразделения ПОО, территориально расположенные на производственных базах бизнес-партнеров, оснащенные техническими средствами доступа к АСУ ПОО, с установленным специализированным программным обеспечением и специально подготовленными тьюторами, осуществляющими техническое и методическое сопровождение обучения. На базовых кафедрах реализуется электронное обучение для сотрудников предприятия и практическая подготовка обучающихся ПОО с использованием ресурсов предприятия (в т. ч. электронных).

Для эффективного функционирования цифровой образовательной среды необходимо организовать повышение квалификации педагогических работников и тьюторов, направленное на формирование умений использования всех инструментов автоматизированной системы управления и организации тьюторского сопровождения обучающихся.

Примерная дорожная карта разработки и запуска цифровой образовательной среды:

1) создание рабочей группы разработки и запуска цифровой образовательной среды;

2) разработка модели цифровой образовательной среды профессиональной образовательной организации;

3) модернизация компьютерной техники и обновление программного обеспечения, в т.ч. антивирусного, мониторинг состояния локальных сетей, серверов, точек доступа к сети;

4) создание информационной системы;

5) формирование нормативной базы использования цифровой образовательной среды;

6) создание сети специализированных сервисных структур – базовых кафедр и ресурсных информационно-методических центров;

7) распределение полномочий пользователей системы;

8) обучение специалистов структурных подразделений, педагогических работников и тьюторов навыкам работы в АСУ;

10) наполнение автоматизированной системы управления нормативным и образовательным контентом;

11) тестовый запуск системы, выявление и устранение проблем в ее функционировании;

12) разработка инструкций для обучающихся по использованию системы;

13) запуск системы в рабочий режим;

14) разработка критериев и показателей эффективности функционирования цифровой образовательной среды.

Таким образом, нормативное обеспечение ЦОС может включать следующие положения ПОО:

- реализация электронного обучения;
- положение о базовой кафедре;

- положение о ресурсном информационно-методическом центре и др.

2. Мероприятия по проектированию модели цифровой образовательной среды профессиональной образовательной организации

В рамках реализации инновационной деятельности по теме «Формирование современной цифровой образовательной среды образовательной организации» в ГБПОУ «Миасский педагогический колледж» разработан проект структуры цифровой образовательной среды.

В соответствии с Паспортом национального проекта «Образование» под цифровой образовательной средой понимается цифровое пространство, позволяющее:

- конструировать и реализовывать индивидуальные учебные планы (программы), в том числе с зачетом результатов обучения по онлайн-курсам;
- автоматизировать административные, управленческие и организационные процессы; проводить процедуры оценки качества образования;
- перевести отчетность образовательной организации в цифровой формат;
- обеспечить возможность организации электронного, смешанного и дистанционного обучения;
- формировать профили «цифровых компетенций» участников образовательных отношений.

Исходя из этого, проект модели ЦОС ГБПОУ «Миасский педагогический колледж» включает в себя следующие компоненты:

Таблица 2 – Основные компоненты цифровой образовательной среды профессиональной ГБПОУ «Миасский педагогический колледж»

№ п/п	Компонент ЦОС	Назначение компонента ЦОС
1.	Корпоративная электронная почта	Обеспечивает вход в цифровое пространство колледжа, доступ к виртуальным чат-комнатам, электронным классам, сетевому сообществу, совместному доступу при работе с документами,

		виртуальной учительской и другим компонентам цифрового пространства. Аккаунт в корпоративной почте имеет каждый участник образовательных отношений.
2.	Виртуальные чат-комнаты: – Коллектив – Администрация – Экспериментальная площадка – Руководители МО – Служба АХР – Классные руководители – Служба сопровождения	Виртуальные тематические комнаты по направлениям деятельности образовательной организации созданы для решения локализованных во времени проблем, организации оперативной работы с документами, иными материалами, проведения оперативных обсуждений решаемых управленческих задач.
3.	Система видеоконференцсвязи (https://bigbluebutton.ru/ - бесплатная вебинарная комната на своем сервере)	Цифровой инструмент предназначен для проведения видеовстреч (совещаний, заседаний методических объединений, классных родительских собраний, дистанционных уроков с обучающимися)
4.	Учебные календари в АИС «Сетевой город» Модуль ПОО (https://poo.edu-74.ru/plan/#/calendars)	Обеспечивает планирование образовательного процесса и его ресурсного обеспечения.
5.	Система электронного документооборота, встроенная в АСУ «ProCollege»	Обеспечивает современные процедуры создания, поиска, сбора, анализа, обработки, хранения и представления информации.
5.	Система дистанционного обучения для студентов на базе АСУ «ProCollege»	Обеспечивает дистанционное взаимодействие участников образовательного процесса, представляет возможность создания электронных курсов, включающих все элементы образовательного процесса.
6.	Электронный журнал в АИС «Сетевой город» Модуль ПОО (https://poo.edu-74.ru)	Обеспечивает планирование образовательного процесса и его ресурсного обеспечения, мониторинг и фиксацию хода и результатов образовательного процесса.
7.	Система поддержки пользователей компьютерной техники: – техподдержка АСУ «ProCollege»; – техподдержка АИС «Сетевой город» Модуль ПОО; – консультации специалиста по ИБ; – консультации системного администратора.	Обеспечивает условия для практического применения компьютерной техники участниками образовательного процесса.
8.	Официальный сайт ГБПОУ «Миасский педагогический колледж» (http://miasspk.ru/)	Обеспечивает информационную открытость образовательной деятельности
9.	Электронная библиотечная система «Юрайт»	Обеспечивает электронными и печатными учебниками, включает виртуальный читальный

	(https://urait.ru/)	зал.
10.	Система оценки / мониторинга качества образования (https://i-exam.ru/)	Обеспечивает оценку уровня фундаментальной и психологической подготовки первокурсников к продолжению обучения; подготовку к процедурам промежуточного, итогового контроля и процедурам внешней независимой оценки качества образования.

Проектируемая цифровая образовательная среда ГБПОУ «Миасский педагогический колледж» является единым пространством для взаимодействия и коммуникации всех участников образовательных отношений.

Наглядно проект модели цифровой образовательной среды колледжа можно представить на рисунке 1.

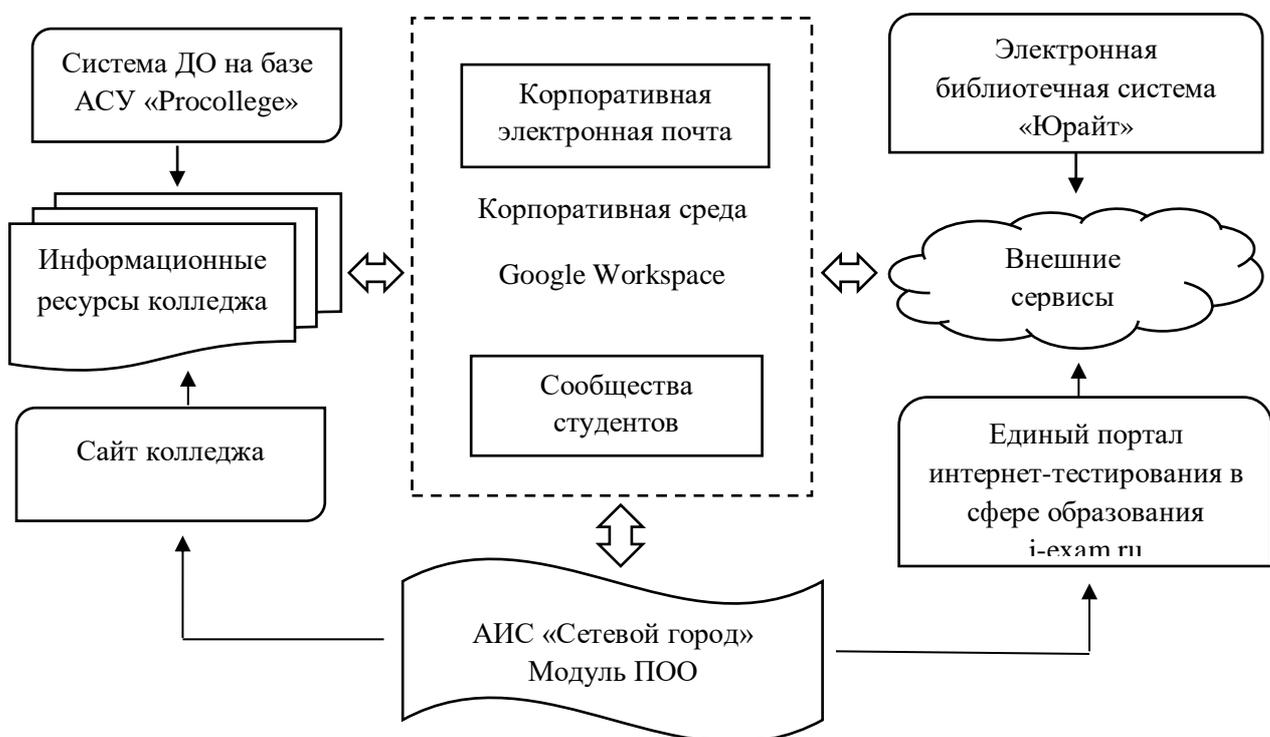


Рисунок 1 – Проект модели цифровой образовательной среды ГБПОУ «Миасский педагогический колледж»

Таким образом, модель цифровой образовательной среды ГБПОУ «Миасский педагогический колледж» является гибкой, открытой к модернизации имеющихся компонентов и дополнению новыми элементами.

3. Меры по совершенствованию осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в цифровой образовательной среде

В настоящее время в Российской Федерации реализуется ряд инициатив, направленных на создание необходимых условий для развития цифровой экономики, что в свою очередь повышает конкурентоспособность страны, качество жизни граждан, обеспечивает экономический рост и национальный суверенитет. Первостепенное значение имеет «Стратегия развития информационного общества в Российской Федерации на 2017- 2030 годы». Приоритетным проектом является «Современная цифровая образовательная среда в Российской Федерации» в рамках реализации государственной программы «Развитие образования». Проект нацелен на создание возможностей для получения качественного образования гражданами разного возраста и социального положения с использованием современных информационных технологий [13].

