



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

**Организация единого информационного пространства образовательной
организации в условиях обеспечения информационной безопасности**

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

Проверка на объем заимствований:
79,69% авторского текста

Работа рекомендована к защите
«17» января 2022 г.
Зав. кафедрой АТИТ и МОТД
Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Орленко Павел Сергеевич

Научный руководитель:
к.т.н., старший преподаватель
Гафарова Елена Аркадьевна

Челябинск
2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	4
ГЛАВА 1. ЕДИНОЕ ИНФОРМАЦИОННОЕ ОБРАЗОВАТЕЛЬНОЕ ПРОСТРАНСТВО ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ.....	15
1.1 ЕДИНОЕ ИНФОРМАЦИОННОЕ ОБРАЗОВАТЕЛЬНОЕ ПРОСТРАНСТВО ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ – СУЩНОСТЬ, ПОДХОДЫ К ОПРЕДЕЛЕНИЮ, КОМПОНЕНТЫ.....	15
1.2 ЕДИНОЕ ИНФОРМАЦИОННОЕ ОБРАЗОВАТЕЛЬНОЕ ПРОСТРАНСТВО МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКОЙ ОБЛАСТИ	21
1.3 АНАЛИЗ УЯЗВИМОСТЕЙ ЕДИНОГО ИНФОРМАЦИОННОГО ОБРАЗОВАТЕЛЬНОГО ПРОСТРАНСТВА МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКОЙ ОБЛАСТИ	32
ГЛАВА 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ	46
2.1.НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ, МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКА	46
2.2. НАПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ ЗАЩИТЫ ЕДИНОГО ИНФОРМАЦИОННОГО ОБРАЗОВАТЕЛЬНОГО ПРОСТРАНСТВА МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКОЙ ОБЛАСТИ.....	63
ГЛАВА 3. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКОЙ ОБЛАСТИ	67
3.1. ОБЩИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКОЙ ОБЛАСТИ	67
3.2. РАЗРАБОТКА И ВНЕДРЕНИЕ МОДЕЛИ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ХРАНИЛИЩА С РАСПРЕДЕЛЕНИЕМ ПРАВ	

ПОЛЬЗОВАТЕЛЕЙ В ЕДИНОЕ ИНФОРМАЦИОННОЕ ОБРАЗОВАТЕЛЬНОЕ ПРОСТРАНСТВО МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКОЙ ОБЛАСТИ	68
ЗАКЛЮЧЕНИЕ	82
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ.....	85

ВВЕДЕНИЕ

Сегодня мы живем в мире, характеризующимся небывалым ростом объема информационных потоков. Идет нарастание темпов изменений в экономике, социальной сфере, политике. На мировом рынке появляются новые технологии, определяющим ресурсом которых становится информация. Идет процесс информатизации общества не только с точки зрения внедрения современных компьютерных технологий, но и с точки зрения овладения информацией как ресурсом управления инновациями.

С целью повышения качества жизни граждан на основе использования информационных и телекоммуникационных технологий была разработана государственная программа Российской Федерации «Информационное общество (2011–2020)».

Одна из задач, которую преследует данная программа – обеспечение предоставления гражданам и организациям услуг с использованием современных информационных и телекоммуникационных технологий. [17]

Всё большие возможности, связанные с использованием информационных и коммуникационных технологий, появляются в сфере образования. Оснащение школ мультимедийным компьютерным оборудованием и цифровыми лабораториями кабинетов физики, химии, биологии; подключение школ к сети Интернет; использование на уроках и в домашних условиях цифровых образовательных ресурсов; использование отдельных приложений для автоматизации административных функций: учет кадров, ведение штатного расписания школы, использование в подготовке расписания занятий, обмен документами с вышестоящими органами управления образованием – все эти процессы указывают на наличие в образовательных учреждениях информационно-образовательной среды, и указывают на тот факт, что традиционная общеобразовательная школа выполнила свои задачи.

Рассматривая тенденции образовательной политики государства в области использования современных информационных технологий хотелось бы упомянуть общероссийский проект, разработанный в соответствии с Федеральной целевой программой развития образования - «Школа цифрового века». Основная концепция данного проекта – создать принципиально новый формат оснащения образовательных организаций, который позволит решать педагогические задачи, используя новейшие цифровые технологии. Основное внимание в данном проекте обращалось на повышение результативности использования современных образовательных технологий (в том числе, информационно-коммуникационных) в профессиональной деятельности, а также вовлечение педагогических работников в цифровое образовательное пространство. Это одна из мер, которая способствовала переходу к новым образовательным стандартам.

Важно понимать, что увеличение количества мультимедийного оборудования, не дает нового качества образования. Основная задача современного образовательного учреждения – создать единое информационно-образовательное пространство, которое было бы комфортно для сотрудничества и взаимодействия учителей, учеников, администрации школы и родителей, в том числе в условиях обеспечения информационной безопасности. С 1 сентября 2015 года вступили в силу поправки к ФЗ « О персональных данных» от 27.07.2006 №152-ФЗ, согласно которым, любая российская компания и образовательная организация, как оператор персональных данных населения, должна обеспечивать систематизацию, запись, накопление, хранение и уточнение персональных данных граждан с использованием баз данных. Помимо защиты баз данных к обеспечению информационной безопасности в образовательной организации также относится препятствие любому виду пропаганды и манипуляций, направленных на учащихся.

Наиболее перспективным направлением развития образовательной организации должно стать разработка и внедрение модели информационного

пространства школы, основанной на организации управленческого, методического и педагогического процессов с помощью современных информационно-коммуникационных и сетевых интерактивных технологий, с выстроенной системой информационной безопасности. Такая модель должна обеспечивать не только соблюдение образовательных стандартов, но и предусматривать защиту сведений и данных в соответствии с действующим законодательством.

Спецификой обеспечения информационной безопасности в образовательной организации является состав характерных угроз, к которым относится деятельность учащихся, их родителей и учителей. Школа должна научиться, не только прогнозировать угрозы, но и обеспечить информационную безопасность таким образом, чтобы получить для себя конкурентные преимущества. Школа должна стать конкурентоспособной, постоянно повышать качество своих услуг.

Выработка стратегии развития информационной безопасности образования в Российской Федерации отражена в следующих федеральных законах, целевых программах и проектах:

1. Концепция информационной безопасности детей.
2. Национальная стратегия действий в интересах детей на 2012-2017 гг., одно из основных направлений реализации которой - обеспечение информационной безопасности детей (Указом Президента Российской Федерации от 29 мая 2017 г. № 240 2018–2027 годы объявлены в России Десятилетием детства). [3]
3. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных".
4. Постановление Правительства РФ от 21 марта 2012 г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним

нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".

5. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".
6. Федеральный закон от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
7. Федеральный закон от 02.07.2013 г. № 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях».
8. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
9. Письмо Министерства образования и науки РФ от 03.10.2017 г. N 09-1995 «Методические рекомендации по проведению мероприятий по повышению правовой грамотности детей, родителей (законных представителей) и педагогических работников, участвующих в воспитании детей».
10. Письмо Министерства образования и науки РФ от 14.05.2018 № 08-1184 «Методические рекомендации 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 и использовании сети «Интернет».
11. Федеральный государственный стандарт основного общего образования.

В современной науке имеется совокупность знаний, необходимых для постановки и решения проблемы, обоснования сущностных изменений

процесса обеспечения информационной безопасности в образовательном учреждении.

Сущностные черты информационного общества определены в трудах Р.Ф.Абдеева, А.Тоффлера, Д.Белла.[1,68,8]

Разработка индикаторов оценки внедрения ИКТ в образовательные организации - Г.К.Нургалиева, А.И.Тажигулова.[38]

Повышению ИКТ-компетентности учащихся посвящены работы А.А.Кузнецова, М.П.Лапчика, В.С.Собкина, В.С.Леднева.[33,66,34]

Использованию цифровых образовательных ресурсов, созданию виртуальных сред - И.А.Лазаревой, А.Ю.Уварова, С.Г.Григорьева.[70,71,18,19]

Разработке, внедрению, развитию современной информационно-образовательной среды образовательных организаций посвящены работы С.В.Зенкина, Б.С. Ахметова, А.Л.Семёнова, А.Г.Асмолова, Е.Ы.Бидайбекова.[6,4,11]

Общие научные и методологические вопросы информационной безопасности рассматривали W. Stallings, А.П. Коваленко, Р.В. Мещеряков, В.И. Ярочкин, и др. [90,36,88]

Правовые аспекты обеспечения информационной безопасности осветили в своих трудах И.Л. Бачило, В.М. Алексеев, Е.А. Чичнева.

Фундаментальные вопросы защиты информации освещены в исследованиях таких ученых, как Л.Дж. Хоффман, Н. Винер, А.Д. Урсул, В.М. Глушков, А.Н. Колмогоров, Д. Керр, С. Мэдник, К. Шеннон.[79,73]

Аспектами обеспечения ИБ и защитой информации на предприятии занимались А.С. Гринберг, И.Р. Конеев, Б.И. Скородумов, М.Д. Тарнавский, Ю.М. Шубин, L. Kreicberga и др.

Рассмотрение факторов риска и проблем защиты личности от информационного воздействия в современном обществе мы наблюдаем у таких исследователей, как Г.В. Грачева, Ю.А. Ермакова, В.Е. Лепского, И.К. Мельника.

Вопросы анализа угроз информационного воздействия и обеспечения информационно-психологической безопасности школьника представили в своих трудах Г.В. Грачев, И.А. Баева, С.В. Шведова, В.П. Заболотский, С.Г. Кара-Мурза, С. Хассен.

Проблемы информатизации и компьютеризации в современном обществе раскрыты в исследованиях Е.И. Гужвенко, Я.А. Ваграменко, О.А. Козлова, С.А. Бешенкова, М.П. Лапчика, А.А. Кузнецова, В.П. Полякова, И. В. Роберт.[33,27,60,61,62]

Технические аспектам защиты информации в информационных системах и сетях раскрыты в работах В.А. Герасименко, В.Н. Лопатина, Ю.Л. Шершневой.

Различные аспекты информационной безопасности находят свое отражение преимущественно в таких науках, как: социология, психология и технических науках. При этом в педагогическом образовании не так много теоретико-методологических исследований, позволяющих сформулировать в полном объеме требования по организации единого информационного пространства образовательной организации в условиях обеспечения информационной безопасности. Такие исследования необходимы, так как в последнее время изменился субъект образовательного процесса и увеличивается степень угроз информационного воздействия на школьников в учебно-воспитательной и внеучебной деятельности, нарастает острота проблемы информационной безопасности всех субъектов образовательного процесса.

Возникает противоречие между усилением необходимости научно-педагогических и программно-технологических разработок и недостаточной разработанностью теоретической базы для осуществления данной деятельности в рамках обеспечения информационной безопасности образовательного учреждения.

Указанное противоречие позволило сформулировать проблему исследования: недостаточная разработанность теоретических и

методологических основ по организации единого информационного пространства образовательной организации в условиях обеспечения информационной безопасности, ведет к неспособности в полной мере удовлетворить требования информационной безопасности школьников, преподавательского состава и административного корпуса в условиях информатизации общества и образования.

Необходимость разрешения противоречия, актуальность и недостаточная теоретическая и практическая разработанность проблемы определили выбор темы исследования: «Организация единого информационного пространства МАОУ «СОШ №21» в условиях обеспечения информационной безопасности».

Гипотеза моего исследования:

если провести анализ результативности использования информационно-образовательной среды МАОУ «СОШ №21», то это позволит разработать механизмы управления данной средой в условиях информационной безопасности.

Гуманизация и демократизация образования, направленные на повышение эффективности обучения, способствуют росту объема информации. Данный факт повышает требования к уровню компьютеризации образовательного учреждения. Обеспечение сохранности и оперативности получения данных, для принятия оптимальных управленческих решений по результатам деятельности, является основой работы школы в инновационном режиме. Многогранный анализ образовательной деятельности, прослеживания динамики изменений и своевременная корректировка работы в условиях обеспечения информационной безопасности - все это определяет **актуальность** темы нашего исследования.

Объект исследования: единое информационное образовательное пространство образовательной организации пространство МАОУ «СОШ №21».

Предмет исследования: модель защищенного информационного хранилища образовательной организации.

Целью исследования является разработка рекомендаций по повышению уровня информационной безопасности единого информационного образовательного пространства образовательной организации (далее – ЕИОПОО) и опытно-экспериментальная проверка предложенных рекомендаций.

Гипотеза исследования состоит в предположении о повышении защищенности ЕИОПОО при внедрении модели защищенного информационного хранилища образовательной организации при размещении данных на выделенном сервере и применении средств аутентификации и идентификации для доступа к ним.

База исследования: МАОУ «СОШ №21» г. Миасса Челябинской области.

Задачи исследования:

1. Изучить единое информационное образовательное пространство образовательной организации, провести анализ его уязвимостей;
3. Проанализировать нормативно-правовое обеспечение информационной безопасности и ее направления в образовательном учреждении;
4. Разработать рекомендации по обеспечению информационной безопасности в МАОУ «СОШ №21» г. Миасса Челябинской области;
5. Провести опытно-экспериментальную проверку предложенных рекомендаций.

Научная новизна исследования состоит в том, что показана возможность обновления функционирования ЕИОП образовательной организации в условиях обеспечения информационной безопасности посредством внедрения модели информационного хранилища.

Теоретическая значимость исследования определяется расширением научных знаний в области обеспечения информационной безопасности образовательных организаций.

Практическая значимость диссертации определяется тем, что разработанная модель информационного хранилища может быть адаптирована в других образовательных организациях.

Основные этапы исследования:

На первом этапе формулировалась тема исследования, проводился сбор информации по теме исследования из различных источников, осуществлялась формулировка гипотезы, постановка цели, задач.

В ходе второго этапа осуществлялся анализ методов и средств, которые задействуются в организации по защите информации в ЕИОПОО, проводился анализ научной литературы и отбор информации по теме исследования, осуществлялась публикация научных статей, была разработана модель защищенного информационного хранилища образовательной организации при размещении данных на выделенном сервере и применении средств аутентификации

Третий этап заключался во внедрении разработанной модели информационного хранилища и апробации его функционирования в ЕИОПОО на базе исследования в МАОУ «СОШ №21» г. Миасса Челябинской области.

Личный вклад соискателя состоит в проведении анализа уязвимостей базы исследования, разработке рекомендаций по обеспечению информационной безопасности в образовательной организации на основе анализа, а также разработке модели информационного хранилища и внедрения разработанной модели в ЕИОП МАОУ «СОШ №21» г. Миасса Челябинской области.

Ход исследования и его результаты докладывались и обсуждались на международных конференциях, проводилась апробация путем научных публикаций:

1. Орленко, П.С. Исторический аспект становления системы защиты информации и анализ современного состояния информационной безопасности [Текст] / П.С. Орленко // Профессиональное образование: методология, технологии, практика: сборник научных статей. –2020. – Выпуск 13. – С.191 – 196.

В первой главе работы рассмотрены различные подходы к определению понятия «информационно-образовательное пространство». Изучены компоненты ЕИОП и определены его уровни. Рассмотрена структура действующего информационного образовательного пространства МАОУ «СОШ №21» г. Миасса Челябинской области. В данной главе рассмотрены виды угроз. По анализу литературных источников приведены методики для определения и категоризации угроз. Подробно рассмотрена методика SWOT-анализа, с помощью которой проведён анализ уязвимостей МАОУ «СОШ №21». Кроме того, в первой главе представлены инструменты, которые были использованы в исследовании текущего состояния ресурсной базы школы №21 г. Миасса Челябинской области.

Во второй главе приведены результаты анализа нормативно-правового обеспечения информационной безопасности в МАОУ «СОШ №21». Определены направления информационной защиты единого информационного образовательного пространства школы. На основании проведённых исследований сделаны выводы и определена задача - разработать модель информационной среды с учётом выявленных недостатков, которая позволит вывести школу №21 г. Миасса на качественно более высокий уровень использования ИКТ в образовательной деятельности.

В третьей главе приведено описание общих рекомендаций по обеспечению информационной безопасности в МАОУ «СОШ №21» г. Миасса Челябинской области, разработана новая модель защищенного информационного хранилища с распределением прав пользователей единого информационно-образовательного пространства МАОУ «СОШ №21», представлен опыт интеграции предложенной модели, разработана пошаговая

инструкция «Создание защищенного файлового хранилища», адаптированная к нуждам образовательной организации, рассмотрены преимущества и недостатки внедренной модели.

Диссертационная работа состоит из введения, трех глав, заключения, библиографического списка и приложений.

ГЛАВА 1. ЕДИНОЕ ИНФОРМАЦИОННОЕ ОБРАЗОВАТЕЛЬНОЕ ПРОСТРАНСТВО ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1 ЕДИНОЕ ИНФОРМАЦИОННОЕ ОБРАЗОВАТЕЛЬНОЕ ПРОСТРАНСТВО ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ – СУЩНОСТЬ, ПОДХОДЫ К ОПРЕДЕЛЕНИЮ, КОМПОНЕНТЫ.

Образовательное пространство представляет собой вид пространства, место, охватывающее человека и среду в процессе их взаимодействия, результатом которого выступает приращение индивидуальной культуры образующегося.[12]

Олефир С.В. предлагает рассматривать информационно образовательное пространство как пространство вербальной и документальной коммуникаций, формируемое для повышения культурного и образовательного уровня его субъектов.[43]

Однако, раскрытие того или иного понятия требует последовательного анализа и изучения нескольких, даже многих источников. Необходим комплексный подход, который позволит проследить взаимосвязь и взаимодействие всех компонентов и процессов педагогической системы. Рассмотрим, какие еще существуют подходы к понятию «информационно-образовательное пространство (среда)».

Андреев А.А. видит данную среду как единое информационное пространство, объединяющее информацию, как на традиционных, так и электронных носителях; компьютерно-телекоммуникационные, учебно-методические комплексы и технологии взаимодействия; педагогическую систему нового уровня, которая включает в себя материально-техническое, финансово-экономическое, нормативно-правовое обеспечение.[3]

Лушников И.Д. трактует информационно-образовательное пространство (среду) как совокупность единой базы данных, технологий их сопровождения и использования, информационных, телекоммуникационных систем, обеспечивающих информационное взаимодействие и удовлетворение

информационных потребностей участников образовательного процесса (администрации образовательной организации, педагогов, обучающихся, родителей (законных представителей), социальных партнёров).[35]

Ильченко О.А. позиционирует ИОП как системно организованную совокупность информационного, технического, учебно-методического обеспечения, которая неразрывно связана с человеком как субъектом образования.[21]

Ахметов Б.С. и Бидайбеков Е.Ы. представляют её как многокомпонентный комплекс образовательных ресурсов и технологий, которые обеспечивают информатизацию и автоматизацию образовательной деятельности учебного заведения.[38]

Захарова И.Г. считает, что ИОП – это открытая система, которая объединяет интеллектуальные, культурные, программно-методические, организационные и технические ресурсы.[20]

Курова Н.Н. видит в ИОС эффективное средство управления процессом информатизации.[32]

Л.А. Чашников характеризует информационную среду образовательного учреждения, как сложное взаимодействие типа «человек - техника», «человек - человек», «человек - знаковая система», «человек – художественный образ». [80]

Е.С. Афолина в своей работе дает следующее определение:

Единое информационное пространство школы – это система, в которой задействованы и на информационном уровне связаны все участники учебного процесса: администраторы, преподаватели, ученики и их родители. Практически все участники образовательного процесса объединены между собой соответствующими информационными потоками.[5]

Проанализировав данные определения, можно сделать вывод, что разные авторы видят информационно-образовательное пространство по-разному, но все они сходятся в одном – это интегрированная многокомпонентная система, представляющая собой непрерывное

взаимодействие всех участников образовательного процесса (учитель-родитель-ученик). В каждом определении речь идет об объединении либо участников процесса, либо ресурсов. Крайне важно мнение Чашникова Л.А., который, называет информационную среду образовательного учреждения важным условием всех взаимодействий.

