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

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

Обеспечение конфиденциальности доступа к сайту образовательной организации

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

Проверка на объем заимствований:
96,71 % авторского текста

Работа рекомендована к защите
«26» 12 2025 г.
Зав. кафедрой АТ, ИТ и МОТД
_____Руднев В.В.

Выполнил:
студент группы ЗФ-309-210-2-1
Куприянов Кирилл Александрович

Научный руководитель:
д.т.н., профессор кафедры АТ, ИТ и
МОТД
Дмитриев Михаил Сергеевич

Челябинск
2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современные образовательные организации функционируют в условиях активной цифровизации, что делает проблему обеспечения конфиденциальности и доступа к сайту не только технической, но и правовой, управленческой и этической.

Актуальность исследования определяется возрастающим значением информационной безопасности в образовательной среде. В условиях обязательной цифровизации документооборота и внедрения электронных журналов, платформ дистанционного обучения и личных кабинетов обучающихся, сайт образовательной организации становится не только средством коммуникации, но и хранилищем чувствительной информации. При этом обучающиеся и сотрудники образовательной организации не всегда обладают достаточной цифровой грамотностью, чтобы осознанно управлять вопросами конфиденциальности. Утечки данных, несанкционированный доступ, использование cookies и цифровых идентификаторов без согласия пользователей вызывают обеспокоенность как у представителей образовательной сферы, так и у законодателей. Поэтому разработка комплексного подхода к обеспечению конфиденциальности и управления доступом к сайту становится неотъемлемой частью стратегии цифровой трансформации образования и требует научного осмысления и методического обеспечения.

Степень разработанности темы в учебно-методической и научной литературе подтверждается работами таких авторов, как И. Н. Гайдарева, которая исследует социальные и правовые аспекты защиты информации в образовательных учреждениях; Н. И. Саттарова, раскрывающая вопросы информационной безопасности образовательной среды; и П. Гилстер, анализирующий цифровую грамотность и риски при использовании электронных ресурсов в образовании. Однако, несмотря на значительный вклад этих и других исследователей, систематизация знаний в контексте

именно сайтов образовательных организаций как особых цифровых объектов, сочетающих технические, правовые и педагогические аспекты, все еще недостаточна.

Несмотря на достижения в понимании механизмов обеспечения информационной безопасности образовательных организаций, остаются нерешенными вопросы, которые определяются наличием ряда противоречий:

– между требованиями законодательства (например, 152–ФЗ «О персональных данных») и реальной практикой обеспечения конфиденциальности на сайтах образовательных организаций;

– между стремлением образовательных организаций к открытости и доступности информации и необходимостью ограничения доступа к чувствительным данным;

– между техническими возможностями защиты и уровнем компетентности персонала образовательных организаций в области цифровой безопасности.

Обозначенные выше противоречия и специфика сайтов образовательных организаций обусловили проблему исследования: каковы условия и эффективные механизмы обеспечения конфиденциальности и регламентированного доступа на сайте образовательной организации в условиях цифровизации образования.

Обеспечение конфиденциальности доступа к сайту образовательной организации является сложной и социально значимой задачей. Осмысление и решение данной задачи позволяет не только обеспечить соблюдение законодательных норм, но и повысить доверие к образовательной среде со стороны всех участников учебного процесса. Эти обстоятельства и актуальность рассматриваемой проблемы обуславливают выбор темы исследования: «Обеспечение конфиденциальности доступа к сайту образовательной организации».

Цель исследования – разработка и реализация условий обеспечения конфиденциальности доступа к сайту образовательной организации.

Объект исследования – процесс обеспечения конфиденциальности доступа к сайту образовательной организации.

Предмет исследования – условия обеспечения конфиденциальности доступа к сайту образовательной организации.

Гипотеза исследования: процесс обеспечения конфиденциальности доступа к сайту образовательной организации будет более эффективным, если разработаны, теоретически обоснованы и реализованы следующие условия:

– разработана политика информационной безопасности сайта образовательной организации, включающая регламент регулярных аудитов, четкое распределение ролей и ответственности за управление правами доступа, а также внедрение процедур реагирования на инциденты;

– функционирование сайта сопровождается участием обучающихся в контролируемых проектах по оценке информационных рисков и защите от SQL-инъекций.

В соответствии с выдвинутой целью, объектом, предметом и гипотезой исследования были определены следующие задачи исследования:

1. Провести теоретический анализ проблемы обеспечения конфиденциальности и доступа к сайту образовательной организации.