Процесс информатизации современного общества сопровождается и существенными изменениями в педагогике, связанных с внесением корректив в содержание технологий обучения. Последние должны быть адекватны современным техническим возможностям и способствовать гармоничному вхождению человека в информационное общество. Использование современных информационных технологий является необходимым условием развития более эффективных подходов к обучению и совершенствованию методики преподавания. Особую роль в этом процессе играют информационные технологии, по причине того, что их применение способствует повышению мотивации обучающихся, экономии учебного времени, а интерактивность и наглядность способствует лучшему представлению, пониманию и усвоению учебного материала.

Основные педагогические цели информационных технологий на занятиях состоят в:

- развитии личности обучающегося, включающее в себя: развитие творческого, конструктивно-поискового мышления, развитие коммуникативных способностей;
- развитию умения принимать неординарные решения в сложных ролевых ситуациях;
- совершенствовании навыков исследовательской деятельности.

Направлениями применения информационных технологий в образовательном процессе это не только разработка педагогических программных средств различного назначения: обучающие, диагностирующие, контролирующие, моделирующие, тренажеры, игровые, а также и разработка web-сайтов учебного назначения, разработка методических и дидактических материалов, осуществление управления реальными объектами (учебными ботами), организация и проведение компьютерных экспериментов с виртуальными моделями, и многое другое.

При использовании информационных технологий необходимо стремиться к реализации всех потенциалов личности – познавательного, морально-нравственного, творческого, коммуникативного и эстетического. Наиболее широко в данный момент используются интегрированные уроки с применением мультимедийных средств. Обучающие презентации становятся неотъемлемой частью обучения, но это лишь простейший пример применения АСУ. В последнее время педагоги создают и внедряют авторские педагогические программные средства, в которых отражается некоторая предметная область, в той или иной мере реализуется технология её изучения, обеспечиваются условия для осуществления различных видов учебной деятельности. Чтобы эти потенциалы были реализованы на достаточно высоком уровне, необходима педагогическая компетентность в области владения информационными образовательными технологиями (далее – ИКТ-компетентность) [15].

Профессиональная ИКТ-компетентность педагога основана на Рекомендациях ЮНЕСКО «Структура ИКТ-компетентности учителей»,

присутствует во всех компонентах профессионального стандарта педагога и определена в Приложении №1 Профессионального стандарта педагога как «квалифицированное использование общераспространенных в данной профессиональной области в развитых странах средств ИКТ при решении профессиональных задач там, где нужно и тогда, когда нужно».

Педагог, использующий ИКТ в своей профессиональной деятельности, обязан быть ИКТ-компетентным.

ИКТ-компетентность педагога включает в себя три компонента:

1. Общепользовательский компонент;
2. Общепедагогический компонент;
3. Предметно-педагогический компонент.

Остановимся кратко на каждом из этих компонентов.

Общепользовательская ИКТ-компетентность включает в себя пользовательские навыки, в том числе использование видео-фотосъемки, умение использования систем мгновенных сообщений, навыки поиска в сети Интернет и базах данных с соблюдением этических и правовых норм использования ИКТ.

Общепедагогическая ИКТ-компетентность связана с глубокой перестройкой методики обучения и содержания образования: применение информационных технологий для разных форм образовательной деятельности: индивидуальной, групповой, коллективной; планирование проектной деятельности с учетом возможностей ИКТ; использование доступных ресурсов Интернета; использование интерактивных моделей, виртуальных лабораторий; использование дистанционных ресурсов при подготовке домашних заданий; подготовка заданий и тестов в электронном виде; привлечение обучающихся к активному участию в образовательном процессе (в АСУ). Немаловажным является задача педагога – привлечение обучающихся к активному участию в образовательном процессе, используя для этого современные средства коммуникаций: электронную почту, форум, Skype и т. п.

Предметно-педагогическая ИКТ-компетентность соответствует области деятельности и определена следующим образом: преподавателю необходимо владеть расширенными приемами самостоятельной подготовки дидактических материалов и рабочих документов, что позволит запланировать и организовать комплексное использование средств ИКТ в образовательном процессе [15].

Таким образом, в приведенном стандарте требования к ИКТ-компетенциям преподавателя можно условно разделить на два уровня – технологический и методический. К первому следует отнести позиции, в которых предусматривается пользовательское владение информационными технологиями. Второй уровень требований – методический – предполагает владение преподавателем методами применения ИКТ в учебной и воспитательной работе с обучающимися.

Оптимальная модель достижения педагогом профессиональной ИКТ-компетентности обеспечивается сочетанием следующих факторов:

- наличие действующего Федерального государственного образовательного стандарта (любой ступени образования);
- наличие достаточной технологической базы (требование ФГОС): широкополосный канал-интернет, постоянный доступ к мобильному компьютеру, инструментарий автоматизированной системы управления, установленный в ПОО;
- наличие потребности у педагога и установки администрации ПОО на действительную реализацию ФГОС, принятие локальных нормативных актов о работе коллектива образовательной организации в АСУ;
- начальное освоение педагогом базовой ИКТ-компетентности в системе повышения квалификации с аттестацией путем экспертной оценки его деятельности в АСУ ПОО.
- самообразование педагога в области ИКТ-компетентности [15].

Развитию всех компонентов ИКТ-компетентности педагога будет способствовать организация курсов повышения квалификации. Программа

повышения квалификации педагогов по вопросам обеспечения информационной безопасности в условиях функционирования цифровой образовательной среды ПОО представлена в приложении 3.

Таким образом, урок (занятие) как основная форма организации обучения – это то место, где сходятся результаты долгих дидактических и методических поисков, где происходит встреча субъектов, в результате которой каждый из них меняется, приобретая что-то новое. В информационно-образовательной среде уроки (занятия) приобретают свои особенности: изменяется позиция педагога на уроке, учебный процесс индивидуализируется, в связи с чем активизируется познавательная деятельность обучающихся, возможность сочетания различных форм познавательной деятельности вне рамок одной ПОО, совместная интерактивная деятельность не только педагогов и специалистов в различных областях знаний с целью повышения научного уровня урока, но и учебный диалог между удаленными группами обучающихся, использование баз данных и лабораторных комплексов с удаленным доступом. Все это требует от педагога высокого уровня владения ИКТ, а движущийся вперед научно-технический прогресс побуждает постоянно совершенствоваться в этом направлении.

4. Меры по обеспечению информационной безопасности студентов в условиях функционирования цифровой образовательной среды

Цифровая образовательная среда профессиональной образовательной организации, как и любая другая информационная среда подвержена различным негативным влияниям внешнего и внутреннего характера. В связи с этим становится важным рассмотреть подходы к формированию модели информационной безопасности несовершеннолетнего студента, как важнейшей составляющей инфобезопасной среды образовательного учреждения.

Проанализировав научно-методическую литературу, классификации, факторы, риски и угрозы информационной безопасности обучающихся на основе выше сформулированных понятий была построена модель обеспечения комплексной информационной безопасности несовершеннолетних студентов. Данная модель представлена на рисунке 2.



Рисунок 2 – Модель обеспечения информационной безопасности студентов

Целью и результатом реализации данной модели является формирование информационно-безопасной личности выпускника. Объектом информационной безопасности является личная информационная среда студента.

На рисунке 2 представлены внутренние и внешние угрозы информационной безопасности несовершеннолетних студентов – совокупность факторов и условий, возникающих в процессе взаимодействия объекта безопасности с другими объектами (субъектами). Информационные опасности современных школьников – негативное проявление перехода к информационному обществу, формирующееся под воздействием вышеуказанных информационных угроз и рисков, которым современный обучающийся должен уметь противостоять, организовывая свою образовательную деятельность и др.

Не менее важным вопросом является определение субъектов информационной безопасности, то есть тех, кто влияет на информационную безопасность студентов и несет ответственность за ее обеспечение. В данной модели определены следующие субъекты: государство, общество, открытые информационные ресурсы (СМИ, Интернет), родители, близкие и родные, сверстники и педагоги. Данные субъекты могут быть источниками как внешних, так и внутренних угроз [9].

Рассматривая внешние и внутренние угрозы более подробно. Необходимо отметить, что на личность несовершеннолетнего в современном информационном обществе воздействует мощный информационный поток, представленный в виде всей информации, которую он получает. И если информация, предлагаемая родными и педагогами чаще является трансформированной под возрастные и психофизиологические особенности обучающегося, то информация получаемая несовершеннолетними студентами из внешней среды (телевидение, интернет, печатная пресса, фото и видео, информационные службы) предлагается им в первоначальном виде, и может негативно влиять на него в большей или меньшей степени в

зависимости от личностных характеристик. Наиболее явные внешние и внутренние угрозы представлены на рисунке 2.

Для обеспечения информационной безопасности, необходимо осуществлять комплексный подход, включающий следующие мероприятия: правовое обеспечение информационной безопасности, нравственный и этический контроль, защита психики и здоровья несовершеннолетнего, воспитательные меры по обеспечению ИБ, техническое и программное обеспечение ИБ, образование в области информационной безопасности, формирование информационной культуры студентов. Рассмотрим их более подробно.

8. Правовое обеспечение информационной безопасности – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту личной информационной среды несовершеннолетнего на законодательной и правовой основе для реализации единой государственной политики в сфере защиты детей от информации, причиняющей вред их здоровью и развитию. К актуальным нормативным документам в данной области относятся следующие:

- Письмо Минобрнауки России от 14.05.2018 № 08-1184 «О направлении информации» вместе с «Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении использовании сети «Интернет»).
- Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.07.2018) «О защите детей от информации, причиняющей вред их здоровью и развитию».
- Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред

здоровью и (или) развитию детей, а также не соответствующей задачам образования.

- Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) «О персональных данных»

9. Нравственный и этический контроль подразумевает соблюдение обучающимися при осуществлении информационной деятельности норм и правил поведения в обществе, а также сетевой культуры и этики, которые складываются по мере распространения информационных технологий в современном информационном обществе.

10. Защита психики и здоровья несовершеннолетнего – меры направлены на актуализацию потребности студентов в хорошем здоровье, физическом благополучии, как средств достижения жизненно важных ценностей, снижение и профилактика компьютерной и Интернет-зависимости среди обучающихся, педагогическая и психологическая помощь в вопросах уменьшения информационных опасностей в жизнедеятельности. Мероприятия по осуществлению нравственного и эстетического контроля, а также по защите психики и здоровья несовершеннолетнего должны включать ознакомительную работу с документами:

- Методические рекомендации по ограничению в образовательной организации доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования
- Памятка для обучающихся об информационной безопасности детей.