Многие авторы уравнивают два термина «пространство» и «среда». Но анализ изученной литературы показывает, что использование этих понятий как синонимов недопустимо. Особенно, когда речь идет об образовательной организации. Среда, по нашему мнению, это условия, в которых приходится функционировать организации. Пространство же является результатом конструктивного педагогического и административного труда, направленного на освоение среды, и адаптации этой среды для решения задач конкретного образовательного учреждения.

Единое информационно-образовательное пространство школы (далее ЕИОП) – это основанная на использовании компьютерной техники программно-телекоммуникационная среда, реализующая едиными технологическими средствами и взаимосвязанным содержательным наполнением качественное информационное обеспечение школьников, педагогов, родителей (законных представителей), администрации учебного заведения и общественности.[81]

Системность информационно-образовательного пространства образовательного учреждения законодательно закреплена в Федеральном государственном образовательном стандарте. «Информационно-образовательная среда образовательного учреждения включает: комплекс информационных образовательных ресурсов, в том числе цифровые образовательные ресурсы, совокупность технологических средств информационных и коммуникационных технологий (ИКТ): компьютеры, иное ИКТ-оборудование, коммуникационные каналы, систему современных педагогических технологий, обеспечивающих обучение в современной информационно-образовательной среде».[76]

Изучая вопрос компонентов ЕИОП в литературных источниках можно встретить разные подходы к их определению. Наиболее важные компоненты, на наш взгляд, представлены ниже.

ЕИОП складывается из следующих главных компонентов:

- информационные ресурсы, содержащие данные, сведения и знания, зафиксированные на соответствующих носителях информации,
- организационные структуры, обеспечивающие функционирование и развитие единого информационного пространства, в частности, сбор, обработку, хранение, распространение, поиск и передачу информации,
- средства информационного взаимодействия учащихся и образовательных учреждений, обеспечивающие им доступ к информационным ресурсам на основе соответствующих информационных технологий, включающие программно-технические средства и организационно-нормативные документы.[67]

К информационно-технологическим компонентам ЕИОП, т.е. технологиям, адаптированным и используемым в деятельности образовательного учреждения относятся:



Рисунок 1. Информационно-технологические компоненты ЕИОП

Компоненты ЕИОП должны соответствовать не только учебной деятельности, но и научно-исследовательской, внеурочной деятельности, а также деятельности по управлению учебным заведением. Такое пространство должно быть вариативным, чтобы была возможность обеспечить любому пользователю возможность полного информационного обеспечения своей деятельности, получения любых образовательных услуг, а также возможность обмена информацией между пользователями.

Изученные методические и научные труды по проблеме исследования позволили нам определить уровни единого информационного пространства образовательного учреждения и выделить процессы, происходящие на каждом из них. Представим информацию в таблице.

Таблица 1 – Уровни и процессы единого информационного пространства образовательного учреждения

Уровень администрации	Уровень образования	Уровень ученика	Уровень родителя
Мониторинговая деятельность	Визуализация учебной информации	Развитие коммуникативных навыков	Оперативное получение и обобщение информации об учебном процессе и успеваемости ребенка
Оперативный контроль учебного процесса для принятия управленческих решений	ЕИОП может выступать, как средство самообразования (создание условий для самостоятельной деятельности учащихся с использованием возможностей информационно-коммуникационных технологий)	Внеурочная деятельность (доступ к информации, банкам знаний, дистанционным ресурсам)	

Продолжение таблицы 1

Составление оптимального расписания, позволяющего максимально эффективно организовать образовательный процесс, используя имеющиеся информационные коммуникации и ресурсы компьютерных сетей	Формирование информационной культуры		
Использование сетевой системы документооборота	Разработка и подбор методик использования новых информационных технологий на занятиях		
Обеспечение материально–технического оснащения образовательного учреждения			
Содержательное наполнение информационных ресурсов			
Организация обучения кадров и создание мотивации использования информационно–коммуникационных технологий			

Анализируя уровни единого информационного пространства образовательного учреждения и происходящие в них процессы совершенно очевидно, что современные информационные технологии, внедряемые в сферу образования позволяют усилить интеллектуальные возможности обучающихся, способствуют интенсификации и персонализации процесса обучения и повышению его качества. Необходимо понимать, что изменение содержания одного компонента любого уровня приведет к изменению в

содержании всех других, и соответственно изменению всего информационно-образовательного пространства.

1.2 ЕДИНОЕ ИНФОРМАЦИОННОЕ ОБРАЗОВАТЕЛЬНОЕ ПРОСТРАНСТВО МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Муниципальное автономное общеобразовательное учреждение "Средняя общеобразовательная школа №21" - это самое молодое образовательное учреждение Миасского городского округа. Тем не менее, ей уже 13 лет и она входит ТОП 5 лучших учебных заведений города. В 2016 и 2017 году школа была обладателем гранта Правительства Челябинской области по программе «ТЕМП». В 2019 году вошло в список 300 лучших учебных заведений России.

За годы работы школа выпустила более 1200 учеников основной школы, 478 выпускников получили полное среднее образование. Практически все выпускники средней школы поступили в ведущие вузы страны и области на бюджетной основе. Обучающиеся школы традиционно имеют высокий бал на ЕГЭ, при этом отмечают, что занимались без репетиторов.

В школе работает талантливый коллектив педагогов, способный решать самые сложные образовательные задачи. В составе педагогов много победителей городских и областных конкурсов профессионального мастерства.

Школа одна из лидеров в области цифровизации образовательного процесса.

Муниципальное автономное общеобразовательное учреждение "Средняя общеобразовательная школа №21" расположено по адресу: 456300 Челябинская область, г. Миасс, Лихачева 33А, Телефон: 8(3513) 52-05-01.

Формы обучения, нормативные сроки обучения.

Начальное общее образование - 4 года.

Основное общее образование - 5 лет.

Среднее общее образование - 2 года.

Режим работы школы.

1-4 классы: 5-ти дневная рабочая неделя.

5-11 классы: 6-ти дневная рабочая неделя.

Учебный год делится на триместры:

I-триместр: с 01 сентября по 30 ноября.

II-триместр: с 01 декабря по 28 февраля.

III-триместр: с 01 марта по 31 мая.

Занятия организованны в две смены:

1 смена: 1,3,5,7,9,10,11 классы.

2 смена: 2,4,6,8 классы.

График работы школы:

с 08.00 часов до 20.30 часов.

Предмет, цели и виды деятельности МАОУ «СОШ №21».

Учреждение создано для выполнения работ, оказания услуг в целях обеспечения реализации предусмотренных законодательством Российской Федерации полномочий органов местного самоуправления Миасского городского округа в сфере образования и осуществляет в качестве основной цели его деятельности образовательную деятельность по образовательным программам начального общего, основного общего и среднего общего образования, а также реализации программ дополнительного образования.[74]

Предметом деятельности Учреждения является образовательная деятельность, направленная на реализацию общеобразовательных программ начального общего, основного общего и среднего общего образования.[74]

Целями деятельности Учреждения являются:

1. Осуществление образовательной деятельности по реализации образовательных программ различных видов, уровней и направлений.

2. На уровне начального общего образования - формирование личности обучающегося, развитие его индивидуальных способностей, положительной мотивации и умений в учебной деятельности (овладение чтением, письмом, счетом, основными навыками учебной деятельности, элементами теоретического мышления, простейшими навыками самоконтроля, культурой поведения и речи, основами личной гигиены и здорового образа жизни).

3. На уровне основного общего образования - становление и формирование личности обучающегося (формирование нравственных убеждений, эстетического вкуса и здорового образа жизни, высокой культуры межличностного и межэтнического общения, овладение основами наук, государственным языком Российской Федерации, навыками умственного и физического труда, развитие склонностей, интересов, способности к социальному самоопределению).

4. На уровне среднего общего образования - дальнейшее становление и формирование личности обучающегося, развитие интереса к познанию и творческих способностей обучающегося, формирование навыков самостоятельной учебной деятельности на основе индивидуализации и профессиональной ориентации содержания среднего общего образования, подготовку обучающегося к жизни в обществе, самостоятельному жизненному выбору, продолжению образования и началу профессиональной деятельности.

5. Формирование и развитие творческих способностей детей и взрослых, удовлетворение их индивидуальных потребностей в интеллектуальном, нравственном и физическом совершенствовании, формирование культуры здорового и безопасного образа жизни, укрепление здоровья, а также на организацию их свободного времени. [74]

Основными видами деятельности Учреждения, непосредственно направленными на достижение поставленных целей, являются:

1. Образовательная деятельность по реализации основной образовательной программы начального общего образования.

2. Образовательная деятельность по реализации основной образовательной программы основного общего образования.

3. Образовательная деятельность по реализации основной образовательной программы среднего общего образования.[74]

К дополнительным видам деятельности относятся:

1) реализация общеобразовательных программ сверх учебного плана, основных образовательных программ, федеральных государственных образовательных стандартов и федеральных государственных требований, финансируемых за счет средств бюджета;

2) реализация дополнительных общеобразовательных общеразвивающих программ для детей и взрослых;

3) деятельность по организации ухода и присмотра за детьми в дневное время;

4) деятельность столовой для питания детей и взрослых;

5) физкультурно-оздоровительная деятельность;

6) деятельность детских лагерей во время каникул и иные услуги в сфере оздоровления;

7) предоставление в аренду и (или) безвозмездное пользование недвижимого имущества, находящегося в оперативном управлении Учреждения;

8) прокат инвентаря для проведения отдыха и досуга;

9) деятельность по организации и постановке театральных представлений, концертов и прочих массовых мероприятий;

10) деятельность библиотек, клубов по интересам;

11) научная, методическая и (или) творческая деятельность;

12) организация олимпиад, конкурсов для обучающихся других образовательных организаций (за рамками реализации основных образовательных программ);

13) деятельность по организации психолого-медико-педагогического и социального консультирования;

14) осуществление копировальных и множительных работ с видеоносителей, звуковых носителей, текстовых материалов;

15) консультационные услуги специалистов: логопеда, психолога, социального педагога, методиста;

16) репетиторство с обучающимися других образовательных организаций.[74]

Рассмотрим систему единого информационного образовательного пространства на примере МАОУ «СОШ №21» города Миасса Челябинской области.

Единая информационная среда школы позволяет решить следующие задачи:

- создать единую для всей школы базу данных, содержащую информацию о различных аспектах учебно-воспитательного процесса: сведения о сотрудниках, учащихся и родителях, учебный план, электронный классный журнал, расписание, разнообразные отчеты и т.п.,

- обеспечивать использование в учебном процессе разнообразных образовательных– ресурсов (как готовых, так и собственной разработки), а также их интегрирование в единую среду,

- предоставить пользователям возможность общения между собой и доступа к общим ресурсам [80] (в МАОУ «СОШ №21» общение пользователей между собой организовано с помощью внутришкольного корпоративного чата),

- внедрить электронный документооборот по средствам выделенного файлового хранилища с последующим доступом пользователей к сетевым ресурсам,

- осуществлять бесперебойную техническую поддержку пользователей путем создания собственного сервера обработки заявок.

Взаимодействие основных информационных потоков в МАОУ «СОШ №21» можно представить следующим образом:

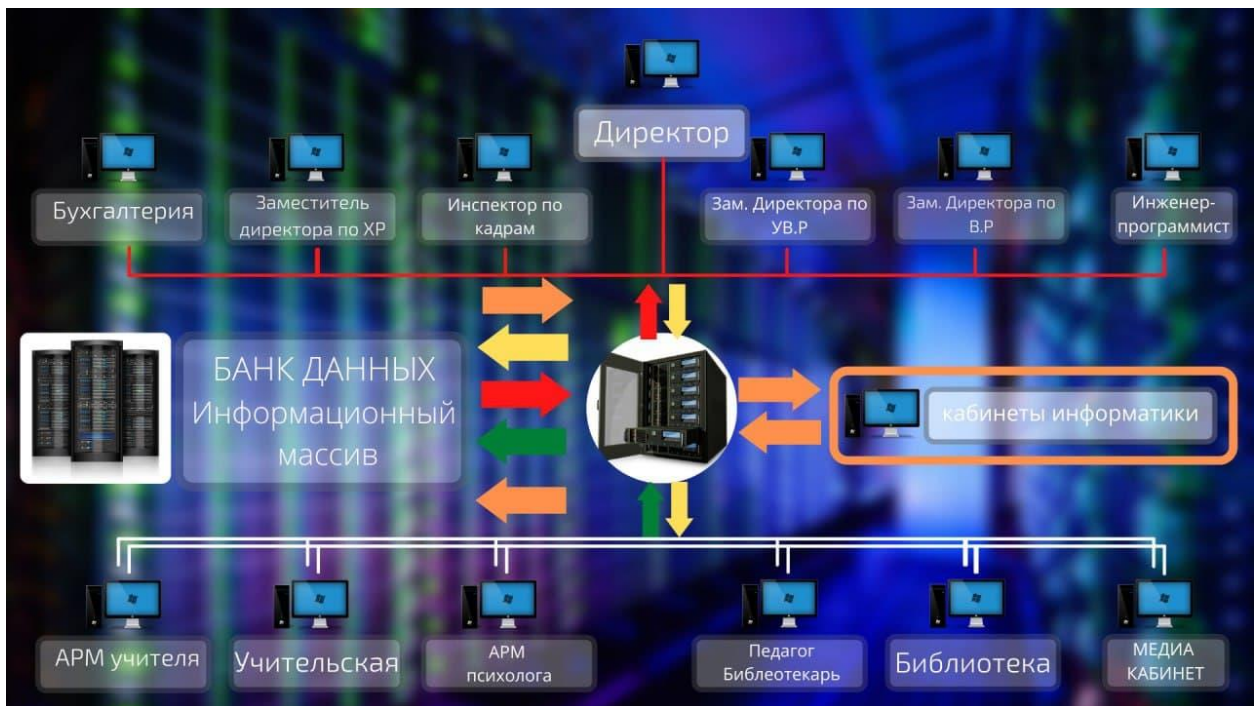


Рисунок 2. Взаимодействие основных информационных потоков МАОУ
«СОШ №21»

Основными пользователями ИСОУ являются:

- директор,
- зам. директора по учебно-воспитательной работе,
- зам.директора по ВР,
- зам. директора по ХЧ,
- инженер-программист,
- педагог-организатор,
- социальный педагог,
- психолог,
- секретарь,
- библиотекарь,
- классный руководитель,
- учитель-предметник,
- ученик,
- родитель.

Анализ представленной схемы взаимодействия основных информационных потоков позволяет сделать следующие выводы:

1. Основой для взаимодействия всех информационных потоков, отражающих основную деятельность образовательного учреждения, является информация общего доступа.

2. Информационные потоки тесно взаимодействуют между собой. Администрирование всех происходящих процессов строится на результатах работ по планированию, организации и управлению учебным процессом, за счет обработки и конкретизации информации общего доступа.

3. Дополнительное обеспечение деятельности образовательного учреждения, а точнее информационные потоки, отражающие процессы дополнительного обеспечения деятельности образовательного учреждения, опирается на информацию общего доступа и тесно взаимодействует с основными информационными потоками, а также между собой.

4. Пользователи ИСОУ это и есть некие информационные модули/блоки, формирующие структуру информационного пространства МАОУ «СОШ №21».

5. Основным пользователем и администратором информации общего доступа является директор школы (несмотря на то, что к выполнению части работ по наполнению данной информации привлекается секретарь). Директор формирует и утверждает такие данные как: учебный план, распределение педагогической нагрузки, штатное расписание образовательного учреждения и т.п.

Для получения полного представления об едином информационном образовательном пространстве МАОУ «СОШ №21» г. Миасса Челябинской области рассмотрим его с нескольких точек зрения: технической, организационной, а также с точки зрения программного обеспечения.

Единое информационное пространство школы реализуется на базе локальной вычислительной сети образовательного учреждения. Локальная сеть позволяет организовать хранение данных на одном носителе, а также обеспечивает удаленный доступ ко всем компьютерам.

Организационная структура локальной сети МАОУ «СОШ №21» г.

Миасса включает:

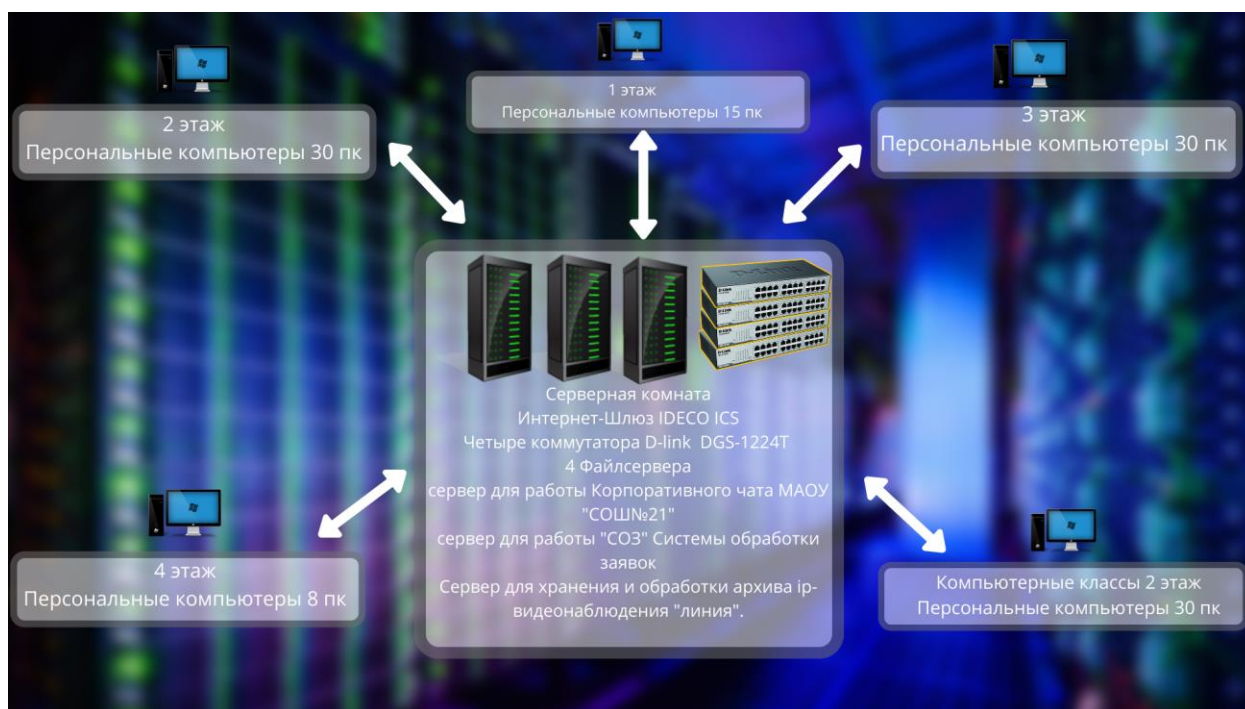


Рисунок 3. Организационная структура локальной сети МАОУ «СОШ №21» г. Миасса.