2. Обосновать условия обеспечения конфиденциальности доступа к сайту образовательной организации.

3. Подобрать инструментарий и провести оценку уровня обеспечения конфиденциальности доступа к сайту образовательной организации.

4. Экспериментальным путем проверить условия обеспечения конфиденциальности доступа к сайту образовательной организации.

5. Оценить эффективность реализации условий обеспечения конфиденциальности доступа к сайту образовательной организации.

Теоретико-методологической базой исследования выступили:

– системный подход (Л. Фон Берталанфи, В. Г. Афанасьев, Н. В. Кузьмина и другие);

– концепция информационной безопасности (И. Н. Гайдарева, Ю. А. Щербаков, В. П. Гришин, В. Н. Бурков, Б. Г. Сызранов, Е. В. Касперский и другие);

– теория цифровой грамотности и цифровой культуры (П. Гилстер, Р. Хоббс, Л. Манович, А. В. Шариков и другие).

– теория информационного обучения (Н. И. Саттарова, В. В. Гриншкун, Т. В. Ковалева и другие);

– практические разработки в области применения ИКТ в образовании (Е. С. Полат, И. В. Роберт, В. А. Красильникова, Н. Н. Двуличанская, И. Г. Захарова и другие).

В соответствии с целью, гипотезой и задачами в ходе данного исследования применялись следующие методы:

– теоретические: теоретический анализ специальной литературы, обобщение результатов исследования;

– эмпирические: веб-аналитика, изучение регламентирующей и технической документации, педагогическое проектирование;

– количественная и качественная обработка полученных результатов.

Этапы исследования:

На первом этапе (2023–2024 гг.) проводился сбор и анализ теоретического материала по проблеме исследования, была выявлена актуальность, определены цель, гипотеза и задачи исследования, разрабатывался план проведения эмпирического исследования.

На втором этапе (2024 г.) подбирался диагностический инструментарий, оценивался уровень и внедрялись условия обеспечения конфиденциальности и доступа к сайту образовательной организации.

На третьем этапе (2025 г.) сравнивались результаты оценки уровня обеспечения конфиденциальности доступа к сайту образовательной

организации до и после реализации предложенных условий, сформулированы и уточнены выводы, оформлена работа.

База исследования: Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный технический колледж» (ГБПОУ «ЮУрГТК», 454080 Челябинская область, г. Челябинск, ул. Горького, д. 15).

Научная новизна исследования:

– разработан и внедрен комплекс условий обеспечения конфиденциальности доступа к сайту образовательной организации, включающий регламент аудитов, распределение ответственности за администрирование, а также интеграцию образовательных практик по диагностике и профилактике цифровых угроз;

– показано, что сочетание административно-нормативных и педагогических механизмов обеспечивает устойчивое повышение уровня защищенности сайта образовательной организации и формирование культуры ответственного отношения к цифровой информации среди участников образовательного процесса.

Теоретическая значимость исследования заключается:

– в уточнении признаков понятий «конфиденциальность сайта образовательной организации» и «доступ к сайту образовательной организации» с учетом правовых, технических и управленческих особенностей данной категории веб-ресурсов;

– в выявлении особенностей обеспечения конфиденциальности доступа к сайту образовательной организации в современной информационно-коммуникационной среде;

– в расширении и дополнении теоретических знаний о направлениях и условиях организационно-педагогической работы по обеспечению конфиденциальности доступа к сайту образовательной организации.

Практическая значимость исследования: разработана и внедрена политика информационной безопасности сайта образовательной организации, апробированы методические приемы вовлечения обучающихся в практическую деятельность по диагностике рисков.

Положения, выносимые на защиту:

1. Разработанная система управленческих мероприятий по обеспечению конфиденциальности доступа к сайту, основанная на политике информационной безопасности, регулярных аудитах и разграничении прав пользователей, обеспечивает устойчивое функционирование цифровой инфраструктуры образовательной организации.

2. Комплексная модель, включающая практико-ориентированное участие обучающихся в диагностике и профилактике цифровых рисков, способствует интеграции образовательных и управленческих аспектов информационной безопасности, что позволяет повысить результативность системы защиты сайта.