Кроме того, необходимо организовать работу по вовлечению студентов во всероссийские акции и мероприятия, направленные на овладение сетевой культурой и этикой, а также защиту психики и здоровья несовершеннолетнего:

- Всероссийская добровольная просветительская интернет-акция «Безопасность детей в сети Интернет» (<https://xn--80aaempceic8avkdac8frhe.xn--p1ai/>).
- Мероприятиях, проводимых Экспертным советом по информатизации системы образования и воспитания в рамках Единого урока. Единый урок представляет собой цикл детских мероприятий, направленных на повышение уровня информационной безопасности, и способствует привлечению внимания родительской и педагогической общественности к проблеме обеспечения безопасности и развития детей в информационном пространстве (<https://www.xn--d1abkefqip0a2f.xn--p1ai/>).
- Федеральный проект «Цифровой Диктант». Цель проекта: мониторинг цифровой грамотности и вовлечение населения в реализацию мероприятий в рамках федерального проекта «Кадры для цифровой экономики». «Цифровой диктант» включает онлайн-тестирование на знание интернет-программ, ориентирование и использование интернет-сервисов, компьютерную грамотность, безопасность в интернете (<https://digitaldictation.ru/>).
- Всероссийской образовательной акции по информационным технологиям «ИТ - диктант». Цель акции - определение и повышение уровня цифровой грамотности населения. ИТ-диктант – это набор тестовых заданий разного уровня сложности, от основ работы с компьютерной техникой и навыков использования интернет-ресурсов до познаний в таких темах, как блокчейн и интернет вещей. Задача тестирования оценить уровень компетенций участников, владение базовыми и продвинутыми цифровыми навыками (<http://xn----8sblocmw8aec.xn--p1ai/>).

А также необходимо провести ряд классных часов с привлечением психолога и проведением анкетирования, направленного на выявление интернет-зависимости. Кроме того, организовать мероприятия по

профилактике компьютерной и Интернет-зависимости среди студентов, например, лекторий на тему: «Интернет-зависимость: мифы и реальность!», дискуссия «Интернет: за и против», «Альтернатива Интернету!» и другие.

11. Воспитательные меры по обеспечению ИБ – меры направленные на формирование культуры безопасности, ответственности за производимые действия в информационном пространстве, меры воспитания и укрепления духовно-нравственных ценностей, патриотизма.

В план воспитательной работы необходимо включить проведение серии медиауроков по теме: «Личная информационная безопасность в сети Интернет». Организовать участие студентов в акции «Урок НТИ» (<https://nti-lesson.ru/>). Через урок необходимо донести до каждого, как важно осваивать технологии будущего. Урок помогает понять, что в основе всех прорывных технологий лежат глубокие знания, в том числе в предметных областях. Данный урок может быть организован по различным направлениям:

- умный город;
- искусственный интеллект;
- технологии беспроводной связи;
- информационная безопасность и др.

Воспитательная меры по обеспечению ИБ могут включать серию мероприятий с привлечением интересных людей (специалистов) в области информационной безопасности.

12. Техническое и программное обеспечение ИБ – это использование различных технических и программных средств, препятствующих нанесению материального или морального ущерба личной информации, программы родительского контроля, технические средств защиты информации.

Для анализа системы защиты информационной системы колледжа необходимо провести анализ реализованных мер комплексной защиты с перечнем мер, предложенных «Лабораторией Касперского» для реализации комплексной программно-технической системы защиты информационных

систем компаний и организаций. Данный анализ позволит выявить и устранить недостатки в системе.

Особое внимание следует уделять контент-фильтрации с присвоением разных профилей фильтрации. Одним из таких средств является SkyDNS. SkyDNS – это программный продукт, позволяющий осуществлять высокоскоростную фильтрацию трафика в сети Интернет без ограничений по объему и полосе пропускания трафика. Контент-фильтр позволяет управлять доступом к онлайн-ресурсам, избавляет от ненужной и вредной информации в Сети. Программные продукты российской компании СкайДНС направлены на обеспечение контентной фильтрации интернета и безопасности пользователей от таких угроз как ботнет-сети, фишинговые, мошеннические и вредоносные интернет-ресурсы.

13. Образование в области информационной безопасности – реализация образовательных модулей в курсе общеобразовательных и общепрофессиональных дисциплин (ОБЖ, безопасность жизнедеятельности и др.), организация дополнительного образования обучающихся по информационной безопасности, повышение квалификации педагогического состава, проведение тематических родительских собраний и встреч с интересными людьми.

Для реализации данных мер необходимо включить разделы, посвящённые информационной и кибербезопасности в учебные дисциплины ОБЖ и безопасность жизнедеятельности, информатика, информатика и ИКТ в профессиональной деятельности [8]. Кроме того, в рамках сетевого взаимодействия с учреждениями дополнительного образования организовать реализацию дополнительной общеобразовательной, общеразвивающей программы «Цифровая гигиена и работа с большими данными».

В комплексе мер по управлению профессиональным образованием важной задачей является также подготовка и повышение квалификации персонала в системе внутрифирменного обучения персонала.

Сегодня информация управления персоналом должна быть автоматизированной частью цифровой платформы управления персоналом. Она должна обеспечивать руководителей анализом в режиме реального времени, сокращать время, затрачиваемое на отчеты и увеличивать время, которое они могут тратить на анализ данных и решение проблем.

В цифровую эпоху на помощь приходят системы автоматизации внутрифирменного обучения персонала, помогающие преподавателям корректировать содержание программ и учитывать все данные, полученные в результате управления эффективностью процесса обучения, внедрять новые цифровые учебные пособия и цифровые образовательные технологии. Для успешного применения на практике новой системы автоматизации внутрифирменного профессионального обучения персонала необходимо:

- составлять список перспективных и талантливых сотрудников, обучение которых станет эффективной инвестицией в будущий результат;
- ранжировать таких сотрудников на профильные группы и для каждой группы составить отдельный план профессионального обучения;
- выявлять преподавателей и инструкторов для проведения такого обучения;
- составить план новых функций и задач каждого сотрудника после обучения;
- сформировать цифровую образовательную среду;
- применять цифровые учебные пособия и цифровые образовательные технологии.

В ряде случаев целесообразно поводить не массовое, а «точечное» обучение, которое должны проходить конкретные сотрудники для освоения знаний, навыков, умений, общекультурных и профессиональных компетенций, а также компетенции в области использования цифровых образовательных технологий, необходимые им для успешной работы в новой

должности, или успешно выполнять дополнительные функции на прежней работе.

14. Формирование информационной культуры студентов – через образовательную и воспитательную среду колледжа, которая определяется как компонент базовой культуры личности и характеристики человека, позволяющей ему эффективно выполнять все виды работы с информацией, понимать природу информационных процессов и осуществлять информационную рефлексию без ущерба для себя и окружающих. Данные мероприятия могут быть реализованы через размещение стендов, посвященных информационной культуре на современном этапе развития общества, а также включать вышеописанную работу по образованию и воспитанию в области информационной безопасности.

Таким образом, реализация данных мероприятий в колледже может способствовать обеспечению информационной безопасности студентов.

5. Цифровые образовательные технологии в среднем профессиональном образовании

Цифровые технологии сегодня – это инструмент эффективной доставки информации и знаний до обучающихся, инструмент создания учебных материалов, инструмент эффективного способа преподавания, средство построения новой образовательной среды: развивающей и технологичной [17].

В настоящее время особую актуальность приобретают следующие цифровые технологии:

- технология совместных экспериментальных исследований педагога и обучающегося;
- технология «Виртуальная реальность»;
- технология «Панорамных изображений»;
- технология «3D-моделирование»;

- технология «Образовательная робототехника»;
- технология МСИ (использования малых средств информатизации); - мультимедийный учебный контент:
- интерактивный электронный контент.

Рассмотрим отдельные из них более подробно.

Технология «Малые средства информатизации» – это технологии, позволяющие обеспечить индивидуальное взаимодействие каждого обучающегося с информационными технологиями, где регулярное применение компьютеров недостижимо.

На применение технологии МСИ ориентированы стандарты, учебные программы и учебники.

Виды малых форм информатизации:

- графические калькуляторы;
- электронные словари;
- различные средства интерактивного опроса и контроля качества знаний.

Малые средства информатизации позволяют:

- значительно повысить качество и эффективность учебного процесса;
- более полно выполнить ФГОС СПО, особенно в области повышения практической направленности обучения;
- обеспечить более высокий балл на промежуточной аттестации по физике, химии, математике за счет применения разрешенного технического средства и умения ими пользоваться.

Преимущества малых форм информатизации:

- использование МСИ непосредственно в процессе освоения предметных знаний на основе дидактического диалога преподавателя и студентов;
- мобильность;
- компактность;
- энергонезависимость.

В практике работы педагогов можно использовать такие технологии, как интерактивный электронный контент и мультимедийный учебный контент.

Интерактивный электронный контент – это контент, обладающий возможностями установления различных форм интерактивного взаимодействия пользователя с электронным образовательным контентом: манипулирование экранными объектами, линейная навигация, обратная связь, конструктивное взаимодействие, рефлексивное взаимодействие, имитационное моделирование и т.д.

Мультимедийный учебный контент – это контент, представляющий собой синтез различных видов информации (текстовой, графической, анимационной, звуковой и видео), при котором возможны различные способы ее структурирования, интегрирования и представления.

С увеличением количества интерактивного оборудования в системе образования, возможности преподавателя в представлении информации для обучающихся значительно увеличились. Интерактивная доска позволяет создавать виртуальные объекты с различными видами информации. Поэтому доступнее применять различную наглядность в обучении, а, значит, при мотивации изучаемой темы не только описывать события устно, но и демонстрировать их в другом формате осмысления. Использование интерактивных элементов повышает интерес к обучению своей необычностью, нестандартностью, возможностью взаимодействия с виртуальной средой обучения.