1. Интернет-Шлюз IDECO ICS.
2. Четыре коммутатора D-link DGS-1224T осуществляющих коммутацию сигналов.
3. Четыре выделенные сервера для хранения открытой и закрытой информации образовательного учреждения.
4. Выделенный сервер для работы Корпоративного чата МАОУ "СОШ№21" на базе open-source платформы rocket.chat.
5. Выделенный сервер для работы "СО3" Системы обработки заявок на базе OTRS 5.0 (открытой системы обработки заявок.).
6. Выделенный сервер, предназначенный для сканирования сети, мониторинга работы подключенных к ним устройств и предупреждения администратора в случае возникновения каких-либо проблем.
7. Сервер для хранения и обработки архива ip-видеонаблюдения "линия".

8. Компьютерные классы для преподавания курса информатики, для компьютерной поддержки общеобразовательных предметов, для организации внеклассной работы.

9. Мобильный компьютерный класс для преподавания курса информатики, для компьютерной поддержки общеобразовательных предметов, для организации внеклассной работы.

10. Автоматизированные рабочие места для административных работников, для сотрудников социально-психологической службы, для библиотеки, для методической работы, в учебных предметных кабинетах.

11. Малые информационные комплексы учебных кабинетов «АРМ учителя» (например, физики, химии) обеспечивают применение информационных технологий при организации фронтальной работы с классом (демонстрационный режим) и индивидуальной работы с 1 – 2 обучающимися.

12. Автоматизированные рабочие места (АРМ) сотрудников администрации образовательного учреждения, АРМ – «Директор», АРМ - «Зам.директора по УВР», АРМ - «Зам.директора по ВР», АРМ - «Зам.директора по АХЧ», АРМ - «Секретарь», АРМ - «Психолог».

Проприетарное программное обеспечение и свободное программное обеспечение единого информационного пространства складывается из:

1. Специализированного программного обеспечения для защиты сетевого периметра Ideco UTM (ранее - Ideco ICS), Dns-фильтрация по средствам сервиса Sky-dns.

2. Программного обеспечения общего назначения (текстовые и графические редакторы, электронные таблицы и др.); Пакет Microsoft Office 2007, Apache OpenOffice 4.1.7, Графический редактор GIMP.

3. Программного обеспечения для автоматизации деятельности различных служб (учета учащихся и родителей, кадрового учета, составления расписания, анализа успеваемости, и др.). В школе установлено программное обеспечение «1с Бухгалтерия».

4. Программно-методического обеспечения для организации учебно-воспитательного процесса (обучающие и развивающие компьютерные программы, электронные справочники, мультимедийные энциклопедии и др.).

5. Информационных ресурсов образовательного учреждения (единая база данных, мультимедийные учебные разработки, хранилище документов, веб-сайт).

С точки зрения тех видов деятельности образовательного учреждения, которые реализуются на основе единого информационного пространства школы, его структура может быть представлена следующим образом:



Рисунок 4. Информационное пространство образовательной организации с точки зрения видов деятельности.

1. Учебно-воспитательная работа: обучающие программы, тренажеры, тестовые системы, медиатеки и электронные энциклопедии, ресурсы Интернета, операционные системы и прикладные программы иного назначения.

2. Управление образовательным процессом: системы учета успеваемости и личных достижений обучающихся, программы составления и редактирования учебной нагрузки, расписания занятий, базы данных по работникам образовательного учреждения и обучающимся.

3. Управление контингентом обучающихся: базы данных по обучающимся, содержащие полные персональные данные, включая сведения по успеваемости и достижениям.

4. Управление кадрами образовательного учреждения: базы данных по работникам, содержащие персональные данные, с возможностью получения сведений о результативности профессиональной деятельности, повышении квалификации, программы подсчета стажа, составления тарификации и т.д.

5. Управление ресурсами: базы данных по обучающимся и кадрам, фондам библиотеки, помещениям, оборудованию, УМК и т. д.

6. Обеспечение коммуникаций.[80]

С точки зрения программного обеспечения, структура единого информационного пространства МАОУ «СОШ №21» представлена ниже:



Рисунок 5. Структура применяемого ПО в МАОУ «СОШ №21» г. Миасса

Основным фактором, обеспечивающим рациональное использование единого информационного образовательного пространства образовательного учреждения, является интеграция программных, технологических и информационных ресурсов в единый комплекс. Выработка единых

технологических решений внутри данного комплекса позволяет оптимизировать работу всего учреждения.

Таким образом, можно сделать вывод, что единое информационное образовательное пространство МАОУ «СОШ №21» г. Миасса Челябинской области соответствует системе задач, которые решаются образовательным учреждением. Участники, вовлеченные в процесс пользования ресурсами единого информационного пространства, четко определены. Программное обеспечение приведено в соответствие с действующим и законодательством и определено финансированием учреждения. Рассмотрев действующее единое информационное образовательное пространство МАОУ «СОШ №21» г. Миасса Челябинской области и изучив нормативно-правовое обеспечение информационной безопасности в образовательном учреждении нами считается необходимым провести анализ уязвимостей данного пространства и разработать наиболее приемлемое техническое решение для создания инфраструктуры информационной среды, учитывая все недостатки. А также определить порядок проведения работ по созданию информационной среды, которая позволит оптимизировать управление, как образовательным процессом, так и образовательным учреждением в целом.

1.3 АНАЛИЗ УЯЗВИМОСТЕЙ ЕДИНОГО ИНФОРМАЦИОННОГО ОБРАЗОВАТЕЛЬНОГО ПРОСТРАНСТВА МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Говоря об уязвимости единого информационного образовательного пространства школы мы обращаемся к ГОСТ Р 56546-2015 Защита информации, который дает нам следующее определение уязвимости:

Уязвимость: Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.[16]

Анализ уязвимостей — это организованный процесс поиска уязвимых мест, угроз, потенциальных способов их осуществления и моделей работы злоумышленников, вовлеченных в эти процессы.[82]

Уязвимость представляет собой слабый компонент в информационной системе любой организации. Угрозой может выступить любое возможное явление или процесс, которые могут скомпрометировать информацию и нарушить основополагающие принципы информационной безопасности.

Анализ уязвимостей единого информационного образовательного пространства школы, на наш взгляд, должен осуществляться по двум направлениям:

1. Анализ информационной среды образовательного учреждения.
2. Анализ источников угроз.

Виды угроз для анализа

Анализ уязвимостей информационной системы возможен только при понимании типов угроз, которые возникают в информационном поле предприятия. Существует несколько способов их классификации.

По состоянию источника угрозы:

- непосредственно в ИС;
- в пределах видимости ИС (например, подслушивающие устройства);
- вне зоны действия/видимости ИС (перехват данных во время прохождения каналами связи).

По степени воздействия:

- несут активную угрозу (вирусы, троянские программы);
- несут пассивную угрозу (кража информации копированием).

По способу доступа:

- через нестандартные каналы связи (например, уязвимости ОС);
- напрямую (через кражу паролей). [19]

Главные цели атаки на информационное образовательное пространство — получения доступа и контроля над ценными информационными

ресурсами, а также препятствие полноценной деятельности организации, путем нарушения работы программ дистанционного обучения и систем оценивания учеников. Угрозы могут быть реализованы путем перехвата данных и нарушения работы локальных сетей.

Информационной безопасности угрожают:

- вредоносное программное обеспечение и хакеры/мошенники;
- сотрудники-инсайдеры (злонамеренные или незлонамеренные);
- стихийные бедствия (пожары, наводнения, аварии на энергосистемах).[82]

Оценка вероятности угроз

Чтобы оценить вероятность наступления угроз, используют трехуровневую качественную шкалу:

Первый уровень — Н, или «низкая вероятность». У нее минимальная вероятность наступления и нет предпосылок (мотивов, инцидентов в прошлом) для того, чтобы реализовать угрозу на практике. Угрозы с низкой вероятностью приводят к реальным инцидентам не чаще одного раза в 5—10 лет.[82]

Второй уровень — С, или «средняя вероятность». Вероятность осуществления такой угрозы выше, чем в предыдущем случае, так как в прошлом имели место аналогичные инциденты, есть информация, что атакующая сторона имеет намерения и/или возможности реализовать их в отношении объекта. Угрозы со средней вероятностью приводят к реальным инцидентам в среднем раз в году.[82]

Третий уровень — В, или «высокая вероятность». Угроза с самыми высокими шансами осуществления. Их подтверждают статистические данные, произошедшие ранее инциденты, серьезные мотивы со стороны атакующей стороны. Ожидать реализацию этой угрозы можно раз в неделю или чаще.[82]

Методы анализа уязвимостей

Есть несколько методик, которые позволяют выполнить анализ уязвимостей системы. Одна из них базируется на вероятностном подходе и учитывает факторы:

1. Потенциал нарушителя: определяется на основе экспертных оценок.
2. Источник угрозы: атака возможна в контролируемой зоне или за ее пределами.
3. Способ воздействия: технический, сетевой или социальный канал.
4. Объект угроз: конфиденциальная информация, средства ее доставки/обработки/хранения, или штатные сотрудники компании.

При анализе уязвимостей ИС важно учесть возможные места дислокации. Для этого выявляют и устраняют ошибки в ОС и прикладном программном обеспечении, а в будущем регулярно и оперативно устанавливать патчи от разработчиков ПО. Для тех уязвимостей, которые связаны с некорректной настройкой средств защиты, регулярно проверяют и выполняют ИТ-аудит систем защиты информации, а в идеале настраивают непрерывный мониторинг. Отдельно проводится работа с сотрудниками предприятия: раздают права доступа, используют ограничения на установку специального ПО, копирование данных, использование внешних носителей информации.

Компания Microsoft предлагает методику STRIDE для определения и категоризации угроз.[89]

Моделирование при помощи STRIDE поможет обеспечить исполнение в информационной системе всех свойств безопасности. STRIDE – аббревиатура от:

- Spoofing Identity (подмена личности).
- Tampering with Data (изменение данных).
- Repudiation (отказ от совершенной операции).

- Information Disclosure (разглашение сведений).
- Denial of Service (отказ в обслуживании).
- Elevation of Privilege (повышение прав доступа).

По этой методике определяются угрозы для каждого компонента информационной системы в зависимости от категории угрозы. Угрозы типа «Подмена личности» актуальны для систем, в которых реализуются разные уровни доступа пользователей. Пользователь не должен иметь возможность притвориться другим пользователем или прочитать атрибуты другого пользователя. Угрозы типа «Изменение данных» реализуют возможность пользователя повлиять на логику работы системы через доступные интерфейсы. Система должна тщательно проверять все исходящие от пользователя данные в процессе их использования и вплоть до момента их сохранения в системе. При недостаточном аудите транзакций в системе угрозы типа «Отказ от совершенной операции» реализуют возможность пользователя отказаться от выполненных им каких-либо действий в системе, что может повлиять на достоверность циркулирующей по системе информации. Например, пользователь может заявить «Я не перечислял денежные средства на этот счет». При недостаточном аудите операций невозможно проверить данное заявление. Угрозы типа «Разглашение сведений» реализуют возможность публикации конфиденциальных данных в системе. Возможно, в системе обнаружится утечка информации. Дизайнеры системы также должны учитывать тот факт, что на нее будут проводиться атаки типа DoS (отказ в обслуживании). Необходимо убедиться, что ресурсоемкие процессы будут недоступны неавторизованным пользователям. Такими процессами могут являться: чтение больших файлов, сложные вычисления, исполнение длинных запросов к базе данных и т.д. Если в системе различаются пользовательские и административные роли, то необходимо убедиться в невозможности повышения прав доступа. Все действия в системе должны проверяться по матрице доступа. На следующем

этапе моделирования все определенные угрозы необходимо зафиксировать в представленном далее виде:

- Описание угрозы.
- Объект возможной атаки.
- Риск.
- Возможный сценарий атаки.
- Предпринимаемые меры по устранению угрозы.

На последнем этапе процесса расставляются приоритеты по устранению угроз в зависимости от их риска. Это позволит заняться в первую очередь угрозами, которые могут нанести системе наибольший ущерб. Экономически невыгодно устранять абсолютно все определенные угрозы, поэтому возможно опустить угрозы, вероятность реализации которых стремится к нулю и ущерб от которых минимален. В итоге, для разработчиков информационной системы представляется документ, позволяющий им сформировать отчетливое понимание о потенциальных угрозах и рисках.

SWOT анализ деятельности образовательного учреждения, на наш взгляд, является универсальным маркетинговым инструментом. Он позволяет обобщить и сопоставить данные совершенно разного типа и назначения, и именно поэтому может быть применен по отношению к любой организации, в том числе и образовательной.

Изначально методика, разработанная американскими профессорами Гарвардского университета в 1965 году, применялась для анализа и разработки бизнес-стратегии развития предприятия или объекта. Сейчас SWOT-анализ широко распространен в различных областях науки и практики как метод стратегического планирования, заключающийся в выявлении факторов внутренней и внешней среды организации и разделении их на четыре категории:

- Strengths (сильные стороны),
- Weaknesses (слабые стороны),

- Opportunities (возможности),
- Threats (угрозы).[40]

Используя метод наблюдения и опроса (коллектив МАОУ «СОШ №21»), а также применив исследовательский метод анализа научной литературы [31,32,33,34,35] с целью определения уязвимостей единого информационного образовательного пространства МАОУ «СОШ №21» г. Миасса Челябинской в 2020 учебном году нам удалось провести SWOT-анализ состояния информационного образовательного процесса. Корректировка численных значений показателей произведена на 01.09.2021 года. Результаты представлены в таблице 2.

Таблица 2 - SWOT-анализ информационно-образовательного пространства МАОУ «СОШ №21» г. Миасса Челябинской области

Внутренняя среда	Внешняя среда
<p style="text-align: center;">Сильные стороны</p> <p>Материально-технические условия</p> <ol style="list-style-type: none"> 1. Локальная сеть присутствует во всех помещениях школы. 2. Серверное помещение 3. Система видеонаблюдения 4. Парк серверов 5. Использование электронного журнала и электронного дневника Сетевой город (sgo.edu.ru) 6. В каждом кабинете, оснащённом компьютером, есть высокоскоростной интернет 7. Закупка новых компьютеров и мультимедийных комплексов в предметные кабинеты и библиотеку 8. Лицензионное или (СПО) программное обеспечение на всех компьютерах 9. Осуществляется dns контент-фильтрация от Skydns 10. Интерактивные доски (6) 11. Кабинеты информатики(2) 12. Мобильный компьютерный класс (14+1) 13. Библиотека 14. Принтеры (20), сканеры(20), многофункциональные устройства МФУ(25) 15. Цифровой микроскоп (2) 	<p style="text-align: center;">Возможности</p> <p>Политика государства в области информатизации образования</p> <ol style="list-style-type: none"> 1. Федеральный закон от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации» 2. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» 3. Приоритетный национальный проект «Образование» 4. Проект «Цифровая образовательная среда» 5. Федеральный закон Российской Федерации от 27 июля 2006 г. N152 "О персональных данных" <p>Преимущества, которые может обеспечить политика государства в области образования</p> <ol style="list-style-type: none"> 1. Омоложение педагогического коллектива 2. Средняя заработная плата педагогических работников общеобразовательных организаций составит не менее 100 % от средней заработной платы по экономике региона 3. Повысится привлекательность педагогической профессии и уровень квалификации преподавательских кадров 4. Молодые учителя, успешно

Продолжение таблицы 2

<p>16. Цифровые видеокамеры (3) 17. Фотоаппарат (3) 18. Программа составления расписания "Расписание 2021" 19. Электронные учебники -ЦОР-библиотека</p> <p style="text-align: center;">Кадровые условия</p> <p>1. Наличие IT службы 2. ИКТ-грамотные учителя (владеющие программами Word, PowerPoint, Excel, использующие электронную почту, умеющие найти нужную информацию в Интернете) (общее кол-во учителей 72) по результатам самооценки (Приложение 1) 3. Группы в социальной сети в контакте методических объединений (6) 4. 40% учителей приняли участие в сетевых образовательных проектах 5. 69% учителей приняли участие в сетевых олимпиадах, конкурсах и интеллектуальных играх 6. Двенадцать обученных учителей по программе «Дистанционное обучение»</p> <p style="text-align: center;">Информационные условия:</p> <p>1. Сайт школы, отвечающий требованиям закона «Об образовании в Российской Федерации» №273-ФЗ от 29.12.2012 (https://sch21-miass.educhel.ru/) 2. Электронная почта (school21_miass@mail.ru) 3. Сообщество в социальной сети ВК (https://vk.com/shkola21_miass) 4. Школьный пресс-центр «МедиаКомар» (https://vk.com/mediamosquito) 5. Электронные паспорта кабинетов 6. Оснащённость библиотеки электронными образовательными ресурсами 7. Есть родители (7%), поддерживающие своих детей и образовательное учреждение в новых образовательных проектах.</p> <p style="text-align: center;">Управление информационной средой</p> <p>1. Наличие в школе корпоративной сети. 2. Современное поколение детей адаптировано к работе в Интернете, что способствует внедрению воспитательных</p>	<p>закрепившиеся в школе, получают возможность взять льготный ипотечный кредит для приобретения жилья 5. Новые требования при аттестации педагогических работников 6. Возможный переход на эффективный контракт 7. Приказ Минтруда России от 18.10.2013 N 544н "Об утверждении профессионального стандарта "Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)"</p> <p style="text-align: center;">Управление информационной средой</p> <p>1. Педагогическое сопровождение процесса воспитания в ЦОС. 2. Обновление и модернизация технологий, методов и форм воспитания в условиях ЦОС. 3. Изменение педагогических функций (организация и поддержка учебно-воспитательного сотрудничества, коммуникации) через использование таких сервисов, как форум, дискуссия, чат, социальные сети и др. 4. Создание условий для формирования стратегий самообразования, самообучения и самовоспитания. 5. Формирование системы мотивации коллектива школы к эффективному освоению и применению разных форм ИТ, в том числе: технологий электронного обучения и дистанционных образовательных технологий, освоения современных программных продуктов, работы в информационных системах школы и системах электронного документооборота. 6. Развитие информационной системы школы, с точки зрения, повышения уровня защищенности информации.</p>
---	--