Структура и объем работы. Работа изложена на 78 страницах, состоит из введения, двух глав (теоретической и экспериментальной), выводов по ним, заключения и списка использованных источников, включающего 60 наименований. Текст иллюстрирован 8 таблицами и 7 рисунками. Имеется приложение.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ДОСТУПА К САЙТУ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1 Конфиденциальность и доступ к сайту как управленческая проблема в образовательной организации

Цифровизация образования стремительно трансформирует организационные процессы в учебных заведениях, придавая особую значимость вопросам информационной безопасности. Сайт образовательной организации в этих условиях становится не просто средством информационного сопровождения учебного процесса, а полноценным элементом управленческой инфраструктуры. Он содержит персональные данные обучающихся, педагогов и сотрудников, размещает документы, касающиеся образовательной политики учреждения, и обеспечивает доступ к образовательным ресурсам [8]. Таким образом, вопросы конфиденциальности и регламентированного доступа к содержанию сайта приобретают не только техническое, но и управленческое измерение, поскольку от их решения напрямую зависит уровень доверия пользователей, соответствие нормативным требованиям и репутационная устойчивость образовательной организации.

Современные вызовы, включая усиление требований к защите персональных данных, рост числа киберугроз и необходимость прозрачности образовательной деятельности, требуют от администрации учреждений системного подхода к проектированию и эксплуатации сайтов. Конфиденциальность и доступность информации перестают быть исключительной зоной ответственности ИТ-специалистов и становятся предметом стратегического управления. Это обусловливает необходимость теоретического осмысления проблематики на стыке педагогики, права,

информатики и управленческих наук, что делает актуальным обращение к разнообразным научным подходам, концепциям и моделям, отражающим многомерность исследуемого явления.

Понятия «конфиденциальность сайта образовательной организации» и «доступ к сайту образовательной организации» формируют самостоятельные, но взаимосвязанные категории в управлении цифровой инфраструктурой учебного заведения. Их осмысление требует построения системного тезауруса, в который входят семантически близкие термины, отражающие сущностные аспекты как технического, так и нормативно-организационного порядка.

К термину «конфиденциальность сайта образовательной организации» семантически близки понятия «информационная защита», «персональные данные», «цифровая безопасность», «политика конфиденциальности», «режим доступа» и «утечка информации». Конфиденциальность в данном контексте обозначает состояние защищенности информации, размещенной на официальных Интернет-ресурсах образовательной организации, от несанкционированного просмотра, копирования и распространения.

Понятие конфиденциальности восходит к международным стандартам обработки данных, в том числе Конвенции Совета Европы № 108 и статье 23 Конституции Российской Федерации, где закреплены нормы защиты частной жизни и персональных данных [33]. В образовательной сфере оно стало активно применяться с развитием электронных дневников, онлайн-платформ и цифровых кабинетов, что потребовало пересмотра подходов к информационной безопасности.

Понятию «доступ к сайту образовательной организации» соответствуют термины «идентификация пользователя», «аутентификация», «авторизация», «публичный интерфейс», «разграничение прав» и «открытость образовательной информации». Доступ в данном случае интерпретируется как возможность получения

информации, представленной на сайте, в соответствии с правовым статусом и функциональной ролью пользователя.

Исторически понятие доступа к информационным ресурсам развивалось параллельно с внедрением локальных и глобальных сетей, а в контексте образования – с 2000-х годов, когда были введены требования об обязательном размещении на сайтах школ и вузов сведений в рамках информационной открытости и прозрачности деятельности.

Оба термина объединяются рядом общих характеристик:

– связаны с регулированием движения информации;

– требуют соблюдения правовых норм;

– обеспечивают устойчивость цифровой инфраструктуры;

– направлены на защиту интересов субъектов образовательного процесса.

Исходя из этого, под конфиденциальностью и доступом к сайту образовательной организации следует понимать систему организационно-технических и правовых мер, направленных на обеспечение защищенного, регламентированного и целесообразного обмена информацией между участниками образовательной среды посредством официального веб-ресурса, с учетом принципов информационной безопасности, открытости и персонализированного подхода к пользовательскому взаимодействию.

Историография проблемы обеспечения конфиденциальности и доступа к сайту образовательной организации формировалась на стыке правового регулирования, развития телекоммуникационных технологий и цифровой трансформации образовательной сферы. Генезис данного явления можно проследить через последовательную смену этапов, каждый из которых отражал специфические исторические, технологические и институциональные условия.

Первый этап охватывает конец 1990-х – начало 2000-х годов и связан с внедрением первых корпоративных сайтов образовательных учреждений. В этот период сайты играли преимущественно информационно-

репрезентативную роль и не содержали персонализированных данных. Вопросы конфиденциальности практически не поднимались, поскольку цифровое взаимодействие между обучающимися, педагогами и администрацией ограничивалось электронными письмами и бумажным документооборотом. На этом этапе доминировал принцип открытости, а правовые нормы, регулирующие интернет-пространство, находились в стадии формирования. Однако именно в этот период начались дискуссии о необходимости правового контроля над распространением информации в цифровой среде [60].