Интерактивная доска не просто отображает то, что происходит на компьютере, а позволяет управлять процессом презентации, вносить поправки и коррективы, делать цветом пометки и комментарии, сохранять материалы урока для дальнейшего использования и редактирования. При этом преподаватель не привязывается к своему компьютеру и не теряет визуального контакта с обучающимися. Благодаря наглядности и интерактивности группа вовлекается в активную работу.

Тесты, созданные в оболочке MyTestX, можно использовать как задания открытого вида, так и закрытого; варианты ответов с однозначным и многозначным выбором; установление истинности и ложности утверждения; ввод ответа числового и буквенного; перестановка букв в слове; задания на соответствие; установление порядка действия; настраиваемая шкала оценивания; контроль за временем; случайный порядок вопросов и ответов (что исключает списывание); ввод символов – вот преимущества этой оболочки.

HotPotatoes – инструментальная программа-оболочка, предоставляющая преподавателям возможность самостоятельно создавать интерактивные задания и тесты для контроля и самоконтроля обучающихся. С помощью программы можно создать 10 типов упражнений и тестов по различным дисциплинам с использованием текстовой, графической, аудио- и видеоинформации.

Особенностью этой программы является то, что созданные задания сохраняются в стандартном формате веб-страницы: для их использования обучающимся необходим только веб-браузер, им не нужна программа HotPotatoes, она требуется только преподавателям для создания и редактирования упражнений.

В состав HotPotatoes входят 5 блоков программ для составления заданий и тестов разных видов. Каждый блок может быть использован как самостоятельная программа.

Для эффективного использования информационных технологий преподавателю необходимо следить за существующими и вновь появляющимися компьютерными средствами обучения. Он должен уметь комбинировать эти средства в зависимости от объема и сложности материала, работать самостоятельно и отбирать программные средства, которые обеспечат подачу нового материала в оптимальной форме, а также создавать собственные дидактические материалы и работать с различными программами. На сегодняшний день, нет необходимости обсуждать, нужна

или не нужна цифровизация образования. Очевидно, что в ближайшем будущем умение преподавателя пользоваться цифровыми инструментами в учебном процессе станет обязательным элементом его профессиональной компетенции.

Технология «Web-квест» (webquest) в педагогике – проблемное задание, проект с использованием интернет-ресурсов.

Вебквест – сценарий организации проектной деятельности обучающихся по любой теме.

Технология веб-квеста способствует повышению качества обучения, так как влияет не только на внешнюю, но и внутреннюю мотивацию. Данная технология позволяет установить тесное сотрудничество с обучающимися, повышает мотивацию к учению, развивает практически все учебные универсальные действия.

Существует определенная последовательность выполнения веб-квеста. Работа выполняется по следующей схеме:

1. Введение. Введение содержит вопрос, над которым и будут размышлять обучающиеся, то есть проблему.
2. Задание. Это исследовательская часть, так как задание должно заставлять обучающихся на основании фактов смотреть дальше, изучая взаимосвязь предметов и событий, отделяя истинные знания от ложных.
3. Процесс. Пошаговое описание процедуры того, что обучающиеся должны сделать для реализации проекта; здесь также приводится список web-сайтов, на которых содержится необходимая информация.
4. Оценка. В этой части приводятся критерии оценки работы обучающихся.
5. Заключение. Подведение итогов проектной деятельности.

Формирование универсальных учебных действий может происходить на всех этапах работы над веб-квестом. Развивается одна из социально – значимых компетентностей – информационная компетентность. Хороший результат дает данный вид деятельности при подготовке к олимпиадам.

Реальное размещение веб-квестов в сети в виде web-сайтов, созданных самими обучающимися, позволяет значительно повысить их мотивацию на достижение наилучших учебных результатов.

Участие в веб-квесте позволяет смоделировать, проиграть ситуацию, которая вскоре может возникнуть в самостоятельной жизни, подготовиться к ней. Обучающийся вместе со своим персонажем учится ориентироваться в различных обстоятельствах, давая объективную оценку своему поведению, учитывая возможности других людей, устанавливая с ними контакты и влияя на их интересы.

В настоящее время в различных сферах деятельности ощущается нехватка специалистов, способных самостоятельно и в команде решать возникающие проблемы, делать это с помощью Интернета. Поэтому работа обучающихся в таком варианте проектной деятельности, как веб-квест, разнообразит учебный процесс, сделает его живым и интересным. А полученный опыт принесет свои плоды в будущем, потому что при работе над этим проектом развивается ряд компетенций:

- использование информационных технологий для решения профессиональных задач (в т.ч. для поиска необходимой информации, оформления результатов работы в виде компьютерных презентаций, веб-сайтов, флеш-роликов, баз данных и т.д.);
- самообучение и самоорганизация;
- работа в команде (планирование, распределение функций, взаимопомощь, взаимоконтроль);
- умение находить несколько способов решений проблемной ситуации, определять наиболее рациональный вариант, обосновывать свой выбор;
- навык публичных выступлений (обязательно проведение предзащит и защит проектов с выступлениями авторов, с вопросами, дискуссиями).

Приведем примеры нескольких крупных и интересных проектов, которые могут применяться для реализации цифровой образовательной среды

и электронного обучения в профессиональных образовательных организациях среднего профессионального образования.

Ведомственная целевая программа «*Российская электронная школа*» (<https://resh.edu.ru>) в рамках приоритетного проекта «Создание современной образовательной среды для школьников» определяет «...создание завершеного курса интерактивных видеоуроков по всей совокупности общеобразовательных учебных предметов, полностью соответствующего федеральным государственным образовательным стандартам и примерным основным образовательным программам начального общего, основного общего, среднего общего образования, учитывающего передовой опыт лучших учителей России и размещенного в открытом доступе в интересах всех обучающихся, в том числе детей с особыми образовательными потребностями и индивидуальными возможностями».

«Российская электронная школа» содержит интерактивные уроки по всему школьному курсу от лучших учителей страны, созданные для того, чтобы у каждого обучающегося была возможность получить бесплатное качественное общее образование.

Особого внимания заслуживает победитель Всероссийского конкурса «Школа навыков XXI века» образовательная среда «*Мобильное электронное образование*» (<https://mobedu.ru>). «МЭО» – система управления качеством образования, инструмент реализации ФГОС общего образования, учитывающая индивидуальные образовательные запросы и возможности каждого ребенка, включая детей с трудностями в обучении и ограниченными возможностями здоровья, обеспечивающая равенство и качество образовательной услуги.

Система разработана командой профессионалов, объединяющей разработчиков ФГОС общего образования и создателей первой в России аккредитованной дистанционной школы «Телешкола» (2001-2013 гг.). Система успешно прошла педагогическую и научную экспертизу в Российской академии наук, а также гигиеническую в ФГАО ННПЦЗД.

Система обладает интуитивно понятным интерфейсом, проста и удобна для работы и взаимодействия руководителей, педагогов, обучающихся и их родителей, обеспечивает реализацию индивидуальной образовательной траектории ребенка и включает:

- модульные основные образовательные программы уровней общего образования, разработанные с учетом примерных основных образовательных программ;
- онлайн-курсы по учебным предметам 1–11 классов, включая контент для обучения высокомотивированных и одаренных детей;
- контент для дошкольного образования (для детей 6-7 лет);
- контент для детей с ОВЗ по 5 адаптированным программам (1 класс);
- методические рекомендации и тематическое планирование для учителей по всем учебным предметам;
- средства интерактивного взаимодействия участников образовательных отношений;
- формирующую систему оценивания;
- возможность подготовки к ОГЭ и ЕГЭ;
- систему профессионального развития педагогов.

Комплексный проект «Одарённые и высокомотивированные дети» включает в себя материалы для подготовки к олимпиадам, интенсивные курсы, сборники межпредметных задач; сборники проектно-исследовательских заданий; курсы повышения квалификации для педагогов.

ЯКласс – образовательный интернет-ресурс для школьников, учителей и родителей. (www.yaklass.ru). Данный ресурс помогает учителю проводить тестирование знаний учащихся, задавать домашние задания в электронном виде. Использование элементов геймификации позволяет создавать рейтинги лидеров класса и школ, добавляет обучению элементы игры, которые стимулируют и школьников, и учителей. В основе ресурса лежит технология генерации огромного числа вариантов для каждого задания Genexis – тем

самым, проблема списывания решена раз и навсегда. Данный ресурс приобретает особую актуальность в процессе подготовки студентов по специальности «Преподавание в начальных классах».

Проект «Стемфорд» реализуется по инициативе Фонда инфраструктурных и образовательных программ в рамках отраслевой программы «Развитие системы электронного образования «e-Learning» на период до 2020 года. Проект направлен на раннюю профориентацию и популяризацию контента в области естественных наук и основ нанотехнологий для учащихся основной и старшей школы.

Цель проекта – дать возможность обучающимся получать знания о новейших разработках в области нанотехнологий и nanoиндустрии с использованием форм обучения, актуальных и интересных для современного подростка: работа в современной цифровой среде, общение с ведущими учёными, изучение реальных технологических решений и кейсов от инновационных компаний, компьютерная игра, выполнение исследовательского проекта, работа в команде.

Stepik – российская образовательная платформа и конструктор бесплатных открытых онлайн-курсов и уроков. Позволяет любому зарегистрированному пользователю создавать интерактивные обучающие уроки и онлайн-курсы, используя видео, тексты и разнообразные задачи с автоматической проверкой и моментальной обратной связью. В процессе обучающиеся могут вести обсуждения между собой и задавать вопросы преподавателю на форуме. Основные охватываемые курсами дисциплины – программирование, математика, биоинформатика и биология, экономика.

Глобальная школьная лаборатория «ГлобалЛаб» основанная на использовании новых технологий, прежде всего Интернет, поддерживающая преподавание любого естественно-научного курса. Одна из основных идей проекта заключается в том, что если обучающиеся в разных частях земного шара будут выполнять согласованные наблюдения и измерения по стандартному протоколу, а потом смогут сравнить и проанализировать

совместно полученные результаты, то вместо традиционного пассивного получения знаний из учебников или от учителей они перейдут к активному конструированию знания: будут участвовать в процессе получения данных, самостоятельно выявлять закономерности и «открывать» законы, возможно, совершать настоящие небольшие открытия на материале своих опытных участков.