Продолжение таблицы 2

<p>задач именно в цифровой образовательный процесс.</p> <p>3. В условиях пандемии разнообразие форм коммуникации (видеосвязь, голосовые и текстовые сообщения, презентации и проектная деятельность) на технической базе МАОУ «СОШ №21» способствует постоянному взаимодействию преподавателей и учеников.</p> <p>4. Прослеживается смена воспитания социальной ответственности с системы отношений «человек-общество» в систему отношений «человек – цифровые средства – общество»;</p> <p>5. воспитание культуры сетевой коммуникации у преподавательского состава;</p> <p>воспитание адаптивности, толерантности к неопределенности, гибкости, чего требует трансформация образования (переход на дистанционный формат, например);</p> <p>6. расширение кругозора обучающихся посредством разнообразных информационно-коммуникационных технологий (ИКТ).</p>	
<p style="text-align: center;">Слабые стороны</p> <p>1. Не используются все возможности интерактивных досок (анализ посещённых уроков)</p> <p>2. Устаревший парк коммутационного оборудования в серверной комнате</p> <p>3. Нет опыта создания собственных Интернет - проектов</p> <p>4. Недостаточная активность учителей в области использования на уроках цифровых инструментов (анализ посещённых уроков)</p> <p>5. Малое количество педагогов поддерживающие собственные блоги</p> <p>6. Не используются образовательные возможности сервисов WEB 2.0. для коллективного педагогического взаимодействия</p> <p>7. Не используются все возможности Сетевой город (sgo.edu.ru) для индивидуального обучения</p> <p>8. Нехватка учителей Информатики и ИКТ</p> <p>9. Не полностью используются возможности классного дневника (sgo.edu.ru) для выстраивания системы взаимодействия с родителями.</p>	<p style="text-align: center;">Угрозы</p> <p>1. Ухудшение здоровья школьников (ослабление зрения)</p> <p>2. Увеличение численности контингента учащихся</p> <p>3. Большая учебная нагрузка у большинства учителей</p> <p>4. Недостаточная компетентность большей части родителей в области ИКТ может стать препятствием для сетевого взаимодействия участников образовательного процесса</p> <p>5. Отсутствие финансирования для постоянного технико-технологического сопровождения педагогов и учащихся в области использования сетевых технологий, необходимого в связи с динамично обновляющимися сервисами современного Интернета.</p> <p style="text-align: center;">Управление информационной средой</p> <p>1. Риски в развитии информационно-образовательной пространства школы связаны с нечеткостью нормативной базы в области применения ИТ технологий в</p>

Продолжение таблицы 2

<p>10. Только 3 классных коллектива имеют свои сайты в сети Интернет</p> <p>11. Нет механизма выявления и распространения точечных педагогических практик использования сетевых технологий и цифровых инструментов.</p> <p>Управление информационной средой</p> <p>1. Технические ограничения серверов школы.</p> <p>2. Низкий уровень квалификации преподавательского состава в области ИТ, неготовность преподавателей работать с ИКТ.</p> <p>3. Неструктурированное, педагогически нецелесообразное использование виртуального пространства и ИКТ.</p> <p>4. Изменение образовательных условий, которые мы можем наблюдать в связи с эпидемиологической ситуации в стране, влияет на выстраивание коммуникации, которая становится опосредованной (через форумы и чаты).</p> <p>5. Неготовность некоторых преподавателей к работе с цифровыми технологиями;</p> <p>6. Недостаточная методическая изученность некоторых ИКТ для реализации воспитательных целей и задач;</p> <p>7. Недоступность Интернета и отсутствие цифровых носителей (компьютеров) для работы в условиях дистанционного обучение у некоторых учеников.</p>	<p>2. образовании.</p> <p>3. Преувеличение возможностей цифровой образовательной среды, цифровых ресурсов и средств обучения без учета финансовых возможностей учреждения.</p> <p>4. Недооценка значимости человеческого фактора в образовательном процессе, в процессе организации информационной безопасности.</p> <p>5. Риск использования ИКТ без учета их воспитательной составляющей не приводит к положительным изменениям в системе воспитания в новых условиях.</p> <p>5. Недостаточный положительный эффект от информатизации в школе вследствие естественного старения преподавательского состава.</p>
---	---

Используя в качестве инструмента SWOT-анализ, нам удалось структурировать имеющуюся информацию об информационно-образовательном пространстве МАОУ «СОШ №21». Факт наличия в школе единого информационно-образовательного пространства очевиден. Но, к сожалению, такой анализ не дает нам, в конечном счете, конкретных рекомендаций по рассматриваемому объекту. В результате анализа большого количества исходной информации, и по итогам работы с матрицей (таблица 2), были сформулированы следующие выводы:

В школе существуют благоприятные условия для развития информационно-образовательного пространства:

- 1) организовано 35 автоматизированных рабочих мест учителей;
- 2) все компьютеры (более 100 машин) подключены к сети Интернет (100Мб/сек);
- 3) все сотрудники администрации регулярно используют компьютер для подготовки документов (текущее делопроизводство), и сбора информации об учебном процессе;
- 4) школа укомплектована кадрами с высоким уровнем квалификации;
- 5) используется электронный журнал для мониторинга успеваемости и организации обратной связи с родителями учащихся.

Выявленные недостатки:

- 1) недостаточно высокий уровень мотивации педагогических работников к освоению и использованию новых ИКТ-технологий;
- 2) технические возможности, предоставляемые школой, не используются или используются нерационально.

То есть возможности для развития ИОП школы достаточны. Школа располагает всеми необходимыми ресурсами и инфраструктурой для осуществления образовательной деятельности. Материально-техническая база школы позволяет в полной мере решать задачи обучения и воспитания детей. Но неоспорим тот факт, что педагогический коллектив с высоким профессиональным уровнем и творческим потенциалом имеет недостаточный уровень информационной и компьютерной грамотности, что снижает продуктивность образовательных усилий, а также препятствует адаптации педагога в современных условиях использования технологий. Зачастую, под этой неграмотностью скрывается обычная боязнь нововведений. Рассматривая единое информационное пространство образовательного учреждения – школы, под информационной грамотностью персонала будем понимать состояние гарантированной доступности ко всем информационным ресурсам учреждения, необходимой для его устойчивого

существования и развития. Под компьютерной грамотностью персонала — обеспеченность надежной защитой учеников и сотрудников, от несанкционированного доступа к конфиденциальной информации и защищенности от воздействия на них угроз.

Основные направления, которым необходимо уделять особое внимание при развитии компьютерной грамотности персонала школы:

1. Барьер непонимания между ИТ-специалистами и персоналом школы.

Умение пользоваться необходимыми для работы программами и понимание работы базовых элементов операционной системы значительно бы снизили временные затраты технических специалистов на устранение ошибок, совершенных из-за компьютерной неграмотности. Такая неграмотность замедляет рабочий процесс.

Защита информационного пространства школы не будет надежной до тех пор, пока весь персонал не будет обладать компетенцией в области компьютерных технологий.

2. Контроль использования USB-устройств.

Частая причина утечки информации, заражения компьютера и даже остановки всего учебного процесса.

Персонал учили четко соблюдать требования охраны труда, применять педагогические технологии и соблюдать стандарт педагога, но никто не объяснял, что вставить USB-накопитель в компьютер, подключенный к АСУ школы, может быть опасно.

3. Отсутствие культуры защиты информации.

Подразумевает строгое выполнение базовых вещей: обновление антивирусных программ, своевременная установка патчей, аккуратная работа с почтовыми сервисами.

Речь идет не об умении персонала самому выполнять данные виды работ, для таких работ существуют ИТ-специалисты. Необходимо повышение социальной ответственности персонала. Умения работы с компьютером

недостаточно, необходимо научить персонал быстро среагировать на вероятную угрозу. Своевременное реагирование на проблему - основа безопасности.

4. Популяризация инноваций.

Инновационная работа в школе должна быть организована по следующим направлениям:

- 1) организация интеллектуально – творческой работы учителей;
- 2) организация интеллектуально-творческой деятельности учащихся;
- 3) информатизация образовательного пространства;
- 4) работа над созданием имиджа школы, благоприятной воспитательной среды.

Под популяризацией инноваций мы понимаем не функционирующие на базе образовательного учреждения инновационные площадки (работающие по направлениям, указанным выше), а формы и методы организации учебного процесса. Сама система образования меняется с течением времени и переходом к информационному обществу. Соответственно, предъявляются и новые требования к интеллектуальным параметрам сотрудников школы.

5. Сокращение «цифрового разрыва» с упором на обучение учителей.

Организация безопасного единого информационного пространства школы, невозможно без повышения уровня информационной и компьютерной грамотности персонала. Это представляет собой сложную, многоаспектную проблему, для решения которой, требуется объединение усилий всех участников образовательного процесса, государства и общества. Информационное пространство школы должно быть структурировано, иметь различные уровни доступа и соответствовать требованиям законодательства в сфере информационной безопасности.

Возникает потребность в создании единого информационного пространства на основе уже существующей аппаратной, программной и административной базы. Нами разработаны рекомендации по техническому

обеспечению ИБ в МАОУ «СОШ №21» г. Миасса Челябинской области. Главным направлением по организации единого информационного пространства МАОУ «СОШ №21» на 2020-2021 учебный год в условиях обеспечения информационной безопасности, считаем – внедрение модели защищенного информационного хранилища с распределением прав пользователей.

ГЛАВА 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1 НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ, МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКОЙ ОБЛАСТИ

НОРМА ПРАВА — общеобязательное, формально определенное правило поведения, установленное либо санкционированное государством и направленное на урегулирование общественных отношений.[54]

Одной из 4 форм права является нормативно-правовой акт.

В российском праве нормативно-правовой акт является основным источником права.

Основные характеристики нормативно-правовых актов:

1. Наиболее точно отражают содержание норм права.
2. Наиболее оперативно позволяют изменять отраженные в них нормы.
3. Доступны и удобны в использовании.
4. В масштабах страны составляют единую стройную соподчиненную систему.[50]

Законодательство РФ об информации, информационных технологиях и о защите информации основывается на Конституции РФ (принята всенародным голосованием 12.12.1993), международных договорах РФ и состоит из многих ФЗ, основные из которых мы рассмотрим ниже.

Нормативно-правовое обеспечение информационной безопасности в образовательной организации представляет собой действующие в этой сфере законы и локальные акты, которые определяют административные, организационные, технические, программно-аппаратные средства для осуществления деятельности в данном направлении. В таких официальных документах определяются, так называемые «массивы» информации, подлежащие защите. Закон выделяет сведения, которые должны быть

недоступны третьим лицам по разным причинам (конфиденциальная информация, персональные данные, коммерческая, служебная или профессиональная тайна), и устанавливает методику для обеспечения защиты таких сведений.

Правовые акты общего назначения, затрагивающие вопросы информационной безопасности

Основой нормативно-правового обеспечения информационной безопасности в образовательной организации выступает высший нормативный правовой акт Российской Федерации – Конституция РФ. Конституция определяет правовые основы информационной безопасности: основные положения правового статуса субъектов информационных отношений, принципы информационной безопасности (законности, уважения прав, баланс интересов личности, общества и государства), конституционный статус государственных органов, обеспечивающих информационную безопасность и прочие. Глава 2 п.4.ст.29 устанавливает право каждого субъекта свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Для формирования комплекса организационных мер по обеспечению защиты всех типов информации привлекаются нормы административного и трудового права. А ответственность за нарушение информационного законодательства предусматривают нормы базовых отраслей права (уголовного, административного, трудового).

В современных условиях практичным и наиболее удобным для граждан считается создание соответствующими законодательными, исполнительными и судебными органами власти информационных серверов, нежели использование бумажных носителей. Соответственно для таких серверов должна быть обеспечена информационная безопасность, в которую входит:

1. Поддержание доступности и целостности информации.
2. Обеспечение конфиденциальности данных.
3. Возможность пользователя применять средства защиты информации.

УК РФ Статья 159.6. Мошенничество в сфере компьютерной информации (введена Федеральным законом от 29.11.2012 N 207-ФЗ) предусматривает наказание за хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.[72]

Трудовой кодекс РФ определяет общие требования по обработке и защите персональных данных работника, устанавливает сроки хранения таких данных и процедуру их использования, передачи, а также права работников в целях обеспечения защиты ПД, хранящихся у работодателя. Этим нормам полностью посвящена глава 14 ТК РФ. В случаях нарушения норм, регулирующих получение, обработку и защиту персональных данных работника, виновные лица (согласно ст. 90 ТК РФ) привлекаются к дисциплинарной, материальной, административной, гражданско-правовой и уголовной ответственности. Трудовой кодекс РФ определяет норму об ответственности за разглашение отдельных видов тайн и персональных данных.[69]

Обзор Федерального законодательства.

Федеральный закон от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

В нем закреплены правовые основы осуществления надзора в сфере защиты от информации, причиняющей вред. В целях реализации данной нормы были распределены полномочия между Роскомнадзор, Роспотребнадзор, Рособрнадзор, Минкульт.

Основной проблемный аспект реализации данного Федерального закона сводится к сложности выполнения администрацией образовательных учреждений требований ч. 1 ст. 14 Федерального закона № 436-ФЗ о применении административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации,

причиняющей вред их здоровью и (или) развитию, в местах доступа к Интернету.

Как мы знаем, доступ к Интернету в школах осуществляется преимущественно в рамках реализации национального проекта «Образование», стартовавшего в 2006 г. На сегодняшний день, данный национальный проект также существует и предполагает создание к 2024 году современной и безопасной цифровой образовательной среды, обеспечивающей высокое качество и доступность образования всех видов и уровней. А самое главное предусматривается обновление материально-технической базы, которое позволит внедрить новые методы обучения и воспитания.

11 мая 2011 г. Минобрнауки России № АФ-12/07вн были утверждены Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации (далее - Правила фильтрации). От установленных средств фильтрации требуется обеспечить фильтрацию по технологии «черных списков» ресурсов, определенных Минобрнауки России и размещенных на указанном сайте.

Согласно этим Правилам школы обязали установить средства контентной фильтрации (далее - СКФ), представлявшие собой аппаратно-программные или программные комплексы. При этом руководителям учреждений предоставлена возможность выбора СКФ рекомендованных Минобрнауки России, либо приобретенных самостоятельно.

В настоящее время школы зачастую самостоятельно заключают договоры с коммерческими организациями (например, МАОУ СОШ№21 работает с ООО «СкайДНС»), которые предоставляют СКФ. То есть не утверждено актуального, обновляемого перечня СКФ, утвержденных, а не рекомендованных, для использования. Руководителям предоставляют право выбора, которое впоследствии может вылиться в нарушение законодательства. Формально выполняя требования правил фильтрации и

устанавливая необходимые программно-аппаратные средства, очевидно, что администрация общеобразовательного учреждения не обладает необходимыми информационными и организационными ресурсами для того, чтобы адекватно оценить и проверить работу СКФ.

Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».

Данный федеральный закон является базовым национальным нормативным актом, регламентирующим отношения в сфере хранения и обработки персональных данных.

В нем даются основные определения:

персональные данные (ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.[77]

В статье 5 Закона определяются принципы обработки персональных данных:

1) законности целей и способов обработки персональных данных и добросовестности;

2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

5) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.[78]

Также в Законе оператор персональных данных обязывается зарегистрировать созданные им информационные системы персональных данных и выполнять требования на защиту персональных данных:

«Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий».[78]

Правительство РФ устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

С 1 сентября 2015 года вступили в силу поправки к закону, касающиеся работы почтовых серверов и социальных сетей. Теперь при регистрации почты или в соцсети запрашивают контактные и личные данные граждан. С этого момента любая организация, работающая с российскими потребителями, должна обеспечить запись, систематизацию, накопление,

хранение, а также уточнение персональных данных граждан с использованием баз данных, которые находятся на российской территории.

Роскомнадзор, который ведет единый государственный реестр РФ информационных систем персональных данных, наделяется правом блокировать сайты, на которых содержатся персональные данные граждан, полученные с нарушением законодательства. Также регуляторами в сфере защиты персональных данных являются:

- ФСТЭК России (привлекается к проверке систем защиты ПДн);
- ФСБ России (привлекается к проверке в случае наличия в системе криптографических средств защиты информации и систем обнаружения атак).

В работе школы сбор, обработку, распространение и использование персональных данных учащегося, его родителей, а также сотрудников образовательной организации регулирует ФЗ 152. Такие сведения являются конфиденциальной информацией и не могут быть использованы администрацией или любым иным лицом в личных целях.

Некоторые аспекты, касающиеся личных данных обучающегося, отражены в Приказах Министерства образования и науки РФ:

1. Приказ Министерства просвещения Российской Федерации от 02.09.2020 г. № 458 "Об утверждении Порядка приема на обучение по образовательным программам начального общего, основного общего и среднего общего образования".
2. Приказ Министерства образования и науки РФ от 12 марта 2014 г. N 177 «Об утверждении Порядка и условий осуществления перевода обучающихся из одной организации, осуществляющей образовательную деятельность по образовательным программам начального общего, основного общего и среднего общего образования, в другие организации, осуществляющие образовательную деятельность по образовательным программам соответствующих уровня и направленности».

Предоставление персональных данных носит добровольный характер, сообщать данные или нет, решает каждый человек самостоятельно. Однако, в приказе №458 отражена информация, которую родители должны предоставлять учебному заведению, если хотят, чтобы ребенок был туда принят.

К обязательной информации, указываемой в заявлении о приеме на обучение родителем (законным представителем) ребенка относится:

- фамилия, имя, отчество (при наличии) ребенка или поступающего,
- дата рождения ребенка или поступающего,
- адрес места жительства и (или) адрес места пребывания ребенка или поступающего,
- фамилия, имя, отчество (при наличии) родителя(ей) (законного(ых) представителя(ей) ребенка, адрес места жительства и (или) адрес места пребывания родителя(ей) (законного(ых) представителя(ей) ребенка,
- адрес(а) электронной почты, номер(а) телефона(ов) (при наличии) родителя(ей) (законного(ых) представителя(ей) ребенка или поступающего,
- о наличии права внеочередного, первоочередного или преимущественного приема,
- о потребности ребенка или поступающего в обучении по адаптированной образовательной программе и (или) в создании специальных условий для организации обучения и воспитания обучающегося с ограниченными возможностями здоровья в соответствии с заключением психолого-медико-педагогической комиссии (при наличии) или инвалида (ребенка-инвалида) в соответствии с индивидуальной программой реабилитации,
- согласие родителя(ей) (законного(ых) представителя(ей) ребенка на обучение ребенка по адаптированной образовательной программе (в случае необходимости обучения ребенка по адаптированной образовательной программе),

- согласие поступающего, достигшего возраста восемнадцати лет, на обучение по адаптированной образовательной программе (в случае необходимости обучения указанного поступающего по адаптированной образовательной программе),
- язык образования (в случае получения образования на родном языке из числа языков народов Российской Федерации или на иностранном языке),
- родной язык из числа языков народов Российской Федерации (в случае реализации права на изучение родного языка из числа языков народов Российской Федерации, в том числе русского языка как родного языка),
- государственный язык республики Российской Федерации (в случае предоставления общеобразовательной организацией возможности изучения государственного языка республики Российской Федерации),
- факт ознакомления родителя(ей) (законного(ых) представителя(ей) ребенка или поступающего с уставом, с лицензией на осуществление образовательной деятельности, со свидетельством о государственной аккредитации, с общеобразовательными программами и другими документами, регламентирующими организацию и осуществление образовательной деятельности, права и обязанности обучающихся,
- согласие родителя(ей) (законного(ых) представителя(ей) ребенка или поступающего на обработку персональных данных. [55]

Эти данные необходимы для оформления личного дела ребенка. На начальном этапе в этом деле хранятся все поступившие от родителей (законных представителей) документы, а в процессе обучения пополняется документами, подтверждающими достижения в учебе, итоговую аттестацию и.т.п.