ГлобалЛаб дает педагогам и обучающимся возможность размещать результаты своих исследований в виде отчетов, таблиц, карт и графиков в базе данных, возможность сравнивать на одной карте или на одном графике данные наблюдений и измерений, проведенных на опытных участках разных школ, возможность обсуждать ход и результаты конкретных исследований на форумах проекта [19].

Учи.ру – интерактивная образовательная онлайн-платформа, полностью соответствующая ФГОС и значительно усиливающая классическое школьное образование. *Учи.ру* способствует решению задач цифровой грамотности обучающихся и педагогов. Программы курсов частично бесплатные, но ограничено количество заданий, которые можно выполнить в день, также бесплатные олимпиады по различным предметам, есть платные курсы, в том числе и по программированию.

Всероссийский форум профессиональной ориентации «*ПроеКТОриЯ*» (<https://proektoria.online>) – интерактивная цифровая платформа для профориентации школьников, которая была запущена в ноябре 2016 года. Представляет собой онлайн-площадку для коммуникации, выбора профессии и работы над проектными задачами, игровую платформу с конкурсами, опросами и флешмобами, а также Интернет-издание с уникальным информационно-образовательным контентом. Объединяет ведущих экспертов и лидеров индустрий, лучших педагогов страны и мотивированных школьников для решения актуальных вопросов в области профессиональной ориентации и самоопределения. Регулярные уроки по профессиональной навигации, которые проводят известные личности:

министры, программисты, спортсмены, режиссёры, певцы, – для старшеклассников проходят в режиме «онлайн».

Для достижения целей проекта «Цифровая образовательная среда» выбран путь широкого внедрения онлайн-обучения, в том числе, массовых открытых онлайн-курсов – обучающих курсов с интерактивным участием и открытым доступом через Интернет. Для этого была создана платформа «Современная цифровая образовательная среда в Российской Федерации» (<http://neorusedu.ru>), которая обеспечивает реализацию доступа к онлайн-курсам по принципу «одного окна». С помощью проекта «Современная цифровая образовательная среда в Российской Федерации» будет обеспечен свободный доступ граждан к обучающим онлайн-курсам любого уровня, при этом будет организована возможность зачета их прохождения учебными заведениями и получение сертификатов, подтверждающих успешное завершение учебы. Реализация данного приоритетного проекта способствует интеграции среднего и высшего образования, проникновению онлайн-технологий в образование и эффективному их применению через повышение компетенций педагогов.

Цифровая образовательная платформа *Лекта* (<https://lecta.rosuchebnik.ru>) – это самая большая библиотека современных учебников в электронной форме.

Национальная электронная платформа педагогического образования (<https://nepro.ru>). Цель платформы – собрать в одном месте учебную и методическую литературу и дать педагогам из разных уголков страны доступ к качественным материалам от ведущих специалистов в педагогике. Регулярно заходя на платформу, учителя смогут привыкнуть использовать в учебном процессе электронные ресурсы. Абитуриенты педагогических вузов смогут до поступления посмотреть вводные курсы и убедиться в правильности своего выбора.

LearningApps.org является приложением Web 2.0 для создания более 20 видов интерактивных заданий: викторин, кроссвордов, пазлов, игр и т.д.

Важно отметить, что правильность выполнения заданий проверяется мгновенно. Основная идея интерактивных заданий заключается в том, что ученики могут проверить и закрепить свои знания в игровой форме, что способствует формированию познавательного интереса учащихся. В LearningApps педагог может создавать задания самостоятельно или использовать задания общедоступных интерактивных заданий, которые были разработаны пользователями ранее. Сервис LearningApps предоставляет возможность получения кода для того, чтобы интерактивные задания были помещены при желании на страницы сайтов или блогов преподавателей и учащихся.

Айрен (irenproject.ru) – бесплатная программа, предоставляющая возможность самостоятельно создавать тесты для проверки знаний и проводить тестирование в локальной сети, с использованием сети Интернет или на одиночных компьютерах. Тесты могут включать в себя задания различных типов: с выбором одного или нескольких верных ответов, с вводом ответа с клавиатуры, на установление соответствия, на упорядочение и на классификацию.

Безусловно, набор прикладных программ и онлайн-ресурсов, которые может использовать педагог в профессиональной деятельности, не ограничивается перечисленными. Их перечень составляет каждый педагог, исходя из учебных задач и личных предпочтений.

Рассмотрим возможности цифровых сервисов при использовании технологий смешанного обучения.

Федеральный государственный образовательный стандарт устанавливает определенные требования к результатам обучения, что вызывает необходимость изменения технологии организации обучения, перенос акцентов с «усвоения знаний» на формирование «компетентностей». Соответственно, для современной профессиональной образовательной организации необходимо создавать новые, совершенно иные образовательные условия, создание инновационной образовательной среды в

каждом из учебных заведений. Неотъемлемой частью учебного процесса становятся информационные технологии. Один из путей их применения – смешанное обучение, синтез классно-урочной системы и дистанционного обучения.

Смешанное обучение – это сочетание традиционной классно-урочной системы и современного цифрового образования. «Перевернутый класс» – одна из наиболее удачных моделей смешанного обучения. В данной случае рассматриваются возможности использования продуктов и сервисов Microsoft в учебной работе, в частности, для работы с технологией «Перевернутый класс».

В настоящее время компания Microsoft представила обществу и успешно реализует проект модернизации региональных систем образования «Реформатика», цель которого – создание инновационной образовательной среды в каждом из учебных заведений.

Современный урок – это сочетание традиционных и цифровых технологий, так называемое «смешанное обучение», где диалог учителя и учащегося сопровождается и аргументируется цифровыми образовательными ресурсами (ЦОР) – презентациями, статьями в Интернет, аудио- или видеозаписями, таблицами, графиками, диаграммами. Вместе с традиционной классной доской на уроке используются мультимедиа проекторы, цифровые доски, компьютеры и соответствующие программные средства.

Технологические решения, представляемые компанией, как нельзя лучше подходят к использованию в модели «Перевернутый класс» (Flipped class). Родоначальниками модели «Перевернутого класса» считаются два американских педагога – Джонатан Бергман (Jonathan Bergman) и Аарон Сэмс (Aaron Sams). В 2007 году эти педагоги искали и нашли возможность, как обеспечить лекционным материалом спортсменов, часто пропускающих занятия. Затем эта идея была развита в новое образовательное направление [6].

Суть модели «Перевернутого класса» состоит в том, что с лекционным (теоретическим) материалом учащиеся знакомятся дома, просматривая подготовленные педагогом тематические видеоролики и презентации в Интернете. Традиционное же домашнее задание они выполняют на следующий день в классе, участвуя в индивидуальной и групповой деятельности, общаясь с одноклассниками и педагогом. Другими словами, основные учебные действия поменялись местами: то, что раньше было классной работой, осваивается в домашних условиях, а то, что когда-то было домашним заданием, становится предметом рассмотрения в классе.

Применение данной модели обучения позволяет решить целый ряд проблем: проблему постоянной нехватки времени («объять необъятное»), проблему усиления деятельностной составляющей. Теперь ученик становится активным участником учебной деятельности, а учитель – направляющим звеном, на уроке акцент смещается от обзорного знакомства с новой темой в сторону ее совместного изучения и исследования. Обучение в рамках модели «Перевернутого класса» происходит следующим образом:

1. Педагоги готовят несколько видео-лекций в неделю. При этом учитель выступает гарантом актуальности материала: презентация в Microsoft PowerPoint или Microsoft Sway, мультимедиа материал в Microsoft OneNote или Microsoft Word, практическая задача в Microsoft Excel. Это могут быть как готовые материалы из сети Интернет, так и материалы, изготовленные с помощью возможностей продуктов и сервисов Microsoft.

2. Обучающиеся смотрят данные видео-лекции дома. Достоинства «домашнего» просмотра лекционных материалов: ученики осваивают материал в индивидуальном темпе; при этом отсутствуют временные ограничения; однако возможность общаться со школьниками не исключается.

3. Урок используется для выполнения практических работ или другой учебной деятельности.

В итоге модель «Перевернутого класса» обладает целым рядом преимуществ по сравнению с традиционными формами, хотя обучение в рамках данной модели, безусловно, требует от педагога дополнительной подготовки. Когда учитель только начинает организовывать подобную работу, необходимо учесть, что каждую видеолекцию следует сопровождать четкими учебными целями и поэтапной инструкцией, а также заданием. Если задания нет, то можно предложить ученикам не только написать краткий конспект, но и составить несколько вопросов к просмотренному материалу [7].

Рассмотрим подробнее применение различных технологических продуктов в формате «Перевернутый класс». Наиболее распространенная программа Microsoft в образовательных организациях на сегодняшний день – PowerPoint – удобная, доступная, понятная и простая. С помощью презентации можно реализовать практически все потребности участников учебного процесса: законспектировать текст, вставить или создать схемы, диаграммы, ссылки на внешнюю или внутреннюю информацию, разработать тестовые задания, записать аудио и видео, организовать групповую работу и многое другое.

С Microsoft Office Mix (надстройка к Microsoft PowerPoint) у педагогов появилась возможность организовывать учебный материал в виде цифрового рассказа (или электронного курса), который можно проигрывать автономно, без непосредственного участия учителя (например, в формате «Перевернутого класса»).

Для любителей облачных решений Microsoft недавно выпустила программу Microsoft Sway, очень быстро ставшую популярной у российских учителей. Microsoft Sway позволяет разработать красочную презентацию, быстро добавляя фото, видео и текстовые материалы, которые предлагает сама программа. Поиск в Интернет осуществляется автоматически, по ключевым словам, содержащимся в названии или тексте презентации.

Презентацию PowerPoint также можно встроить в Microsoft Sway и работать с ней далее в сетевом формате.

Microsoft Excel – опрос предназначен для быстрого создания опросов, анкет и текстов разных типов. Ссылку на тест можно вставить в цифровой образовательный ресурс, разработанный в любой программе, и организовать самопроверку или проверку усвоения нового материала.

Очень полезным для систематизации материала в форме групповой работы является совместное составление обобщающих таблиц, схем и т.п. В ходе занятий нередко требуется организовать совместную работу обучающихся, результат которой должен быть зафиксирован в общем итоговом документе (дневник учебного проекта, презентация, доклад, таблица...). Такой документ может являться результатом групповой работы, или персонифицированным – где каждый участник записывает свой результат на персональной страничке. В этом случае обучающийся имеет доступ только к своей странице и к общей странице учителя с методическими указаниями, а все персональные странички составляют единый файл для удобства просмотра преподавателем результатов работы группы.

Организовать групповую работу на уроке или вне стен класса можно, используя различные программы Microsoft: Microsoft OneDrive, Microsoft PowerPoint, Microsoft OneNote, Microsoft Sway, Microsoft Word, Microsoft Excel. Достаточно (в технологическом плане) «поделиться» документом с участниками учебного процесса, отправив на почту участника ссылку совместного доступа. Работать с общим файлом можно с любого устройства – компьютера, планшета, телефона, как очно, так и дистанционно. Все изменения пользователей сохраняются и автоматически вносятся в общий документ при подключении к сети Интернет.

Онлайн-сервис Microsoft OneDrive также является полезным для технологий смешанного обучения. Поскольку результатом выполнения учащимся домашней работы с использованием компьютера являются

цифровые файлы различного формата – тексты, аудио, видео (запись интервью или хода эксперимента), интерактивные презентации (сочетание мультимедиа всех форматов), Microsoft Sway-страницы и т.п., то необходима возможность работы с данными файлами с нескольких устройств.

Все менее используется такой способ для хранения и переноса разработанных дома цифровых продуктов, как использование флеш-карт. Размещение результатов персональной или совместной работы обучающихся в облачном файлохранилище становится все более популярным. Школьник отображает ход и результаты учебной работы с помощью различных инструментов (видео, текст, презентации, схемы, таблицы и т.д.), размещая документы в облачном файлохранилище. Использование облачных сервисов обеспечивает доступ к результатам персональной или совместной работы школьников с любого устройства (ПК, планшеты, мобильные телефоны и т.п.) [5].

Таким образом, сочетание возможностей современных цифровых ресурсов и образовательных технологий позволяет педагогу эффективно организовать учебную деятельность в соответствии с современными требованиями ФГОС. Педагог совершенствует навыки применения ИКТ-технологий в области преподавания предмета, повышает собственный уровень научно-методической подготовки.

Расширяется спектр видов учебной деятельности, в которые вовлекаются обучающиеся, при этом процесс обучения направляется в русло практического применения полученных знаний. Как результат, происходит формирование способности ориентироваться в многообразии информационных потоков и осваивать новые знания по мере необходимости. Индивидуализация обучения с расширением зон ответственности учащихся за результат обучения способствует формированию тех актуальных ключевых компетенций, которые необходимы для дальнейшей самореализации и успешной деятельности личности в современной реальности.

ЗАКЛЮЧЕНИЕ

Создание и функционирование цифровой образовательной среды, а также применение цифровых технологий обучения является особенно актуальным, как для студентов, так и для преподавателей.

Успешное функционирование ЦОС помогает:

Студентам:

- использовать цифровые образовательные технологии;
- использовать учебные объекты с сочетанием различных способов: с помощью текста, видео, графиков, фото, звука и анимации;
- получить доступ к разнообразным печатным и электронным образовательным ресурсам;
- обеспечивать новые возможности для перехода от обучения в аудитории к обучению в разных местах и в разное время;
- проектировать индивидуальный образовательный маршрут, удовлетворять образовательные потребности личности.

Преподавателям:

- использовать цифровые образовательные технологии;
- применять разнообразные печатные и электронные образовательные ресурсы;
- представлять учебные объекты с сочетанием различных способов (с помощью текста, видео, графиков, фото, звука и анимации);
- устранять бюрократические нагрузки за счет ее автоматизации;
- снижать рутинные нагрузки по контролю выполнения заданий студентами за счет автоматизации;
- улучшать возможности и удобства организации и мониторинга образовательного процесса;
- стимулировать и мотивировать студентов при освоении учебного материала и выполнении заданий;

– превращать студентов из пассивных объектов в активных субъектов учебного процесса.

Особое внимание следует уделять комплексному обеспечению информационной безопасности в условиях функционирования цифровой образовательной среды, которая включает в себя систему защиты информационной системы колледжа в целом, систему обеспечения информационной безопасности студентов, осведомленность и выполнение сотрудниками колледжа основных принципов и правил защиты при работе в цифровой образовательной среде.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

88. Аксютин, А.А. Информационные технологии в образовании и науке / Аксютин А.А., Вицен А.А., Мекшенева Ж.В. // Современные наукоемкие технологии, 2019. № 11. С. 50–52.

89. 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.

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

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

92. Главный тренд российского образования – цифровизация. [Электронный ресурс] // URL: <http://www.ug.ru/article/1029/> (дата обращения: 30.09.2020).

93. Информатизация образования. [Электронный ресурс] // Российская педагогическая энциклопедия. Режим доступа: <https://pedagogicheskaya.academic.ru/1241/> (дата обращения: 15.03.2020).

94. Информационный сервис для профессионального образовательного сообщества «Агрегатор новостей образования» [Электронный ресурс] // URL: https://akvobr.ru/cifrovaya_obrazovatel'naya_sreda_ehto.html (дата обращения: 15.04.2020).

95. Кашина, Е.А. Прогнозирование структуры интегрированного курса информатики: дис. канд. пед. наук / Е.А. Кашина. Екатеринбург, 2017. 187 с.

96. Меняйся или уходи. Цифровое образование бросает вызов преподавателям вузов. [Электронный ресурс] // URL: <http://www.poisknews.ru/theme/edu/31969/> (дата обращения: 30.09.2020).

97. Об утверждении Целевой модели цифровой образовательной среды: [приказ Министерства просвещения РФ от 02.12.2019 № 649, зарегистрирован в Минюсте РФ 24.12.2019, регистрационный № 56962] [Электронный ресурс] // Правовая база Гарант. — 2020. — URL: <https://www.garant.ru/> (дата обращения: 20.03.2020).

98. Образовательные экосистемы для общественной трансформации. Доклад Global Education Futures [Электронный ресурс] / П. Лукша, Дж. Кубиста, А. Ласло // Образование для сложного общества. – С. 77. URL: <https://drive.google.com/file/d/0B9ZvF6mQ5FMbSTFKVmhodU5rNTNiTXpUZ2QwZktiR0pzSmJR/view> (дата обращения: 18.09.2020)

99. Петрова, Н. П. Цифровизация и цифровые технологии в образовании / Н. П. Петрова, Г. А. Бондарева // Мир науки, культуры, образования. – 2019. – № 5 (78). – С. 353–355.

100. Приоритетный проект в области образования «Современная цифровая образовательная среда в Российской Федерации». [Электронный ресурс] // URL: <http://neorusedu.ru/about/> (дата обращения: 30.09.2020).

101. Распоряжение Правительства РФ от 28.07.2017 N 1632-р «Об утверждении программы Цифровая экономика Российской Федерации» [Электронный ресурс] // URL: [base.garant.ru/71 734 878](http://base.garant.ru/71734878) (дата обращения: 12.08.2020)

102. Сичинский, Е. П. О системе непрерывного повышения квалификации работников среднего профессионального образования Челябинской области / Е. П. Сичинский, И. Р. Сташкевич, З. А. Федосеева // Современная наука: актуальные проблемы теории и практики. – 2018. – № 8. – С. 72-75.

103. Сташкевич, И. Р. Информатизация как стратегический фактор развития профессионального образования / И. Р. Сташкевич //

Инновационное развитие профессионального образования. – 2016. – № 4 (12). – С. 25-28.

104. Сташкевич, И. Р. Информационно-образовательная среда профессиональной образовательной организации – смена образовательной парадигмы / И. Р. Сташкевич // Профессиональное образование и рынок труда. – 2014. – № 9 (13). – С. 26-28.

105. Стратегия развития информационного общества в РФ на 2017–2030 годы [Электронный ресурс]. URL: docs.cntd.ru/document/420 397 755 (дата обращения: 12.08.2020)

106. Тайлаков У. Н. Единое информационно-образовательное пространство школы как фактор повышения качества образовательных процессов [Текст] / У. Н. Тайлаков // Молодой ученый. – 2013. – №5. – С. 768-772.

ПРИЛОЖЕНИЕ 1

Глоссарий

Дистанционное обучение – технология организации образовательного процесса, которая предполагает взаимодействие педагога и обучающегося исключительно на расстоянии, на основе онлайн курсов.

Информационно-коммуникационные технологии (ИКТ) – информационные процессы и методы работы с информацией, осуществляемые с применением средств вычислительной техники и средств телекоммуникации. К средствам ИКТ часто относят аппаратные (компьютер, принтер, сканер, фотоаппарат, видеокамера, аудио- и видеомаягнитофон) и программные (электронные учебники, тренажеры, тестовые среды, информационные сайты, поисковые системы Интернета и т.д).

Прорывные технологии – технологии, потенциально способные изменить представление о возможности устройств и инструментов, расширяя их функциональные возможности, делая их более простыми и возможными.

Включают в себя:

- программирование эмоций;
- сотовые сети;
- гибкие системы;
- географически привязанные сервисы;
- машинное обучение;
- переводчики речи;
- беспроводную передачу энергии.

Система организации деятельности в цифровой образовательной среде носит условный характер и не должно восприниматься буквально, т.к. предметом цифровой дидактики выступает деятельность человека (обучаемого, обучающего), а не функционирование цифровых

образовательных средств. Цифровые ресурсы и технические средства обучения являются лишь средством обучения.

Смешанное обучение, blended learning – сочетание традиционных форм аудиторного обучения с элементами электронного обучения. В нем используются специальные информационные технологии (компьютерная графика, аудио и видео, интерактивные элементы и т.д.). Учебный процесс в этом случае представляет собой чередование фаз традиционного и электронного обучения. Смешиваться могут очное и дистанционное, самостоятельное и групповое обучение.

Технологии визуализации – используются в различных формах анализа визуальных данных; основаны на способности мозга быстро обрабатывать визуальную информацию, интуитивно выявлять особенности сложных процессов и явлений, изучать динамические процессы:

- 3D моделирование и прототипирование;
- дополненная и виртуальная реальность;
- анализ визуальных данных.

Цифровая безопасность – включает в себя знание и умение защиты персональных данных, организации надежного пароля; использование легального контента, культуру поведения, цифровую репутацию, этику, хранение информации, создание резервных копий.