В отношении тех лиц, которые не предоставляют согласие на обработку данных, должна быть выполнена норма 152-ФЗ, а именно соблюдение обязанности по блокированию обработки данных:

Статья 21. п.5. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить

обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.[78]

При отказе предоставить согласие на обработку данных персональные данные ребенка блокируются в «Личном деле», исключаются из всех информационных систем школы (электронный журнал, списки участников олимпиад и конкурсов) и отсутствуют во всех заполняемых учетных документах. Ребенок принимает участие только в тех мероприятиях, которые не сопровождаются составлением списка участников, и учета его участия в школьной жизни может не быть.

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

Принят Государственной Думой 8 июля 2006 года – базовый законодательный акт в сфере интернет - безопасности, регламентирующий контрольно-надзорные полномочия федеральных органов исполнительной власти в сфере информационной безопасности детей.

В нем регулируются отношения, возникающие при:

- 1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
- 2) применении информационных технологий;
- 3) обеспечении защиты информации.

Важным, на наш взгляд, является определение «конфиденциальности информации», приведенное в данном законе:

конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.[76]

Согласно этому определению конфиденциальность = неразглашение.

В статье 3 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации. В качестве основных принципов, которые присутствуют в данном Законе, выступают целостность и доступность информации.

Ключевой нормой данного закона для обеспечения информационной безопасности образовательной организации является статья 15.1. Данная статья регламентирует порядок работы единого реестра доменных имен, указателей страниц сайтов и сетевых адресов, содержащих информацию, распространение которой на территории РФ запрещено.

ФЗ РФ «Об информации, информационных технологиях и о защите информации» вводит понятие «подписанного электронного документа»:

- a. электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
- b. электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.[76]

Целостность (защищенность) электронных сообщений в МАОУ «СОШ №21» строится на основе несимметричных криптографических алгоритмов с использованием электронной цифровой подписи (ЭЦП). Речь идет о сдаче бухгалтерской и налоговой отчетности, участие в закупках и т.п.

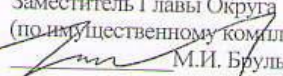
Правовую основу использования электронной подписи определяет ФЗ РФ «Об электронной цифровой подписи». Там определяется понятие ЦП, а также нормы регулирования общественных отношений по созданию, проверки и использованию ЦП в РФ.

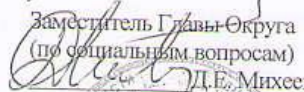
Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.[79]

В России действуют три вида электронной подписи (ЭП): простая, усиленная неквалифицированная и усиленная квалифицированная.

Обзор локальных актов

Основные сведения, регулирующие вопросы обучающего процесса отражены в уставе МАОУ «СОШ №21». Устав утвержден Постановлением Администрации МГО от 24.03.2020 № 1381.

СОГЛАСОВАН
Заместитель Главы Округа
(по имущественному комплексу)

М.И. Бруль


Заместитель Главы Округа
(по социальным вопросам)

Д.Е. Михеев

Начальник Управления образования
Администрации МГО

А.В. Овсянникова

УТВЕРЖДЕН
Постановлением Администрации МГО
от 24.03.2020 № 1381




Глава Миасского городского округа
Г.М. Тонких

УСТАВ
Муниципального автономного
общеобразовательного учреждения
«Средняя общеобразовательная школа № 21»

г. Миасс
2020

Рисунок 6. Устав МАОУ «СОШ №21»

Основные требования к уставам образовательной организации закреплены в ст. 25 Федерального закона № 273-ФЗ. К сожалению, в уставе

отсутствуют положения по требованиям обеспечения информационной безопасности.

МАОУ «СОШ №21» в своей деятельности, опираясь на федеральное законодательство, разрабатывает собственные локальные акты, которые конкретизируют сведения, относящиеся к персональным данным, определяют ответственное лицо, имеющее право доступа к персональным данным обучающегося/родителей/сотрудников организации, а также определяют права и обязанности работников, получивших доступ к персональным данным учеников, родителей и сотрудников школы.

Локальные акты:

Приказ об организации обработки ПД.

Данный документ содержит непосредственно приказ и приложение к нему.

В тексте приказа прописано ответственное за организацию обработки ПД лицо. В приложении к приказу представлена должностная инструкция ответственного сотрудника.

В инструкции прописано 4 основных момента:

Общие положения, обязанности и права ответственного лица, а также его ответственность.

ДИРЕКТОР МУНИЦИПАЛЬНОГО АВТОНОМНОГО ОБЩЕОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ «СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 21»
ПРИКАЗ

Миасский городской округ

11.01.2016

№ 1/17

О назначении должностного лица,
ответственного за организацию
обработки персональных данных в МАОУ «СОШ № 21»

Во исполнении Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки персональных данных МАОУ «СОШ № 21», инспектора по кадрам, Кяккинен Наталью Геннадьевну.
2. Утвердить «Инструкцию ответственного лица за обработку персональных данных в МАОУ «СОШ № 21» (Приложение).
3. Возложить на Кяккинен Н.Г., инспектора по кадрам следующие обязанности:
 - предоставление на утверждение списка лиц, доступ которых к персональным данным, обрабатываемым в МАОУ СОШ № 21» необходим для выполнения служебных (трудовых) обязанностей, а также изменений к нему;
 - осуществление внутреннего контроля за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
 - доведение до сведения работников (оператора) положения законодательства Российской Федерации о персональных данных, требований к защите персональных данных, требований к защите персональных данных;
 - организация приема и обработка обращений субъектов персональных данных или их представителей и осуществление контроля за приемом и обработкой таких обращений.
4. Контроль за исполнением настоящего приказа оставляю за собой.

С.А. Орленко

С приказом ознакомлен:

Рисунок 7. Приказ о назначении должностного лица, ответственного за организацию обработки ПД В МАОУ «СОШ №21».

Положение о защите ПД МАОУ «СОШ №21».

Приложение 1
к приказу № 1/18 от 11.01.2016 года



УТВЕРЖДАЮ:
Директор MAOU «СОШ № 21»
С.А. Орленко
11 января 2016 года

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ MAOU «СОШ № 21»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Целью данного Положения является защита персональных данных учащихся и их родителей (законных представителей), работников муниципального автономного общеобразовательного учреждения средней общеобразовательной школы №17 (далее Учреждение) от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», нормативно-правовых актов Российской Федерации в области трудовых отношений и образования, Устава школы.

1.3. Настоящее Положение утверждается и вводится в действие приказом директора Учреждения и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным учащихся и их родителей (законных представителей), сотрудников.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ УЧАЩИХСЯ И ИХ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ)

2.1. Персональные данные учащихся и их родителей (законных представителей) (далее - ПДн) – информация, необходимая Учреждению в связи с осуществлением образовательной деятельности. Под информацией об учащихся и их родителях (законных представителях) понимаются сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

2.2. В состав персональных данных учащихся и их родителей (законных представителей) входят:

- фамилия, имя, отчество учащегося и их родителей (законных представителей);
- гражданство;
- дата рождения учащегося и их родителей (законных представителей);
- адрес регистрации и проживания, контактные телефоны;
- паспортные данные родителей (законных представителей);
- данные свидетельства о рождении учащегося;
- сведения о месте работы (учебы) родителей (законных представителей);
- документы об отсутствии медицинских противопоказаний для обучения в Учреждении;
- документы, подтверждающие права на дополнительные гарантии и компенсации по социальным основаниям, предусмотренным законодательством;
- оценки успеваемости ребенка;
- фотографии учебно-воспитательного процесса;
- учебные работы ребенка.

1

Рисунок 8. Положение о защите ПД MAOU «СОШ №21»

Данный локальный правовой акт утвержден директором MAOU "СОШ 21" С. А. Орленко 11 января 2016 г.

Структура документа представляет собой 8 разделов, в которых представлена следующая информация:

- понятие и состав ПД учащихся, родителей, работников,
- основные условия проведения обработки ПД,
- право доступа к ПД,
- понятие Защиты ПД,
- права, обязанности и ответственность сторон (субъекта и оператора).

Резюмируя изложенное, следует отметить, что действующие в настоящее время правовые нормы общего характера, в области информационной безопасности, не способны обстоятельно обеспечить регулирование отношений в рассматриваемой сфере. Действующее информационное законодательство содержит большое количество дублирования, и в тоже время много пробелов регулирования правоотношений. Так, например, Концепция информационной безопасности детей, утвержденная Правительством РФ в 2015 году, не является нормативным актом, обязательным к применению, а носит лишь формальный характер. А единственный самостоятельный правовой акт, предназначенный для обеспечения информационной безопасности детей (ФЗ № 436), затрагивает всего лишь часть всех информационных взаимоотношений детей в процессе социализации. Кроме того, он не содержит средства обеспечения информационной безопасности детей, не содержит правовых механизмов.

На законодательном уровне отсутствуют программы обучения по направлению безопасного поведения в интернет пространстве. Работа, проводимая в школе, сводится лишь к периодической пропаганде осторожной работы в сети Интернет, и представляет собой проведение внеклассного мероприятия с учениками, или собрания с коллективом учреждения.

На локальном уровне актуальной задачей для руководства учреждения, на наш взгляд, является развитие внутренней документации в части разработки правил и процедур в сфере обеспечения информационной

безопасности в соответствии с действующим законодательством. Существующие локальные акты можно было бы дополнить, как минимум, положением об использовании ЭЦП (в соответствии с ФЗ 149), а также зафиксировать нормы обеспечения информационной безопасности и в учредительном документе (Устав). Обязательной должна стать разработка документа, регламентирующего соблюдение требований конфиденциальности. При этом необходим принцип постоянной требовательности со стороны директора МАОУ «СОШ №21», ведь зачастую пользователи информации нарушают порядок обращения с ней.

2.2 НАПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ ЗАЩИТЫ ЕДИНОГО ИНФОРМАЦИОННОГО ОБРАЗОВАТЕЛЬНОГО ПРОСТРАНСТВА МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Информационная защита единого информационно-образовательного пространства МАОУ «СОШ №21» носит комплексный характер и включает в себя 5 основных направлений.

1. Нормативно-правовая защита информационной безопасности.

Основным действием является ограничение агрессивного воздействия на сознание ребенка.

На втором месте должно оказаться обеспечение безопасности баз данных.

Защита информации опирается на действующие в этой сфере законы и иные нормативные акты, определяющие отдельные ее массивы как подлежащие защите. Они выделяют те сведения, которые должны быть недоступны третьим лицам по разным причинам (конфиденциальная информация, персональные данные, коммерческая, служебная или профессиональная тайна) и подробно рассмотрены нами в главе 2.1.

2. Морально-этические средства обеспечения информационной безопасности

В образовательной сфере большую роль играет система морально-этических ценностей, то есть стандартов поведения. Система мер, защищающих подростка от травмирующей, этически некорректной информации должна основываться на не писанных правилах честности и патриотизма. Однако основой работы в данном направлении является, принятый в МАОУ «СОШ №21» Устав. А также поддержание внутри коллектива школы здорового морального микроклимата.

3. Административно-организационные меры

К этой категории мер информационной безопасности относят защитные меры административно-процедурного характера, с помощью которых осуществляется регламентация процессов работы систем обработки информации, эксплуатации их ресурсов, деятельности сотрудников, порядка взаимодействия пользователей и работников организации с информационными системами так, чтобы в максимальной степени затруднить или исключить вероятность реализации угроз безопасности, либо уменьшить объемы возможных потерь при их реализации. [23]

Комплекс административно-организационных мер включает в себя должностные инструкции, посвященные информационной безопасности, внутренние методики, порядок доступа детей и сотрудников к сети Интернет. Локальные документы МАОУ «СОШ №21» были рассмотрены нами в главе 2.1.

4. Физические меры

Организация и внедрение данной системы мер лежит полностью на директоре образовательного учреждения и сотруднике IT-подразделения.

К физическим мерам относятся:

пропускная система защиты в помещения, содержащие носители информации,
организация контроля доступа посетителей,
установления различных степеней допуска.

Кроме того, к мерам физической защиты относится вся работа IT-подразделения.

К физическим мерам информационной безопасности также можно отнести средства визуального наблюдения, связи, охранной сигнализации. [23]

5. Технические меры

Комплексную систему защиты всего периметра компьютерной сети должны обеспечивать специализированные программные продукты, например, DLP-системы и SIEM-системы, выявляющие все возможные угрозы безопасности и применяющие меры по борьбе с ними. Для учебных заведений, бюджет которых не позволяет внедрение профессиональных систем, необходимо использование разрешенных и рекомендуемых программных мер защиты, в частности антивирусов. [64]

В частности в МАОУ «СОШ №21» используются шлюзы безопасности, межсетевые экраны - ideco UTM, антивирус - Kaspersky Endpoin security 11 , файловое хранилище - samba сервер, а также мессенджер Rocket Chat.

Электронная почта, к которой имеют доступ сотрудники и учащиеся, должна быть защищена и контролируема. Оптимально также ввести полный запрет на копирование любой информации с жестких дисков компьютеров образовательного учреждения.

Кроме того, согласно 436 ФЗ Федеральному закону "О защите детей от информации, причиняющей вред их здоровью и развитию" в МАОУ «СОШ №21» предусмотрено программное обеспечение, ограничивающее доступ ребенка к сайтам и материалам не соответствующим задачам образования - используется dns фильтрация «Sky-dns контент фильтр».

Все меры должны применяться в комплексе, при этом необходимо определение одного или нескольких лиц, отвечающих за реализацию всех аспектов информационной безопасности. Желательно привлечение к этой проблеме родителей учеников, в ряде случаев они помогут провести аудит

мер безопасности и порекомендовать современные решения. Кроме того, на родителей должны быть возложены обязанности и по ограничению информации, которую ребенок может получить дома. Необходимо просматривать страницы, посещаемые ребенком. На основании анализа его поиска можно вносить изменения в перечень сайтов, доступ к которым ограничен с компьютеров, установленных в учебном заведении.

ГЛАВА 3. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКОЙ ОБЛАСТИ

3.1 ОБЩИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Информационная безопасность ОО тесно связана с управлением IT-инфраструктурой: хорошо управляемую сеть сложнее взломать, чем плохо управляемую.

Одной из главных составляющих деятельности по обеспечению информационной безопасности в МАОУ «СОШ №21» должна стать проблема взаимоотношений с персоналом. Рекомендуется разработать следующую внутреннюю документацию по усилению ИБ:

- Положение об использовании ЭЦП (в соответствии с ФЗ 149).
- Зафиксировать нормы обеспечения информационной безопасности в учредительном документе (устав).
- Разработать правила для сотрудников, работающих в школьном информационном пространстве и желающих использовать свои личные цифровые устройства.

Рекомендуемые действия по обеспечению ИБ в МАОУ «СОШ №21» г. Миасса Челябинской области:

- Сокращение «цифрового разрыва» с упором на обучение Учителей – увеличить количество инструктажей.
- Осуществить настройку межсетевого экрана Idecso UTM для предотвращения атак со стороны входящих соединений.
- Повышение социальной ответственности персонала, требующее быстрой реакции на вероятную угрозу.
- Внедрить систему анализа заявок поступающих в it-службу, позволяющую определить уровень ИКТ компетентности персонала.

- Разработать список уязвимостей программного обеспечения используемого пользователями МАОУ «СОШ№21» для усиления информационной безопасности.
- Усилить контроль сотрудников имеющих доступ к конфиденциальной информации или тех, у кого есть повышенные права доступа в информационных системах.

Основные информационные потоки МАОУ «СОШ № 21» обрабатываются, хранятся, и передаются через файловые обменники (сервера). Настоятельно рекомендуется реализовать на практике модель защищенного файлового хранилища. Предусмотреть возможность распределения прав доступа между пользователями. Реализовать возможность авторизации пользователей по средствам логин и пароль. Подробнее как реализовать данную задачу рассмотри в параграфе 3.2.

3.2 РАЗРАБОТКА И ВНЕДРЕНИЕ МОДЕЛИ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ХРАНИЛИЩА С РАСПРЕДЕЛЕНИЕМ ПРАВ ПОЛЬЗОВАТЕЛЕЙ В ЕДИНОЕ ИНФОРМАЦИОННОЕ ОБРАЗОВАТЕЛЬНОЕ ПРОСТРАНСТВО МАОУ «СОШ №21» Г.МИАССА ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Гипотеза внедрения модели защищенного информационного хранилища состоит в предположении о повышении защищенности информационных ресурсов образовательной организации при размещении данных на выделенном сервере и применении средств аутентификации/идентификации для доступа к ним.

Задача.

При хранении, обработке и передаче различных типов данных на открытом файловом хранилище (Samba сервер), под управлением операционной системы Ubuntu 16.04 LTS все сотрудники ОО имеют неограниченный доступ к данным хранящимся на удаленном ресурсе. Какими способами можно разграничить права пользователей и

предотвратить возможные риски по краже, уничтожению, и изменению данных?

Варианты решения:

Существует множество технических вариантов по выполнению поставленной задачи. Поскольку операционная система Ubuntu 16.04 LTS является UNIX подобной системой, основой ее ядра является LINUX, это предоставляет возможность перенастроить любой сервер под нужды конкретной образовательной организации. Для выполнения поставленной задачи необходимы базовые знания при работе с операционной системой Ubuntu. В МАОУ "СОШ №21" малое количество специалистов обладающими опытом работы с UNIX подобными системами, поэтому мной была разработана *методическая инструкция* из семи шагов для реализации поставленной задачи. В дальнейшем это позволит менять конфигурацию защищаемых ресурсов и каталогов, не только системному администратору, но и пользователям, не обладающими глубокими познаниями и компетенциями в ОС ubuntu и конфигурационных файлах Samba сервера.

Samba сервер находится под управлением операционной системы Ubuntu 16.04 LTS и будет располагаться в закрытом сегменте локальной сети МАОУ «СОШ №21». Это напрямую повысит информационную безопасность и устойчивость всех каталогов сервера к атакам из сети Интернет или внешних источников. Необходимо отметить тот факт, что идеального способа защиты программного обеспечения от несанкционированного использования и распространения не существует. Ни одна существующая система не обеспечит абсолютную защиту и не лишит потенциального взломщика самой возможности ее нейтрализации. Однако использование качественной и эффективной защиты может максимально усложнить процесс взлома программного продукта. Позволит сделать взлом нецелесообразным с точки зрения потраченного на это времени и усилий.

С учетом проведенного анализа защищенности файлового хранилища МАОУ «СОШ №21», выявленных тенденций обеспечения информационной

безопасности данных школы был реализован разграниченный доступ к файловому хранилищу, путем определения групп пользователей, и дальнейшей настройки аутентификации пользователей по средствам логин, пароль.