Цифровая грамотность – набор знаний и умений, которые необходимы для безопасного и эффективного использования цифровых технологий и ресурсов интернета. Включает в себя: цифровое потребление; цифровые компетенции; цифровую безопасность. **Цифровая дидактика** – отрасль педагогики, научная дисциплина об особенностях организации процесса обучения в условиях цифрового общества.

Цифровая образовательная среда – система условий и возможностей, подразумевающая наличие информационно-коммуникационной инфраструктуры и предоставляющая набор цифровых технологий и ресурсов для обучения, развития, социализации, воспитания человека.

Цифровая среда – система условий и возможностей, подразумевающая наличие информационно-коммуникационной инфраструктуры и предоставляющая человеку набор цифровых технологий и ресурсов для самореализации, личностно-профессионального развития, решения различных бытовых и профессиональных задач.

Цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг. Главным способом обеспечения эффективности цифровой экономики становится внедрение цифровых технологий обработки данных, что позволит уменьшить затраты при производстве товаров и оказании услуг.

Цифровизация (в широком контексте) – переход с аналоговой формы передачи информации на цифровую.

Цифровизация образовательного процесса – встречная трансформация элементов образовательного процесса, с одной стороны, и цифровых технологий и средств, используемых в образовательном процессе, с другой, с целью максимально полного использования потенциальных дидактических возможностей цифровых технологий и максимально полного приспособления их к решению педагогических задач.

Цифровое общество – в научной литературе отсутствует точное определение. В бытовом смысле понятие рассматривается с разных позиций. Позитивная точка зрения рассматривает цифровое общество как общество равных возможностей, в котором сняты физические, административные и социальные барьеры для самореализации человека благодаря развитию технологий. Существует также негативная трактовка этого понятия как общества, в котором большинство поработчено меньшинством за счет использования информационных технологий, глобальных и локальных сетей,

при этом цифровые технологии рассматриваются как причина появления безработицы, кризисных явлений в экономике, ухудшения экологической обстановки и т.д. В целом цифровое общество рассматривается как система, основанная на использовании новых технологий в созданной цифровой среде, с новыми требованиями экономики к кадрам.

Цифровой образовательный процесс – специально организованный процесс индивидуальной и групповой учебной деятельности обучающихся, направленный на полное усвоение знаний/освоение умений, компетенций на основе использования цифровых технологий при мотивирующей, организационно-посреднической роли педагога.

Цифровые компетенции – навыки эффективного пользования технологиями. Включают в себя умение поиска информации, использования цифровых устройств, использования функционала социальных сетей, организации финансовых операций с помощью ИКТ-технологий, онлайн-покупки, критическое восприятие информации, производство мультимедийного контента, синхронизацию устройств.

Цифровые образовательные продукты – цифровые образовательные комплексы, онлайн-платформы, компьютерные программы и т.п., разработанные на основе взаимодействия между участниками образовательных отношений и разработчиками таких продуктов с учетом образовательных потребностей и целей, особенностей цифрового поколения, возможностей обучающихся и педагогов, дидактических принципов и особенностей образовательного процесса профессионального образования и обучения.

Цифровые образовательные технологии – способы применения устройств и программного обеспечения в учении или преподавании в классе и за его пределами, в формальном, неформальном и информальном образовании:

- обучение с использованием персональных цифровых устройств;

- перевернутые классы;
- геймификация;
- геолокация.

Цифровые технологии – информационно-коммуникационные, телекоммуникационные, виртуальные, мультимедийные технологии, позволяющие обеспечить сбор и представление информации о различных объектах с целью обеспечения удаленного взаимодействия между ними и (или) управления ими. Часто такие технологии называют «умные» (smart) (например, дополненная и виртуальная реальность, Интернет вещей, искусственный интеллект, 3D печать и т.д.). «Умные» технологии позволяют автоматизировать большинство рутинных операций. При позитивном сценарии развития цифрового общества именно такие технологии обеспечат снятие физических, административных и социальных барьеров для самореализации человека.

Электронное обучение, e-Learning – обучение с использованием информационно-образовательных ресурсов, информационно-коммуникационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу информационно-образовательных ресурсов и взаимодействие участников образовательного пространства. К электронному обучению относятся дистанционные технологии, web-конференции, web-семинары, web-квесты, интерактивные задания, образовательные интернет-сообщества, социальные сети.

ПРИЛОЖЕНИЕ 2

Бланк оценочного листа для проведения экспертизы.

Уважаемый эксперт! Оцените защищенность ресурсов (компонентов ЦОС), а также эффективность предлагаемых мер защиты

ФИО эксперта:	
Параметры	Оценка (от 1 до 5)
<i>Мероприятия по проектированию модели цифровой образовательной среды профессиональной образовательной организации</i>	
Корпоративная электронная почта	
Виртуальные чат-комнаты	
Система видеоконференцсвязи (https://bigbluebutton.ru/)	
Учебные календари в АИС «Сетевой город» Модуль ПОО	
Система электронного документооборота, встроенная в АСУ «ProCollege»	
Система дистанционного обучения для студентов на базе АСУ «ProCollege»	
Электронный журнал в АИС «Сетевой город» Модуль ПОО	
Система поддержки пользователей компьютерной техники: <ul style="list-style-type: none"> – техподдержка АСУ «ProCollege»; – техподдержка АИС «Сетевой город» Модуль ПОО; – консультации специалиста по ИБ и системного администратора. 	
Официальный сайт ГБПОУ «Миасский педагогический колледж»	
Электронная библиотечная система «Юрайт»	
Система оценки / мониторинга качества образования (https://i-exam.ru/)	
<i>Меры по совершенствованию осведомленности и выполнения сотрудниками колледжа основных принципов и правил защиты при работе в ЦОС</i>	
Организация курсов повышения квалификации по развитию компетенций в области информационной безопасности (программа прилагается)	
<i>Меры по обеспечению информационной безопасности студентов в условиях функционирования цифровой образовательной среды</i>	
Правовое обеспечение информационной безопасности	
Нравственный и этический контроль	
Защита психики и здоровья несовершеннолетнего	
Техническое и программное обеспечение ИБ	
Воспитательные и информационные меры по обеспечению ИБ	
Формирование информационной культуры студентов	
Образование в области безопасности жизнедеятельности и ИБ	

ПРИЛОЖЕНИЕ 3

**Дополнительная профессиональная программа
повышения квалификации
«Обеспечение информационной безопасности функционирования
цифровой образовательной среды профессиональной образовательной
организации»**

Дополнительная профессиональная программа
повышения квалификации
«Обеспечение информационной безопасности функционирования
цифровой образовательной среды профессиональной образовательной
организации»

1. Цели реализации программы

Дополнительная профессиональная программа повышения квалификации направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации по обеспечению информационной безопасности функционирования цифровой среды профессиональной образовательной организации.

2. Требования к результатам обучения. Планируемые результаты обучения

2.1. Характеристика нового вида профессиональной деятельности, трудовых функций и (или) уровней квалификации

№ п/п	Содержание совершенствуемой или вновь формируемой компетенции
1	Анализировать и оценивать угрозы информационного воздействия на личность обучающегося в условиях функционирования цифровой образовательной среды
2	Соблюдать основные требования информационной безопасности, в том числе политики информационной безопасности образовательной организации
3	Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
4	Обеспечивать охрану жизни и здоровья обучающихся при реализации образовательного процесса

Программа разработана в соответствии с профессиональным стандартом «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования)

(воспитатель, учитель)» (утвержден приказом Минтруда России от 18 октября 2013 года № 544н);

К освоению программы допускаются лица, имеющие среднее профессиональное и (или) высшее образование. Медицинские ограничения регламентированы Перечнем медицинских противопоказаний Минздрава России.

2.2. Требования к результатам освоения программы

В результате освоения дополнительной профессиональной программы у слушателя должны быть сформированы компетенции, в соответствии с разделом 2.1. программы.

В результате освоения программы слушатель должен

знать:

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- основные нормативные правовые акты в области информационной безопасности и защиты информации;
- правовые основы организации защиты персональной информации, коммерческой, служебной и профессиональной тайны;
- принципы и методы противодействия негативному информационному воздействию на личность обучающегося и манипуляции его сознанием;
- методы фильтрации контента и родительского контроля в интернете;

уметь:

- использовать и соблюдать федеральное законодательство в области обеспечения информационной безопасности и защиты персональных данных;
- формулировать и проектировать политику информационной безопасности образовательных организаций, знать и осуществлять организационные меры по защите персональных данных;

– анализировать и оценивать угрозы и факторы рисков негативного воздействия на личность в условиях функционирования цифровой образовательной среды;

– осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

3. Содержание программы

Категория слушателей: лица, имеющие среднее профессиональное образование и (или) высшее образование.

Трудоемкость обучения: 40 академических часов.

Форма обучения: очная.