Новая модель защищенного информационного хранилища с распределением прав пользователей единого информационно-образовательного пространства МАОУ «СОШ №21» схематически может быть представлена следующим образом:

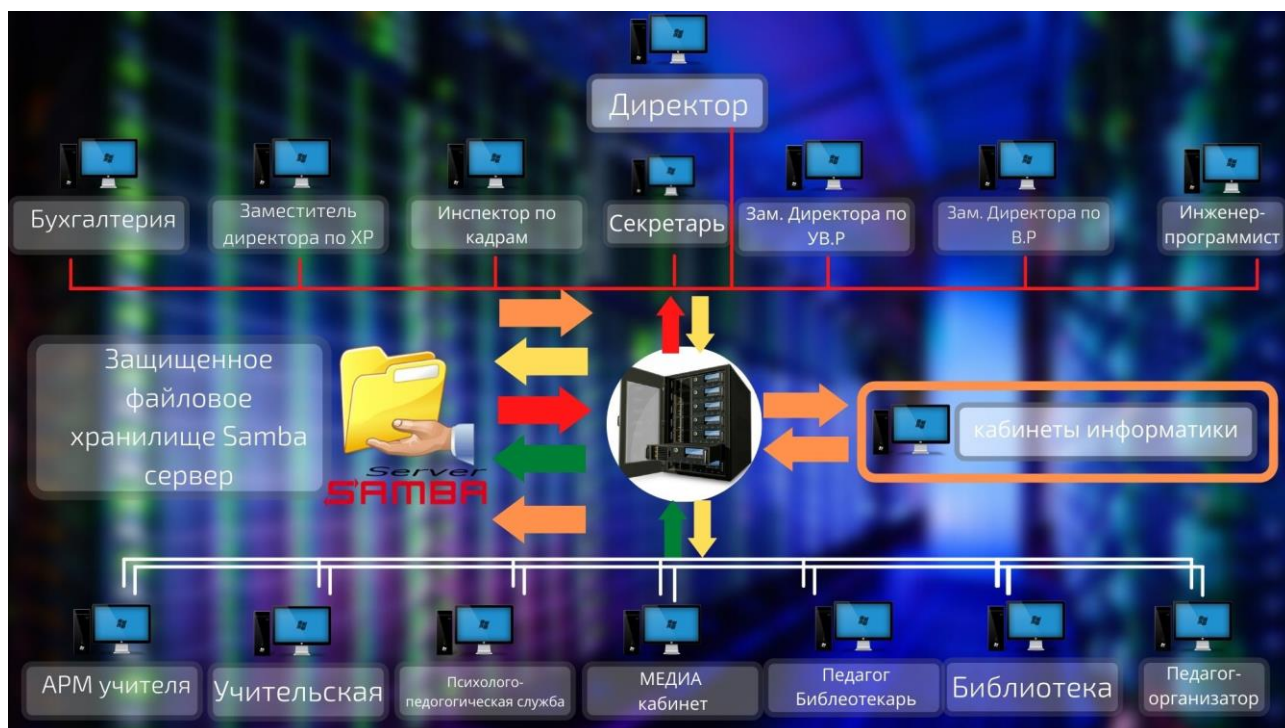


Рисунок 9. Модель защищенного информационного хранилища с распределением прав пользователей единого информационно-образовательного пространства МАОУ «СОШ №21»

Инструкция «Создание защищенного файлового хранилища»:

1.Режимы безопасности Samba.

Samba сервер не воспринимает латиницу, поэтому все команды будут вводиться на английском языке, а все пользователи, группы, и каталоги будут прописываться транслитом. Для конечного пользователя, в дальнейшем пользующегося каталогами, поддержка латиницы присутствует. Вследствие

этого все каталоги можно будет прописывать на любом языке удобном пользователю.

Всего доступны два уровня безопасности для сетевого протокола CIFS (разделяемая файловая система интернета): уровень пользователя (user-level) и уровень ресурса (share-level). Реализация режима безопасности Samba обеспечивает большую гибкость и вариативность, предоставляя четыре способа реализации уровня пользователя и один вариант реализации уровня разделяемого ресурса:

security = user: требует от клиента предоставить имя пользователя и пароль для подключения к ресурсу. Учетные записи пользователей Samba отделены от системных учетных записей операционной системы. В этом случае нам также понадобится пакет `libram-smbpass`, который необходимо дополнительно установить на сервер. Данный пакет синхронизирует системных пользователей и пароли с пользовательской базой данных Samba. Далее необходимо рассмотреть файл конфигурации `smb.conf`, в котором находятся все параметры безопасности и детальная настройка каталогов samba сервера.

security = share: данный параметр позволяет клиентам подключаться к разделяемому ресурсу без предоставления имени пользователя и пароля. Он идеально подходит для сервера файлового хранилища в кабинетах информатики. Он позволяет большому количеству пользователей работать с одним каталогом без авторизации.

```
global]
workgroup = WORKGROUP
server string = %v
netbios name = MARK1
security = user
map to guest = bad user
wins support = no
dns proxy = no
```

Рисунок 10. Параметр share

Для нашего же сервера данный параметр необходимо изменить.

Вместо share используем

security = user

Изменив этот параметр, мы запретили доступ к ресурсам не авторизованных пользователей, в том числе и пользователям с параметрами `nobody:nogroup`.

Далее следует добавить параметр:

map to guest = Bad User

Данный параметр означает, что все запросы с неправильным паролем будут отклонены, если такое имя пользователя существует. Если не существует, то такие запросы будут считаться, как попытки зайти гостем (неавторизованным пользователем).

2. Авторизация пользователей.

Далее необходимо рассмотреть, каким образом перенастроить сервер Samba, чтобы в результате при обращении к каталогам, у пользователя запрашивалась авторизация.

Сначала установим пакет `libpam-smbpass`, который будет синхронизировать системных пользователей с базой данных пользователей Samba. Для этого в окне терминала сервера необходимо прописать команду, приведенную ниже, затем ввести пароль администратора и подтвердить установку:

sudo apt-get install libpam-smbpass

После успешной установки пакета нам необходимо вернуться и вновь отредактировать файл конфигурации сервера, находящийся по адресу `/etc/samba/smb.conf` Создаем в секции `[share]`:

guest ok = no

Далее необходимо перезагрузить сервер Samba, чтобы корректно начала работать новая конфигурация. Для этого в окне терминала вводим следующие команды:

sudo restart smbd

sudo restart nmbd

После успешно проделанных изменений, при последующем подсоединении к разделяемым каталогам сервера, у вас будет запрашиваться окно с требованием ввести имя пользователя и пароль.

3.Создание каталогов.

При создании каталогов в операционной системе нам потребуется любой файл менеджер, например mc(midnight commander). Можно воспользоваться стандартными командами ОС Ubuntu 16.04 LTS.

В корневом каталоге "/" ОС необходимо создать каталог SAMBA. В нем будут располагаться ресурсы, каталоги и файлы, которые можно добавлять или уничтожать по мере необходимости.

Внутри папки samba создаем подкаталог и назовем его "obmen". Чтобы "obmen" впоследствии стал защищенным от несанкционированного пользователя, осуществим действия по средствам следующих команд:

```
sudo mkdir /samba
```

```
sudo mkdir /samba/obmen
```

Каталоги успешно созданы. В будущем при технической необходимости данные каталоги можно расширять, добавлять новые и убирать старые, по средствам тех же команд в операционной системе Ubuntu 16.04 LTS (для корневых каталогов) или же из любого доступного ПК организации с ОС Windows, Linux, Mac OS (если речь идет о подкаталогах).

4.Создание пользователей и паролей.

Далее необходимо создать пользователей и назначить им пароли, для этого необходимо в окне терминала ввести следующие команды/

```
useradd director
```

```
useradd sekretar
```

```
useradd admin
```

```
useradd teacher
```

```
useradd teacher
```

```
useradd zavuch
```

```
smbpasswd -a director
```

smbpasswd -a sekretar

smbpasswd -a admin

smbpasswd -a teacher

smbpasswd -a zavuch

После создания пользователей и их паролей необходимо переходить к дальнейшему усилению безопасности самих каталогов сервера.

5. Создание групп. Распределение пользователей по группам.

Существует несколько опций для усиления безопасности по каждому конкретному разделяемому каталогу. *На примере [obmen], эта секция рассматривает наиболее распространенные опции.*

Группы определяют коллекции компьютеров или пользователей, которые имеют общий уровень доступа к определенным сетевым ресурсам, и обеспечивают уровень модульности при управлении доступом к этим ресурсам. Например, если определены группа adm, которая содержит пользователей **director, admin и sekretar**, и другая группа teachers, которая содержит пользователей **zavuch, admin и teacher**, то некоторый сетевой ресурс, настроенный на доступ группы teachers, будет соответственно предоставлять доступ для **zavuch, admin и teacher**, но не **director** или **sekretar**. Поскольку пользователь **admin** относится к обеим группам adm и teachers, он будет иметь доступ к ресурсам, настроенным на доступ для любой из этих групп, в то время как все остальные - только к ресурсам, настроенным на определенные группы, которым они принадлежат.

Для добавления группы используем команду,

sudo addgroup adm

sudo addgroup teachers

Для добавления нового пользователя в группу ADM(администрация), используем команду:

sudo adduser director adm

sudo adduser sekretar adm

sudo adduser admin adm

Для добавления нового пользователя в группу teachers (учителя), используем команду:

```
sudo adduser teacher teachers
```

```
sudo adduser admin teachers
```

```
sudo adduser zavuch teachers
```

По умолчанию Samba ищет локальные системные группы, находящиеся в /etc/group, для автоматического определения какие пользователи им принадлежат.

При определении групп в файле настроек Samba /etc/samba/smb.conf используется синтаксис распознавания с предшествующим символом "@". На нашем примере, мы определим группу с именем teachers в определенной секции файла /etc/samba/smb.conf, мы сможем сделать это, указав имя группы как @teachers.

6.Права доступа к файлам.

Права доступа определяют явные права компьютера или пользователя на определенный каталог, файл или набор файлов. Такой доступ может быть определен редактированием файла /etc/samba/smb.conf и заданием явных разрешений определенному разделяемому файловому ресурсу или каталогу.

Мы определили Samba ресурс с названием obmen и собираемся дать права только на чтение группе пользователей, известной как teachers, но хотим предоставить возможность записи для группы с именем adm и пользователю admin. Чтобы это осуществить необходимо отредактировать файл /etc/samba/smb.conf, добавив следующие записи в секцию [obmen]:

```
read list = @teachers
```

```
write list = @adm, zavuch
```

```
#=====
[obmen]
path = /samba/obmen
guest ok = no
writable = yes
browsable = no
read list = @teachers
write list = @adm, zavuch
```

Рисунок 11. Права чтения и записи для групп и пользователей

После сохранения изменений группа teachers сможет просматривать данный каталог, но не изменять его. Группа adm, напротив, сможет не только просматривать, но и полноценно редактировать его. Стоит обратить внимание, что пользователь zavuch находится в группе teachers, но мы добавили его отдельно в файл конфигурации, что приведет к его способности также изменять, дополнять и удалять любую информацию из данного каталога.

Другим возможным разрешением Samba сервера будет определение административных привилегий на определенный разделяемый ресурс. Пользователи с административными правами могут читать, записывать или изменять любую информацию, которую содержит ресурс, на который у данного пользователя существуют административные привилегии. Мы хотим, предоставить пользователю director административные права доступа к ресурсу obmen, нам потребуется отредактировать файл /etc/samba/smb.conf и добавить следующую строку в раздел [obmen]:

```
admin users = director
```

```
#=====
[obmen]
path = /samba/obmen
admin users = director
guest ok = no
writable = yes
browsable = no
```

Рисунок 12. Предоставление административных прав доступа к ресурсу obmen для director

Такой вариант настройки каталога идеально подойдет для закрытых каталогов определенных пользователей. В МАОУ «СОШ №21» именно по

такой конфигурации существуют отдельные каталоги для работников бухгалтерии и отдела кадров.

После изменений `/etc/samba/smb.conf` перезапустите Samba для применения изменений:

```
sudo restart smbd
```

```
sudo restart nmbd
```

7.Распределение прав на каталоги.

В завершении нам осталось распределить права на ранее созданный каталог «obmen».

Для назначения прав в UNIX подобных системах используются три группы флагов:

первая определяет права для владельца;

вторая - права для основной группы пользователя;

третья - для всех остальных пользователей в системе.

Для файлов:

r - право на чтение из файла;

w - разрешает запись в файл (в частности перезапись или изменение);

x - позволяет исполнить файл.

Для каталогов, флаги r, w, x имеют несколько отличный смысл:

r - позволяет читать только имена файлов в каталоге;

x - позволяет иметь доступ к самим файлам и их атрибутам (но не именам);

w имеет смысл только в сочетании с x, и позволяет (в дополнение к x) манипулировать с файлами в каталоге (создавать, удалять и переименовывать).

w без x - не имеет никакого эффекта.

Рассмотрим таблицу, чтобы было понятнее:

ОСТ	BIN	Mask	Права на файл	Права на каталог
0	000	---	отсутствие прав	отсутствие прав
1	001	--x	права на выполнение	доступ к файлам и их атрибутам ¹⁾
2	010	-w-	права на запись	отсутствие прав
3	011	-wx	права на запись и выполнение	все, кроме доступа к именам файлов ²⁾
4	100	g--	права на чтение	только чтение имен файлов
5	101	g-x	права на чтение и выполнение	чтение имен файлов и доступ файлам и их атрибутам ³⁾
6	110	g-w-	права на чтение и запись	только чтение имен файлов
7	111	gwx	полные права	все права

Рисунок 13. Распределение прав для каталогов

Чтобы соответствовать приведенной выше конфигурации Samba группе **teachers** требуется предоставить права на чтение. Запись и выполнение для каталога `/samba/obmen`, необходимо предоставить группе **adm**, а файлы должны принадлежать пользователю `zavuch`. Для этого введите следующее в терминале:

```
sudo chown -R zavuch /samba/obmen/
```

```
sudo chgrp -R teachers /samba/obmen/
```

```
sudo setfacl -R -m g:adm:rx /samba/obmen/
```

Команда `setfacl` предоставляет права на выполнение программ для всех файлов в каталоге `samba/obmen`, что для вас может быть желательным или нежелательным исходя из конкретной ситуации.

Теперь из клиента Windows вы можете заметить, что применяются новые права на файлы.

В Завершении необходимо перезагрузить Samba, чтобы воспринялась новая конфигурация:

```
sudo restart smbd
```

```
sudo restart nmbd
```

Теперь при обращении к каталогу необходимо пройти этап Аутентификация, путем ввода логина и пароля.

Внедрение системы аутентификации для открытого файлового хранилища Samba сервера позволило сделать его закрытым для неавторизованных пользователей, то есть дало возможность преподавателям и сотрудникам школы безопасно осуществлять хранение, передачу, обработку служебной информации. Администратор системы и владельцы ресурсов и каталогов получает возможность разграничить потоки данных и предоставить защищенные каталоги конечному пользователю.

Интеграция Samba -сервера в ИТ-инфраструктуру МАОУ «СОШ №21» способствовала появлению в ЕИОП учреждения ряда преимуществ:

1. Ключевой составляющей внедрения самба - сервера является защита от несанкционированного доступа.

Реализованы следующие способы защиты информации:

- идентификация (распознавание) и аутентификация (проверка подлинности) субъектов (пользователей, процессов),

- регистрацию и анализ событий,

- разграничение доступа к ресурсам,

- резервное копирование ресурсов.

2. Внедрение самба - сервера позволило соблюсти основные принципы информационной безопасности, такие как:

- простота использования;

- распределение прав доступа к файлам и каталогам;

- контроль за операциями.

3. Уникальность внедренной системы безопасности заключается в том, что учтены все особенности информационно-образовательного пространства МАОУ «СОШ №21».

Учтен выявленный посредством SWOT - анализа основной источник угроз - человеческий фактор. А именно нежелание сотрудников учреждения обучаться работе с информационными системами, неумышленное нарушение сотрудниками правил работы с информационными системами.

Создание внедряемой системы безопасности является сложным и ответственным процессом, поэтому в подготовке внедрения самба - сервера участвовал IT-специалист.

В ходе исследования мы не старались организовать абсолютно надежную защиту – такой защиты просто не существует, но интеграция данного сервера носит комплексный характер, т.е. позволила объединить разнородные меры противодействия угрозам (правовые, организационные, программно-технические).

Так как в государственных учреждениях приветствуется переход на открытое и отечественное программное обеспечение, при построении единого информационно-образовательного пространства в МАОУ «СОШ №21» было решено использовать свободное программное обеспечение (СПО).

Учтена особенность операционных систем, используемых школой. За счет открытых спецификаций сетевого протокола SMB и преемственности в подходах реализации последующих версий, клиентами сервера на базе Samba могут быть рабочие станции с операционными системами, начиная с Windows XP вплоть до Windows 10.

При выборе способа усовершенствования информационной безопасности ЕИОП школы учитывалась численность сотрудников учреждения. Внедрение самба – сервера это хорошее решение, если в образовательной организации локальная сеть до 100-150 компьютеров и нужды в расширении до значений 250 и более ПК не планируется.

4. Практическое внедрение не требует никаких финансовых затрат.

Эффективность внедренной системы защиты информации достигается ее способностью адекватно реагировать на все попытки несанкционированного доступа к информации, а не количеством вложенных материальных ресурсов.

То есть благодаря технологии Samba мы сократили расходы образовательной организации. И улучшили it-инфраструктуру.

5. Samba сервер очень не требователен к аппаратным ресурсам сервера. Его можно развернуть практически на любой ПК аппаратной составляющей.

6. Сообщество разработчиков со всего мира систематически обновляют версию пакета программ Samba, последняя стабильная версия вышла 9 ноября 2021 года, а обновление безопасности 10 января 2022 года.

7. Огромным плюсом Samba является вариативность настройки безопасности ресурсов, каталогов и файлов. При правильном планировании можно решить 100 процентов нужд и потребностей сотрудников в защите контента от злоумышленников.

К недостаткам можно отнести техническое ограничение:

Максимальный размер базы данных Samba ограничен 4 Гб. Это связано 32-битной архитектурой tdb. И это означает, что для крупных учреждений, с условными сотнями тысяч каталогов и объектов, которые решили совершить переход на Samba, это может оказаться практически невозможным.

Результаты, внедренного закрытого файлового хранилища оцениваем положительно и считаем доказанной гипотезу исследования.

ЗАКЛЮЧЕНИЕ

Целью работы являлось определение текущего состояния информационного пространства МАОУ «СОШ №21» и разработка новой модели единого информационного образовательного пространства, которая позволит найти результативные механизмы управления данной средой в условиях информационной безопасности.

В работе рассмотрены различные подходы к определению понятия «информационно-образовательное пространство», определены компоненты ЕИОП, рассмотрено ЕИОП конкретного учреждения, произведен анализ уязвимостей ЕИОП МАОУ «СОШ №21», рассмотрено нормативно-правовое обеспечение и направления информационной безопасности в образовательной организации, мировые тенденции в подходах к определению уязвимостей.

Для оценки информационно-образовательного пространства МАОУ «СОШ №21» г. Миасса Челябинской был проведен SWOT-анализ.