3.1. Учебный план

№	Наименование модулей	Всего, ак.час.	В том числе			Форма контроля
			лекции	практ. занятия	промежут. и итог. контроль	
1	2	3	4	5	6	7
1.	Модуль 1. Основные понятия информационной безопасности	10	6	4	-	-
2.	Модуль 2. Правовые основы информационной безопасности и защита интеллектуальной собственности	14	6	8	-	-
3.	Модуль 3. Виды информационных угроз	4	4	-	-	-
4.	Модуль 4. Обеспечение информационной безопасности в условиях функционирования цифровой образовательной среды	6	4	2	-	-
6.	Итоговая аттестация (защита проекта)	6	-	-	6	Защита проекта
	ИТОГО:	72	24	46	8	

3.2. Учебно-тематический план

№	Наименование модулей	Всего, ак. час.	В том числе			Форма контроля
			лекции	практ. занятия	промежут. и итог. контроль	
1	2	3	4	5	6	7
1.	Модуль 1. Основные понятия информационной безопасности	10	6	4	-	-
1.1	Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Модели безопасности. Понятие «национальная безопасность». Доктрина безопасности Российской Федерации	2	2	-	-	-
1.2	Понятие конфиденциальной информации, ее виды.	2	2	-	-	-
1.3	Концепция информационной безопасности. Основные этапы обеспечения защиты информации	6	2	4	-	-
2.	Модуль 2. Правовые основы информационной безопасности и защита интеллектуальной собственности	14	6	8	-	-
2.1	Нормативно-правовые документы, регламентирующие отношения в сфере информационной	2	2	-	-	-

	безопасности.					
2.2	Правовой институт по охране авторского права. Субъекты авторского права. Права обладателей авторских прав.	6	2	4	-	-
2.3	Всемирная конвенция об авторском праве. Основные институты и понятия международного авторского права.	6	2	4	-	-
3.	Модуль 3. Виды информационных угроз	4	4	-		
3.1	Факторы, риски угроз информационным ресурсам. Виды угроз и типы атак.	2	2			
3.2	Классификация компьютерных преступлений	1	1			
3.3	Угрозы информационно-психологической безопасности личности и их основные источники	1	1			
4.	Модуль 4. Обеспечение информационной безопасности в условиях функционирования цифровой образовательной среды	6	4	2	-	-
4.1	Система обеспечения информационной безопасности в условиях функционирования цифровой образовательной среды	4	2	-	-	-
4.2	Обеспечение информационной безопасности студентов	4	2	2	-	-

7.	Итоговая аттестация	6	-	-	6	ЗП
7.1	Защита проекта (ЗП)	6	-	-	6	ЗП
	ИТОГО:	40	20	14	6	

3.3. Содержание программы

Модуль 1. Основные понятия информационной безопасности

Тема 1.1 Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности.

Лекция. Понятие об информационной и национальной безопасности. Модели безопасности. Доктрина безопасности Российской Федерации.

Тема 1.2 Понятие конфиденциальной информации, ее виды.

Лекция. Классификация информации по категории доступа. Виды информации. Понятие ценности информации. Перечень сведений, доступ к которым не может быть ограничен. Конфиденциальность информации.

Тема 1.3 Концепция информационной безопасности. Основные этапы обеспечения защиты информации

Лекция. Определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. Меры по защите информации.

Практическое занятие. Выполнение учебного проекта «Принципы комплексного подхода к обеспечению информационной безопасности»

Модуль 2. Правовые основы информационной безопасности и защита интеллектуальной собственности

Тема 2.1 Нормативно-правовые документы, регламентирующие отношения в сфере информационной безопасности.

Лекция. Предмет и задачи правового обеспечения информационной безопасности. Законодательство о безопасности и защите информации, его структура и содержание.

Тема 2.2 Правовой институт по охране авторского права. Субъекты авторского права. Права обладателей авторских прав.

Лекция. Авторские и патентные права. Ущерб от незаконного использования авторских и смежных прав. Интеллектуальная собственность.

Практическое занятие. Правовые аспекты деятельности в глобальной сети

Интернет.

Тема 2.3 Всемирная конвенция об авторском праве. Основные институты и понятия международного авторского права.

Лекция. Институты и понятия международного авторского права. Произведения, пользующиеся охраной. Правовые нормы и стандарты по лицензированию и сертификации.

Практическое занятие. Безопасность и конфиденциальность в Интернете.

Модуль 3. Виды информационных угроз

Тема 3. 1 Факторы, риски угроз информационным ресурсам. Виды угроз и типы атак.

Лекция. Угрозы информационным ресурсам. Информационные войны. Информационное оружие. Анализ и оценивание угроз информационной безопасности личности в современном информационном обществе.

Тема 3.2 Классификация компьютерных преступлений.

Лекция. Группы компьютерных преступлений. Хакерство в мире и в России. Закрывание информации как средство ее защиты от несанкционированного доступа.

Тема 3.3 Угрозы информационно-психологической безопасности личности и их основные источники.

Лекция. Информационно-психологическая безопасность личности. Сущность и современное состояние манипуляции сознанием и поведением людей. Информационная среда иллюзии и реальности.

Модуль 4. Обеспечение информационной безопасности в условиях функционирования цифровой образовательной среды

Тема 4.1 Система обеспечения информационной безопасности в условиях функционирования цифровой образовательной среды.

Лекция. Мероприятия, направленные на обеспечения информационной безопасности в условиях функционирования цифровой образовательной среды.

Тема 4.2 Обеспечение информационной безопасности студентов.

Лекция. Воспитательные мероприятия, направленные на обеспечение информационной безопасности студентов. Образование в области информационной безопасности.

Практическое занятие. Анализ образовательных интернет-ресурсов, направленных повышение уровня информационной безопасности.

3.4. Календарный учебный график (порядок освоения модулей)

Период обучения (недели)*	Наименование модуля
1 неделя	Модуль 1. Название
2 неделя	
	Итоговая аттестация
*Точный порядок реализации модулей (дисциплин) обучения определяется в расписании занятий.	

4. Организационно-педагогические условия реализации программы

4.1. Материально-технические условия реализации программы

Наименование помещения	Вид занятий	Наименование оборудования, программного обеспечения
<i>1</i>	<i>2</i>	<i>3</i>
Аудитория	Лекции	Компьютер, мультимедийный проектор, экран, доска, флипчарт

Лаборатория, компьютерный класс	Лабораторные и практические занятия, тестирование, защита итогового проекта	Компьютеры, мультимедийный проектор, экран, принтер, доска, флипчарт
------------------------------------	--	--

4.2. Учебно-методическое обеспечение программы

- печатные раздаточные материалы для слушателей;
- учебные пособия, изданных по отдельным разделам программы;
- профильная литература;
- отраслевые и другие нормативные документы;
- электронные ресурсы и т.д.

Профильная литература:

1. Баймакова, И.А. Обеспечение защиты персональных данных. Методическое пособие / И.А. Баймакова, А.В. Новиков, А.И. Рогачев – М.: 1С -Пабблишинг, 2014. – 214 с.

2. Белов, Е.Б. Основы информационной безопасности [Текст]. Учебное пособие для вузов / Е.Б.Белов, В.П.Лось, Р.В.Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2016. – 544 с.

3. Богатырева, Ю.И. Модель обеспечения информационной безопасности школьников при создании инфобезопасной среды образовательного учреждения / Ю.И. Богатырева // Известия Тульского государственного университета. Гуманитарные науки. Вып. 3. Ч. 2. Тула: изд-во ТулГУ, 2013. – 343 с. – С. 14-25.

4. Захарова, И.Г. Информационные технологии в образовании: учеб. пособие для студ. высш. пед. учеб. Заведений / И.Г. Захарова. – М: ИЦ «Академия», 2015. -192 с.

5. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст]. Учеб. пособие для вузов / А.А. Малюк. – М.: Горячая линия-Телеком, 2014. – 280 с.

6. Чипига, А.Ф. Информационная безопасность автоматизированных систем: учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности [Текст]/ А.Ф. Чипига. – М.:ГелиосАРМ, 2017. – 336 с.

4.3. Кадровые условия реализации программы

Реализацию дополнительной профессиональной программы повышения квалификации осуществляют представители преподавательского состава ГБПОУ «Миасский педагогический колледж», имеющие образование и квалификацию, соответствующие требованиям.

5. Оценка качества освоения программы

Итоговая аттестация проводится в форме защиты индивидуального проекта.

Тематика проектов:

1. Информация, относящаяся к государственной тайне.
2. Понятие персональных данных.
3. Информация, составляющая коммерческую тайну.
4. Объекты информационной безопасности.
5. Случайные и целенаправленные угрозы нарушения сохранности информации.
6. Понятие «противоправный контент».
7. Риски информационной безопасности школьников.
8. Понятие информационного оружия. Информационные войны
9. Критерии безопасности.
10. Аудит информационной безопасности.
11. История хакерства. Хакерство в России.
12. Правовые механизмы защиты информации на разных уровнях.
13. Задачи и способ функционирования межсетевое экрана.
14. Политика безопасности администратора сети и брандмауэра.
15. Инфобезопасная среда в образовательной организации.

Требования к проекту

<i>Количественная оценка проекта</i>							
<i>Выполненные работы</i>							
Оцениваемые составляющие проекта	Электронный текст	Электронные таблицы	Презентация, Буклет	Сетевые технологии	Содержание	Дизайн проекта	Итого
Баллы	1	2	3	4	5	5	20
Название проекта							
Автор							

6. Составители программы

М.В. Бугаевская М.В., магистрант ФГБОУ ВО «ЮУрГГПУ»

ПРИЛОЖЕНИЕ 4

Памятка для педагогических работников по обеспечению информационной безопасности обучающихся

1. Объясните обучающимся правила поведения в Интернете. Расскажите о мерах, принимаемых к нарушителям, ответственности за нарушение правил поведения в сети.
2. Совместно с обучающимися сформулируйте правила поведения в случае нарушения их прав в Интернете.
3. Приучайте несовершеннолетних уважать права других людей в Интернете. Объясните им смысл понятия «авторское право», расскажите об ответственности за нарушение авторских прав.
4. Проявляйте интерес к «виртуальной» жизни обучающихся, и при необходимости сообщайте родителям о проблемах их детей.
5. Научите обучающихся внимательно относиться к информации, получаемой из Интернета. Формируйте представление о достоверной и недостоверной информации. Наставляйте на посещение проверенных сайтов.
6. Обеспечьте профилактику интернет-зависимости обучающихся через вовлечение детей в различные внеклассные мероприятия в реальной жизни (посещение театров, музеев, участие в играх, соревнованиях), чтобы показать, что реальная жизнь намного интереснее виртуальной.
7. Периодически совместно с обучающимися анализируйте их занятость и организацию досуга, целесообразность и необходимость использования ими ресурсов сети для учебы и отдыха с целью профилактики интернетзависимости и обсуждайте с родителями результаты своих наблюдений.
8. В случае возникновения проблем, связанных с Интернетзависимостью, своевременно доводите информацию до сведения родителей, привлекайте к работе с обучающимися и их родителями психолога, социального педагога.

9. Проводите мероприятия, на которых рассказывайте о явлении Интернет-зависимости, ее признаках, способах преодоления.
10. Систематически повышайте свою квалификацию в области информационно-коммуникационных технологий, а также по вопросам здоровьесбережения.
11. Станьте примером для своих учеников. Соблюдайте законодательство в области защиты персональных данных и информационной безопасности. Рационально относитесь к своему здоровью. Разумно используйте в своей жизни возможности интернета и мобильных сетей.