Для оценки педагогического аспекта состояния информационно-образовательной среды – проведен педагогический самоанализ использования средств ИКТ в образовательной практике школы.

Разработана модель защищенного информационного хранилища с распределением прав пользователей.

В работе представлен опыт интеграции предложенной модели и разработана пошаговая инструкция «Создание защищенного файлового хранилища», адаптированная к нуждам образовательной организации. Рассмотрены преимущества и недостатки внедренной модели.

Основные выводы диссертационного исследования:

1. Современные информационные технологии, внедряемые в сферу образования позволяют усилить интеллектуальные возможности обучающихся, способствуют интенсификации и персонализации процесса обучения и повышению его качества.

2. Компоненты информационно-образовательной среды взаимосвязаны: изменение содержания одного компонента любого уровня приведет к изменению в содержании всех других, и соответственно изменению всего информационно-образовательного пространства.

3. Основным фактором, обеспечивающим рациональное использование единого информационного образовательного пространства образовательного учреждения, является интеграция программных, технологических и информационных ресурсов в единый комплекс. Выработка единых технологических решений внутри данного комплекса позволяет оптимизировать работу всего учреждения.

4. Информационное пространство школы должно быть структурировано, иметь различные уровни доступа и соответствовать требованиям законодательства в сфере информационной безопасности.

5. Организация безопасного единого информационного пространства школы, невозможно без повышения уровня информационной и компьютерной грамотности персонала.

6. Все меры по обеспечению информационной безопасности в образовательной организации должны применяться в комплексе, при этом необходимо определение одного или нескольких лиц, отвечающих за реализацию всех аспектов информационной безопасности.

Основные результаты исследования:

1. Проведено исследование текущего состояния информационного пространства МАОУ «СОШ №21» г. Миасса Челябинской области.

2. Разработана новая модель защищенного информационного хранилища с распределением прав пользователей единого информационно-образовательного пространства МАОУ «СОШ №21».

3. Представлен опыт интеграции предложенной модели.

4. Разработана пошаговая инструкция «Создание защищенного файлового хранилища», адаптированная к нуждам образовательной организации.

5. Рассмотрены преимущества и недостатки внедренной модели.

В заключение хочется отметить, что реализация модели защищенного информационного хранилища с распределением прав пользователей единого информационно-образовательного пространства на основе разработанной инструкции, возможна и на базе других образовательных учреждений, соответствующих минимальным техническим требованиям.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Абдеев, Р.Ф. Философия информационной цивилизации [Электронный ресурс] : цифровая библиотека по философии. Режим доступа: <http://filosof.historic.ru/books/item/f00/s00/z0000892/index.shtml>
2. Абдраимов, Д.И. Теоретико-методологические основы разработки, мониторинга качества и экспериментальной апробации компьютерных учебно-методических комплексов нового поколения [Текст] : учеб.пособие для вузов / Д.И. Абдраимов, Е.Ы. Бидайбеков, Г.Б. Камалова. – Алматы: КазНПУ, 2005. –146 с.
3. Андреев, А.А. Основы открытого образования [Текст] : Отв. ред. В.И.Солдаткин; Российский государственный институт открытого образования – Москва: НИИЦ РАО,2002. – 680с.
4. Асмолов, А.Г. Российская школа и новые информационные технологии: взгляд в следующее десятилетие [Текст] : А.Г. Асмолов, А.Л. Семенов, А.Ю. Уваров. – Москва: НексПринт, 2010. – 84 с.
5. Афонина, Е.С. Организация информационного пространства общеобразовательной школы [Текст] : Е. С. Афонина. – Молодой ученый. – 2014. – №5. – С. 2–4.
6. Ахметов, Б.С. 3-я Всероссийская научно-практическая конференция-выставка [Электронный ресурс] : Информационная образовательная среда вуза: разработка, внедрение, перспективы / Б.С Ахметов, Е.Ы. Бидайбеков. – Омск, 2006. – Режим доступа: <http://www.omsu.ru/conference/stat.php>. – Загл. с экрана.
7. Баженова, С.А. Роль информационных технологий в процессе обучения и воспитания детей и молодежи [Текст] : Вестник Московского городского педагогического университета. Серия информатика и информатизация образования. / С.А. Баженова, Г.А. Краснова, А. Нухулы. – Москва : МГПУ, 2017. – №1 (39). – С. 32-40.

8. Белл, Д. Грядущее индустриальное общество: Опыт социального прогнозирования [Текст] / Даниел Белл, В.Л.Иноземцев. – Москва : Academia, 1999. – 783 с.
9. Бешенков, С. А. Информатика и информационные технологии [Текст] : учеб. пособие для гуманитарных факультетов педвузов / С. А. Бешенков, А. Г. Гейн, С. Г. Григорьев. – Екатеринбург : Изд-во УГПУ, 1995. – 144 с.
10. Бидайбеков, Е.Ы. Информационное интегрирование и анализ образовательной области в разработке электронных средств обучения [Текст] : Монография / Е.Ы. Бидайбеков, С.Г. Григорьев – Алма-Ата: Министерство образования и науки Республики Казахстан, АГУ им. Абая. – 2002. – 100 с.
11. Бидайбеков, Е.Ы. Теоретико-методологические основы (концепция) формирования информационной образовательной среды КазНПУ им. Абая [Текст] : Монография / Е.Ы. Бидайбеков, С.Ж. – Алматы: КазНПУ, 2010. – 140 с.
12. Борисенков, В. П. Поликультурное образовательное пространство России: история, теория, основы проектирования [Текст] : монография/ В. П. Борисенков, О. В. Гукаленко, А. Я. Данилюк. – Москва: Изд-во ООО «Педагогика», 2006. – 464 с.
13. Борисенков, В.П. Сравнительный анализ. Взгляд из России [Текст] / В.П. Борисенков, Мэй Ханьчэн // Россия-Китай: тенденции развития образования в XXI в.: Сравнительный анализ. – Москва: Наука, – 2019. – С. 208-211.
14. Вербицкий, А. А. Цифровое обучение: проблемы, риски, перспективы [Электронный ресурс] / Homo Cyberus. 2019. – № 1 (6). – Режим доступа: http://journal.homocyberus.ru/Verbitskiy_AA_1_2019. – Загл.с экрана
15. Влияние качества информационных ресурсов на формирование готовности педагогов к информатизации образования [Текст] /

- Казанский педагогический журнал.– Казань: ИППО РАО, 2016. – №6 (119). – С. 28-33.
16. ГОСТ Р 56546-2015. Национальный стандарт российской федерации Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем [Текст] –Введ. 2016-04-01. –Москва : Стандартиформ, 2018. – 12 с.
 17. Государственная программа «Информационное общество». Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. – Режим доступа: <https://digital.gov.ru/ru/activity/programs/1/>– Загл.с экрана.
 18. Григорьев, С. Г. Информатизация образования. Фундаментальные основы [Текст] : учеб. пособие / С. Г. Григорьев, В. В. Гриншкун. – Томск : ТМЛ-Пресс, 2008. – 286 с.
 19. Григорьев, С.Г. Программно-методическое обеспечение применения технологий цифровой экономики в образовательном процессе [Текст] : монография / С.Г.Григорьева., Д.Б. Абушкин, Е.К. Андрейкина. – Москва : Образование и Информатика, 2019. – 123 с.
 20. Захарова, И.Г. Формирование информационной образовательной среды высшего учебного заведения: автореферат дис. доктора пед.наук / И.Г. Захарова. – Тюмень, 2003. – 46с.
 21. Ильченко, О.А. Организационно-педагогические условия разработки и применения сетевых курсов в учебном процесс(на примере подготовки специалистов с высшим образованием) [Текс] : автореферат дис. канд.пед.наук / О.А. Ильченко. – Москва : Центр креативной педагогики Московской государственной технологической академии, 2002. – 15 с.
 22. Изевич, А.И. Информатизация образования (для аспирантов педагогических вузов) [Текст] : учебное пособие / А.И. Изевич, О.Ю. Заславская, В.С. Корнилов. – Москва : МГПУ, 2018. – 66 с.

23. Информационный портал и профессиональное сообщество специалистов по информационной безопасности [Электронный ресурс] – Режим доступа: <https://cisoclub.ru/mery-obespecheniya-informacionnoj-bezopasnosti/> – Загл.с экрана.
24. Как образование должно реагировать на новые технологические и информационные революции [Текст] / Сборник материалов IX Международной научно-практической конференции «Инфо-Стратегия 2017. Общество. Государство. Образование» – Самара, 2017. – С. 304-308.
25. Кондаков, А.М. Концепция совершенствования (модернизации) единой информационной образовательной среды, обеспечивающей реализацию национальных стратегий развития Российской Федерации [Текст] / А.М Кондаков, А.А. Вавилова, С.Г. Григорьев. –Москва : Педагогика, 2018. – С. 98-125.
26. Конопатова, Н.К. Оценка качества школьной информационно-образовательной среды в структуре управления образовательными системами [Текст] : Выпускная квалификационная работа. – СПб, 2013. – 49 с.
27. Концепция федеральных государственных образовательных стандартов общего образования. Проект [Текст] : под ред. А. М. Кондакова, А. А. Кузнецова. – Москва : Просвещение, 2008. - 36 с.
28. Корт, С.С. Теоретические основы защиты информации [Текст] / С.С. Корт. Москва : Гелиос АРВ, 2004 – 240 с.
29. Краснова, Г.А. Развитие образования в эпоху четвертой промышленной революции [Текст] / Информатика и образование №1(280). Москва : 2017. – С. 42-45.
30. Краснова, Г.А. Новые индустриальные и информационные революции и их влияние на систему образования [Текст]. Вестник Московского городского педагогического университета. Серия информатика и

- информатизация образования – Москва: МГПУ, 2017. – №1 (39). – С. 45-52.
31. Критерии отбора, особенности разработки и использования цифровых ресурсов в образовании [Текст] : Сборник материалов XI Международной научно-практической конференции «Инфо-Стратегия 2019. Общество. Государство. Образование». – Самара, 2019. – С. 49-52.
32. Курова, Н.Н. Информационная среда образовательного учреждения как управленческий ресурс современного руководителя школы [Электронный ресурс] : Конференция «Информационные технологии в образовании. / Курова Н.Н. – Москва, 2005. – Режим доступа: <http://www.ito.su/main.php?pid=26&fid=5434&PHPSESSID=00a0f682fb916586aca80c70e80f2ab0>.
33. Лапчик, М.П. Информатика и информационные технологии в системе общего и педагогического образования [Текст] : учебное пособие / М.П. Лапчик. – Омск: изд-во ОмГПУ, 1999. – 294 с.
34. Леднев, В. С. Содержание образования [Текст] : учеб. пособие /В. С. Леднев. – Москва : Высш. шк., 1991. – 224 с.
35. Лушников, И.Д. Цифровая школа как ресурсный центр сетевого взаимодействия [Текст] : Справочник заместителя директора школы / Лушников И.Д. 2013. – С.66-88.
36. Мещеряков, Р.В. Технические средства и методы защиты информации [Электронный ресурс] : учебное пособие / Р.В. Мещеряков, И.В.Голубятников. ISBN 978-5-9912-0084-4. – 2009г. – 622 с.
37. Носкова, Т. Н. Проблемы воспитания средствами информационной образовательной среды [Текст] : Известия Российского государственного педагогического университета им. А. И. Герцена / Т.Н. Носкова. – 2015. – № 177. – С. 61-69
38. Нургалиева Г.К. Индикаторы оценки внедрения ИКТ в организациях образования [Текст] : учебное пособие по спецкурсу / Г.К.Нургалиева,

- А.И.Тажигулова. – Алматы: Национальный центр информатизации, 2010.- 65с.
39. Об образовании в Российской Федерации [Электронный ресурс]: [принят Государственной Думой 21 декабря 2012 года] : офиц. текст последняя редакция / Федеральный закон от 29 декабря 2012 г. № 273-ФЗ. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_140174/
40. Овинова, Л. Н. SWOT-анализ процесса воспитания в цифровой образовательной среде вуза Педагогика. Вопросы теории и практики [Электронный ресурс]: Pedagogy. Theory & Practice ISSN 2686-8725 (online) ISSN 2500-0039 (print) 2021. / Овинова, Е.Г. Шрайбер. Том 6. Выпуск 4. С. 700-707
41. О взаимозависимости качества электронных ресурсов и готовности педагогов к информатизации образования: Информатизация образования: теория и практика. [Текст] : Сборник материалов международной научно-практической конференции. – Омск: ОмГПУ, 2016. – С. 9-13.
42. О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» по вопросам воспитания обучающихся [Электронный ресурс]: Федеральный закон от 31 июля 2020 г. № 304-ФЗ. Режим доступа: <https://rg.ru/2020/08/07/ob-obrazovanii-dok.html>
43. Олефир, С.В. Информационно-образовательное пространство для детей и подростков: принципы формирования [Электронный ресурс] : Фундаментальные исследования – Электрон. журн. / – 2013. – № 8-2. – С. 459-463; Режим доступа: <http://www.fundamental-research.ru/ru/article/view?id=31943>
44. О проведении эксперимента по внедрению цифровой образовательной среды [Электронный ресурс]: Постановление Правительства Российской Федерации от 07.12.2020 № 2040. Режим доступа: <http://www.consultant.ru/edu/teacher/obrazovanie/obzor/>

45. Организация коллективной учебной деятельности с использованием сетевых технологий: учебное пособие. / М.: МГПУ. – 2020. 93 с. (В соавторстве Азевич А.И., Баженова С.А., Заславская О.Ю., Заславский А.А., Львова О.В., Рудакова Д.Т.)
46. Орынбаева, Л.К. Международный опыт использования инновационных и информационных технологий для формирования личностных качеств и воспитания школьников [Текст] / Л.К. Орынбаева // Вестник Российского университета дружбы народов. Серия «Информатизация образования». – Москва : РУДН, 2017. – №1. – С. 7-16.
47. Орынбаева, Л.К. Существующая практика и особенности информатизации воспитательной деятельности в школе [Текст] : Вестник Московского городского педагогического университета. Серия информатика и информатизация образования. / Л.К. Орынбаева. – Москва : МГПУ, 2017. – №1 (39). – С. 8-17.
48. Определение подходов к комплексному исследованию информационной образовательной среды в системах общего, профессионального и дополнительного образования [Текст]: // Вестник Российского университета дружбы народов. Серия «Информатизация образования». – Москва: РУДН, 2019.. №1. С. 12-21.
49. Особенности разработки и использования ресурсов проекта «Московская электронная школа»: учебно-методическое пособие для преподавателей педагогических вузов. – Москва : МГПУ, 2019. – 103 с.
50. Парошин, А.А. Нормативно-правовые аспекты защиты информации [Текст] / А.А. Парошин. – Изд-во Дальневосточного федерального университета, 2010. – 116с.
51. Педагогическая практика в условиях реализации проекта «Московская электронная школа» [Текст]: учебно-методическое пособие для преподавателей педагогических вузов / Азевич А.И. и др. – Москва : МГПУ, 2019. – 81 с.

52. Подготовка научно-квалификационной работы аспирантов по специальности 13.00.02 - теория и методика обучения и воспитания (информатизация образования) [Текст] : учебное пособие / О.Ю. Заславская, В.С. Уорнилов – Москва : МГПУ, 2018. – 74 с.
53. Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет [Текст]: [реализованной Министерством образования и науки Российской Федерации от 11 мая 2011 года N АФ-12/07вн.] <https://docs.cntd.ru/document/499053312> Электронный фонд правовых и нормативно-технических документов.
54. Правовой словарь [Текст] / Л.Ю. Грудицина - Москва: Эксмо, 2008. – 341 с.
55. Приказ Министерства просвещения Российской Федерации от 02.09.2020 г. № 458 "Об утверждении Порядка приема на обучение по образовательным программам начального общего, основного общего и среднего общего образования" [Текст] : [зарегистрировано в Минюсте РФ 11 сентября 2020 г.] Гарант.РУ информационно-правовой портал.
56. Проблемы и пути эффективного использования технологий информатизации в образовании [Текст] : Вестник московского университета. Серия 20. Педагогическое образование – Москва : Изд-во МГУ – 2018. – №2. –С. 34-47.
57. Проект «Школа цифрового века» [Электронный ресурс]. Режим доступа: <https://ds.1sept.ru/>
58. Применение исследовательских подходов в обучении информационным технологиям: особенности отечественного и зарубежного опыта [Текст] : Инновации и качество лицейского образования: идеи, опыт, практика. Спецвыпуск. Январь, 2017. – Москва : ГБОУ «Лицей №1575», 2017. – С. 22-25.

59. Разработка и использование ресурсов проекта «Московская электронная школа» [Текст] : учебно-методическое пособие для студентов педагогических вузов / Е.К. Андрейкина и др. – Москва : МГПУ, 2019. – 84 с.
60. Роберт, И. В. Современные информационные технологии в образовании: дидактические проблемы, перспективы использования [Текст] / И. В. Роберт. – Москва : Школа-Пресс, 1994. – 206 с.
61. Роберт, И. В. Концепция комплексной, многоуровневой и многопрофильной подготовки кадров информатизации образования [Текст] / И. В. Роберт, О. А. Козлов. – Москва : ИИО РАО, 2005. – 49 с.
62. Роберт, И. В. Толковый словарь терминов понятийного аппарата информатизации образования [Текст] / И. В. Роберт, Т. А. Лавина. – Москва : ИИО РАО, 2006. – 86 с.
63. Роль информационных технологий в развитии международной мобильности педагогов и студентов вуза [Текст] / Вестник Российского университета дружбы народов. Серия «Информатизация образования». – Москва: РУДН, 2016. – №3. – С. 7-13.
64. Сайт Государственное бюджетное общеобразовательное учреждение города Москвы "Школа № 167 имени Маршала Л.А. Говорова" [Электронный ресурс] Режим доступа: https://sch167s.mskobr.ru/info_add/informacionnaya_bezопасnost
65. Сайт муниципального автономного общеобразовательного учреждения "Средняя общеобразовательная школа № 21" г. Миасса [Электронный ресурс] Режим доступа: <http://s21-miass.ucoz.ru/>.
66. Собкин, В. С. Мониторинг социальных последствий информатизации: что изменилось в школе за три года? [Текст] / В. С. Собкин и др. – Москва: Ин-т социологизации образования РАО, 2008. – 159 с.
67. Тайлаков, У. Н. Единое информационно-образовательное пространство школы как фактор повышения качества образовательных

- процессов [Текст] / У. Н. Тайлаков. // Молодой ученый. – 2013. – № 5 (52). – С. 768-772.
68. Тоффлер, Э. Третья цивилизационная волна [Электронный ресурс] : Университет социологии SOCIO City. Режим доступа: <http://www.sociocity.ru/scitys-274-1.html>
69. Трудовой кодекс Российской Федерации [Текст] : [Принят Государственной Думой 21 декабря 2001 года, Одобрен Советом Федерации 26 декабря 2001 года] : офиц. текст : по состоянию на 29.12.2020. – Москва: АСТ, 2020. – 272 с.
70. Уваров, А. Ю. Электронный учебник: теория и практика [Текст] / А. Ю. Уваров. – Москва : Изд-во УРАО, 1999. – 220 с.
71. Уваров, А.Ю. Кластерная модель преобразования школы в условиях информатизации образования [Текст] : автореф. дис. . д-ра пед. наук / А.Ю. Уваров. Москва : Изд-во ИСМО РАО, 2009. – 41 с.
72. Уголовный кодекс Российской Федерации [Текст] : [Принят Государственной Думой 24 мая 1996 года, Одобрен Советом Федерации 5 июня 1996 года] : офиц. текст: по состоянию на 30.12.2020. . – Москва: Омега-Л, 2021. – 272 с.
73. Урсул, А. Д. Стратегия перехода России на модель устойчивого развития: проблемы и перспективы [Текст] / А. Д. Урсул, В. А. Лось. Москва : Луч, 1994. – 273 с.
74. УСТАВ Муниципального автономного общеобразовательного учреждения «Средняя общеобразовательная школа № 21» [Текст], 2020. – 17 с.
75. Устинова, М.В. Перспективные направления применения технологий информатизации при обучении школьников по программам Международного бакалавриата [Текст] / М.В. Устинова, Е.И. Никонорова; Вестник Московского городского педагогического университета. Серия информатика и информатизация образования. – Москва : МГПУ, 2018. – №3 (45). – С. 14-22.

76. Федеральный государственный образовательный стандарт основного общего образования [Текст] : [Утвержден приказом Министерства образования и науки Российской Федерации от «17» декабря 2010 г. № 1897]
77. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ [Электронный ресурс] : [Принят Государственной Думой 8 июля 2006 года, Одобрен Советом Федерации 14 июля 2006 года] : офиц. текст : по состоянию на 27.07.2006. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/
78. Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ [Текст] : [Принят Государственной Думой 8 июля 2006 года, Одобрен Советом Федерации 14 июля 2006 года] : офиц. текст : по состоянию на 01.03.2021. – Москва : Проспект, 2021. – 48 с.
79. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ [Текст] : [Принят Государственной Думой 25 марта 2011 года, Одобрен Советом Федерации 30 марта 2011 года] : офиц. текст. – Москва : Приоритет, 2021. – 41 с.
80. Хофман, Л. Современные методы защиты информации [Текст] / Л. Дж. Хофман. Москва : Советское радио, 1980. – 264 с.
81. Чашников, Л.А. Проектирование информационной среды образовательного учреждения [Текст] : Курс лекций / Чашников Л.А. [Электронный ресурс] / Режим доступа: <http://www.avers-edu.ru/ProektSchool/Lek/mat/lek2.pdf>
82. Электронный образовательный портал [Электронный ресурс]. Программа информатизации «Школа – единое информационное образовательное Пространство» (2012-2017) / Режим доступа: <https://infourok.ru/programma-informatizacii-shkola-edinoe-informacionnoe-obrazovatelnoe-prostranstvo-615678.html>

83. Электронный блог компании «СТЕК» (системный ИТ-интегратор) [Электронный ресурс] / Анализ уязвимостей. Режим доступа: <https://www.stekspb.ru/outsorsing-it-infrastruktury/it-glossary/analiz-uyazvimostey/>
84. Ярочкин, В.И. Безопасность информационных систем [Текст] / В.И. Ярочкин. – Москва.:Ось-89, 1996. – 132 с.
85. Ярочкин, В. И. Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами [Текст] / В.И. Ярочкин. – Москва: ИПКИР,1998. – 57 с.
86. Ярочкин, В.И. Несанкционированный доступ к источникам конфиденциальной информации [Текст] / Ярочкин В.И. Предприниматель и безопасность. – Москва : Ось-89, 1994. – 71 с.
87. Ярочкин, В.И. Обеспечение сохранения коммерческой тайны предприятия [Текст] / В.И.Ярочкин – Москва : ИПКИР, 1998. – 103 с.
88. Ярочкин, В.И. Технические каналы утечки информации [Текст] / В.И.Ярочкин – Москва : ИПКИР, 1994. – 58 с.
89. Ярочкин, В.И. Каталог обобщенных мероприятий по защите конфиденциальной информации [Текст] / В.И.Ярочкин, Г.Л. Шевцова . –Москва: ИПКИР,1997. – 30 с.
90. The STRIDE Threat Model [Электронный ресурс]. Режим доступа: <http://msdn.microsoft.com/en-us/library/ee823878%28v=cs.20%29.aspx>
91. William Stallings. Wireless Communications and Networking/ Вильям Столлингс. Беспроводные линии связи и сети. 640 стр., с ил.; ISBN 5-8459-0409-9, 0-1304-0864-6.
92. Fostering Tolerance During Life-Long Learning via Means of Informatization [Текст] : Вестник Российского университета дружбы народов. Серия «Информатизация образования». / С.Г. Григорьев, О.В. Львова, Л.А. Шунина. – Москва : РУДН, 2016. – №2. – С. 7-15.

В ходе исследования был проведен мониторинг преподавателей, с целью определения их информационной грамотности, применения информационных технологий в учебной и воспитательной деятельности.

Путем проведения анкетирования оценивались следующие направления:

Владение базовыми программами Word, PowerPoint, Excel,

Работа с электронной почтой

Работа с интернет ресурсами

Внедрение технологий в образовательный процесс

Использование электронного журнала.

Вопросы анкетирования:

1. Владение текстовым редактором:

- печатаю
- печатаю и строю таблицы
- печатаю, строю таблицы, умею вставлять графические объекты
- что вообще такое текстовый редактор?
- умею все перечисленное и даже больше.

2. Владение программой создания презентаций:

- делаю текстовые презентации
- делаю презентации с текстом и графическими изображениями
- делаю презентации с анимацией и разными дизайнами
- умею все перечисленное и даже больше.

3. Владение программой работы с электронными таблицами:

- умею вносить данные в таблицу
- умею самостоятельно создать таблицу
- умею организовать таблицы и строить диаграммы
- умею настроить автоматизированные расчеты.

4. Работа с электронной почтой:

- есть электронный почтовый ящик

- есть электронный почтовый ящик, умею читать входящие письма
- есть электронный почтовый ящик, умею читать входящие письма и отправлять письма самостоятельно
- нет электронной почты.

5. Адрес вашего e-mail:

6. Какие интернет сайты посещаете?:

- сайт школы
- социальные сети
- новостные ленты
- специализированные сайты для работников образования
- наука и образование

7. Внедрение технологий в образовательный процесс:

- работа с классом с использованием проектора, интерактивной доски
- рекомендую учащимся для самостоятельной работы ссылки на информационные ресурсы в Интернете
- подготовка к уроку (мероприятию) с использованием Интернета
- разработка дидактических материалов на компьютере.

8. Использование электронного журнала и электронного дневника Сетевой город (sgo.edu.ru):

- формирование и рассылка информации родителям
- выставление оценок
- домашнее задание
- использую встроенный конструктор уроков

9. Работа с файлами и каталогами в среде одной из операционных систем:

- умею в полной мере
- умею почти всё
- есть затруднения

- не умею.

10. Значок «Мой компьютер» в Windows служит для:

- выхода в Интернет
- доступа к устройствам хранения информации в компьютере
- получения IP-адреса устройства
- выключения компьютера.

Проанализировав активность работы педагогов в электронном журнале и электронном дневнике Сетевой город (sgo.edu.ru), выяснилось, что использование данного сервиса учителями ограничивается лишь выставлением текущих оценок (%) и предоставлением домашней работы (%). Все члены преподавательского состава указали, что используют на уроках интерактивные доски, умеют подготовить презентации с текстом и графическими изображениями. Только половина учителей смогли указать действующий адрес электронной почты.

Для оценки результатов исследования учителей, мы использовали трехуровневую шкалу:

Высокий уровень – 60% и выше – учителя умеют, используют.

Средний уровень – 30-60%.

Низкий уровень – менее 30%.



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

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

**Организация единого информационного пространства образовательной
организации в условиях обеспечения информационной безопасности**

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

Проверка на объем заимствований:
79,69% авторского текста

Работа рекомендована к защите
«17» января 2022 г.
Зав. кафедрой АТИТ и МОТД
Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Орленко Павел Сергеевич

Научный руководитель:
к.т.н., старший преподаватель
Гафарова Елена Аркадьевна

Челябинск
2022



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

ОТЗЫВ РУКОВОДИТЕЛЯ
ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Выпускная квалификационная работа выполнена	
Студентом	ОРЛЕНКО ПАВЕЛ СЕРГЕЕВИЧ
Группа	ЗФ-309-210-2-1
Направление	Профессиональное обучение (по отраслям)
Профиль	Управление информационной безопасностью в профессиональном образовании
Наименование темы	ОРГАНИЗАЦИЯ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА МАОУ «СОШ №21» В УСЛОВИЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Научный руководитель	Гафарова Елена Аркадьевна

Оценка соответствия требованиям ФГОС ВО
подготовленности автора выпускной квалификационной работы

Требования к профессиональной подготовке	Соответствует	В основном соответствует	Не соответствует
Знание материала исследования, свободное ориентирование в содержании работы	+		
Умение корректно формулировать и ставить задачи своей деятельности при выполнении научной работы, анализировать, диагностировать актуальность проблем	+		
Владение основными методами научных исследований	+		
Умение рационально планировать работу, определять грамотную последовательность и объем действий при решении поставленной задачи	+		
Умение анализировать и интерпретировать полученные результаты исследования	+		
Умение пользоваться научной литературой профессиональной направленности	+		
Владение способами представления результатов своей научной работы	+		
Объем и качество выполнения графического материала, его соответствие тексту научной работы и стандартам	+		
Уровень оригинальности ВКР – %			

Отмеченные достоинства: магистрантом проведено исследование текущего состояния информационного пространства МАОУ «СОШ №21» г. Миасса Челябинской области, разработана новая модель защищенного информационного хранилища с распределением прав пользователей единого информационно-образовательного пространства МАОУ «СОШ №21», представлен опыт интеграции предложенной модели, разработана пошаговая инструкция «Создание защищенного файлового хранилища», адаптированная к нуждам образовательной организации, рассмотрены преимущества и недостатки внедренной модели. Практическая значимость проведенного исследования состоит в том, что реализация модели защищенного информационного хранилища с распределением прав пользователей единого информационно-образовательного пространства на основе разработанной инструкции, возможна и на базе других образовательных учреждений, соответствующих минимальным техническим требованиям.

Замечания: существенных замечаний при оценивании работы не отмечено

Заключение: Работа соответствует требованиям, предъявляемым к магистерским квалификационным исследованиям.

Рекомендуемая оценка: ОТЛИЧНО

Научный руководитель _____ / Гафарова Е.А. «24» января 2022 г.

№ п/п	Критерий оценки	Оценки	Комментарии
1	Актуальность темы исследования		
2	Научность и достоверность исходных данных		
3	Методология исследования		
4	Объем и структура работы		
5	Качество изложения		
6	Грамотность и соблюдение правил оформления		
7	Степень самостоятельности работы		
8	Степень научности и новизны		
9	Степень практической значимости		
10	Степень полноты раскрытия темы		
11	Степень обоснованности выводов		
12	Степень оригинальности		
13	Степень научности		
14	Степень практической значимости		
15	Степень полноты раскрытия темы		
16	Степень обоснованности выводов		
17	Степень оригинальности		
18	Степень научности		
19	Степень практической значимости		
20	Степень полноты раскрытия темы		
21	Степень обоснованности выводов		
22	Степень оригинальности		
23	Степень научности		
24	Степень практической значимости		
25	Степень полноты раскрытия темы		
26	Степень обоснованности выводов		
27	Степень оригинальности		
28	Степень научности		
29	Степень практической значимости		
30	Степень полноты раскрытия темы		
31	Степень обоснованности выводов		
32	Степень оригинальности		
33	Степень научности		
34	Степень практической значимости		
35	Степень полноты раскрытия темы		
36	Степень обоснованности выводов		
37	Степень оригинальности		
38	Степень научности		
39	Степень практической значимости		
40	Степень полноты раскрытия темы		
41	Степень обоснованности выводов		
42	Степень оригинальности		
43	Степень научности		
44	Степень практической значимости		
45	Степень полноты раскрытия темы		
46	Степень обоснованности выводов		
47	Степень оригинальности		
48	Степень научности		
49	Степень практической значимости		
50	Степень полноты раскрытия темы		
51	Степень обоснованности выводов		
52	Степень оригинальности		
53	Степень научности		
54	Степень практической значимости		
55	Степень полноты раскрытия темы		
56	Степень обоснованности выводов		
57	Степень оригинальности		
58	Степень научности		
59	Степень практической значимости		
60	Степень полноты раскрытия темы		
61	Степень обоснованности выводов		
62	Степень оригинальности		
63	Степень научности		
64	Степень практической значимости		
65	Степень полноты раскрытия темы		
66	Степень обоснованности выводов		
67	Степень оригинальности		
68	Степень научности		
69	Степень практической значимости		
70	Степень полноты раскрытия темы		
71	Степень обоснованности выводов		
72	Степень оригинальности		
73	Степень научности		
74	Степень практической значимости		
75	Степень полноты раскрытия темы		
76	Степень обоснованности выводов		
77	Степень оригинальности		
78	Степень научности		
79	Степень практической значимости		
80	Степень полноты раскрытия темы		
81	Степень обоснованности выводов		
82	Степень оригинальности		
83	Степень научности		
84	Степень практической значимости		
85	Степень полноты раскрытия темы		
86	Степень обоснованности выводов		
87	Степень оригинальности		
88	Степень научности		
89	Степень практической значимости		
90	Степень полноты раскрытия темы		
91	Степень обоснованности выводов		
92	Степень оригинальности		
93	Степень научности		
94	Степень практической значимости		
95	Степень полноты раскрытия темы		
96	Степень обоснованности выводов		
97	Степень оригинальности		
98	Степень научности		
99	Степень практической значимости		
100	Степень полноты раскрытия темы		

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ
УНИВЕРСИТЕТ»
ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

РЕЦЕНЗИЯ
на выпускную квалификационную работу магистра

Выпускная квалификационная работа выполнена студентом: Орленко Павел Сергеевич

Кафедра Автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Группа: 3Ф-309-210-2-1

Направление подготовки: Профессиональное обучение (по отраслям)

Тема: Организация единого информационного пространства образовательной организации в условиях обеспечения информационной безопасности

Рецензент: Цуканова Екатерина Александровна, МАОУ «СОШ № 21», директор, учитель информатики высшей категории.

Оценка выпускной квалификационной работы

Показатель	Оценка				
	5	4	3	2	•
1. Актуальность тематики работы	5				
2. Степень полноты обзора состояния вопроса и корректность постановки задачи	5				
3. Уровень и корректность использования в работе методов исследований, математического моделирования	5				
4. Степень комплексности работы, применение в ней знаний естественно-научных, социально-экономических, общепрофессиональных и специальных дисциплин	5				
5. Ясность, четкость, последовательность и обоснованность изложения	5				
6. Применение в работе современного математического и программного обеспечения, компьютерных технологий	5				
7. Качество оформления пояснительной записки (общий уровень грамотности, стиль изложения, качество иллюстраций, соответствие требованиям стандартов)	5				
8. Практическая ценность	5				
9. Внедрение результатов	5				

• — не оценивается (трудно оценить).

Отмеченные достоинства:

К достоинствам проведенного исследования следует отнести глубокую и вдумчивую проработку темы с использованием всех доступных первоисточников. В ходе исследования учтены все особенности информационно-образовательного пространства МАОУ «СОШ №21».

Практическая, подтвержденная в ходе апробации значимость данного исследования заключается в предотвращении возможных рисков по уничтожению и изменению данных, без вложения материальных ресурсов.


Представленный практический материал достоверен, сделанные выводы обоснованы, рекомендации имеют практическую значимость.

Отмеченные недостатки:

Существенных недостатков работа не имеет.

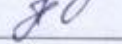
Рекомендуемая оценка «отлично»

Автор работы заслуживает / не заслуживает присвоения степени магистр по направлению 44.04.04. Профессиональное обучение (по отраслям)

Рецензент  «24» января 2022 г.



С отзывом рецензента ВКР ознакомлен.

Студент  / Орленко М / Дата «24» января 2022 г.

подпись

И.О. Фамилия

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ
УНИВЕРСИТЕТ»

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

РЕЦЕНЗИЯ

на выпускную квалификационную работу магистра

Выпускная квалификационная работа выполнена студентом: Орленко Павел Сергеевич

Кафедра Автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Группа: ЗФ-309-210-2-1

Направление подготовки: Профессиональное обучение (по отраслям)

Тема: Организация единого информационного пространства образовательной организации в условиях обеспечения информационной безопасности

Рецензент: Семендяев Константин Николаевич, к.т.н., доцент, ГБПОУ «Южно-Уральский государственный колледж»

Оценка выпускной квалификационной работы

Показатель	Оценка				
	5	4	3	2	•
1. Актуальность тематики работы					
2. Степень полноты обзора состояния вопроса и корректность постановки задачи					
3. Уровень и корректность использования в работе методов исследований, математического моделирования					
4. Степень комплексности работы, применение в ней знаний естественно-научных, социально-экономических, общепрофессиональных и специальных дисциплин					
5. Ясность, четкость, последовательность и обоснованность изложения					
6. Применение в работе современного математического и программного обеспечения, компьютерных технологий					
7. Качество оформления пояснительной записки (общий уровень грамотности, стиль изложения, качество иллюстраций, соответствие требованиям стандартов)					
8. Практическая ценность					

9. Внедрение результатов

--	--	--	--	--

• — не оценивается (трудно оценить).

Отмеченные достоинства:

Материал в работе изложен грамотно, логично, хорошо структурирован – определены цель исследования, объект, предмет, задачи, порядок исследования, сформулированы выводы.

Отмеченные недостатки:

В качестве недостатков к содержанию практической части следует отметить излишнюю краткость в описании эксперимента.

Рекомендуемая оценка «отлично»

Автор работы заслуживает / не заслуживает присвоения степени магистр по направлению 44.04.04. Профессиональное обучение (по отраслям)

Рецензент _____ «_____» _____ 2022 г.



Зам. дир. по РИО
К. Я. СЕМЕНЯЕВ

С отзывом рецензента ВКР ознакомлен.

Студент _____ / _____ / Дата « 24 января 2022 г. подпись _____ И.О. Фамилия _____

АДМИНИСТРАЦИЯ МИАССКОГО ГОРОДСКОГО
ОКРУГА
МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ
ШКОЛА № 21»

улица Лихачева, 33а, г. Миасс
456 300 РФ Челябинская область
Тел/факс 8 (3513) 52 05 01

24 февраля 2022 год

Справка о внедрении

результатов диссертационного исследования Орленко Павла Сергеевича на
тему: "Организация единого информационного пространства
образовательной организации в условиях обеспечения информационной
безопасности"

МАОУ "СОШ№21" подтверждает, что научные исследования Орленко П.С
по усилению информационной безопасности были рассмотрены, одобрены и
приняты к использованию на предприятии, в частности, рекомендована для
внедрения:

Модель защищенного информационного хранилища (Samba сервер).

Директор



Е.А. Цуканова