Второй этап, пришедшийся на 2006–2012 годы, ознаменовался внедрением в образовательные процессы таких элементов, как электронные дневники, журналы и личные кабинеты пользователей. Развитие платформ дистанционного и смешанного обучения сопровождалось ростом объемов собираемых и обрабатываемых персональных данных. Возникла объективная необходимость в нормативном регулировании информационного обмена внутри образовательных организаций, что способствовало активизации научных исследований в области цифровой безопасности. В это время появились первые рекомендации Минобрнауки России, а также локальные регламенты по защите данных пользователей образовательных ресурсов [60].

Третий этап начался с 2013 года и продолжается по сей день. Его содержание во многом определилось вступлением в силу новых редакций Федерального закона «О персональных данных», а также принятием международных стандартов в области информационной безопасности (в том числе ISO/IEC 27001) [60].

Сайты образовательных организаций стали выполнять не только репрезентативные, но и функционально-управленческие задачи: через них осуществляется подача заявлений, регистрация на курсы, взаимодействие с контингентом обучающихся и публикация отчетной документации. Углубление цифровизации привело к возникновению сложных вопросов

разграничения доступа, многоуровневой идентификации, хранения и передачи защищенной информации. В научной литературе все чаще стали подниматься темы интеграции правовых, технических и психолого-педагогических решений в единую модель управления цифровыми рисками в образовательной среде [10].

В таблице 1 представлены различные подходы к проблеме обеспечения конфиденциальности доступа к сайту образовательной организации (таблица 1).

Таблица 1 – Ключевые подходы к определению сущности процесса обеспечения конфиденциальности доступа к сайту образовательной организации

Подход	Автор	Краткая характеристика
Технологический	Т. Ю. Степанова	Рассматривает защиту информации в образовательной среде как задачу реализации технических средств безопасности: шифрования, межсетевых экранов, систем обнаружения вторжений. Подход акцентирует внимание на аппаратной и программной защите, применимой в ИТ-инфраструктурах образовательных организаций.
Нормативно-правовой	И. Н. Гайдарева	Делает упор на правовые аспекты защиты персональных данных в образовательных учреждениях. Исследует соответствие деятельности образовательных организаций требованиям законодательства, включая 152-ФЗ и положения о прозрачности сайтов.
Психолого-педагогический	М. В. Кузнецова	Анализирует конфиденциальность через призму цифровой культуры, осознанности пользователей и уровня их цифровой грамотности. Подчеркивает важность формирования компетенций безопасного поведения в сети у всех участников образовательного процесса.
Управленческий	Р. Д. Хамидуллин	Интерпретирует обеспечение доступа и конфиденциальности как часть общего процесса цифрового управления организацией. Акцентирует внимание на роли руководства в формировании стратегий, политик и организационных моделей по защите информации.

Продолжение таблицы 1

Цифрово-компетентностный	П. Гилстер	Предлагает рассматривать проблему через формирование цифровой грамотности и компетенций, включая способность различать уровни доступа, оценивать риски и управлять персональной информацией в цифровой среде. Подход применим к образовательным сайтам в контексте пользовательской активности.

Анализируя приведенные в таблице 1 подходы, можно выделить как их значимость, так и ограничения.

Технологический подход, предложенный Т. Ю. Степановой, дает четкое понимание инструментальных механизмов защиты, но слабо охватывает управленческие и этические аспекты, связанные с организационной культурой и вовлеченностью сотрудников [52].

Правовой ракурс И. Н. Гайдаревой ориентирован на соблюдение норм, однако практически не рассматривает практические проблемы их имплементации в условиях ограниченных ресурсов и низкой ИТ-квалификации сотрудников образовательных организаций [15].

Психолого-педагогический подход Н. И. Саттаровой, несмотря на ценность в воспитательной работе, ограничивается рассмотрением поведенческой стороны проблемы, не затрагивая системную инфраструктуру безопасности образовательной организации [48].

Управленческая модель Р. Д. Хамидуллина акцентирует важность стратегического подхода, однако требует дополнения конкретными техническими регламентами и инструментарием оценки рисков [56].

Подход известного писателя и журналиста П. Гилстера ориентирован в большей степени на пользователя, чем на организацию, и не охватывает специфики внутренней ИТ-политики учреждения образования [16].

Следует отметить, что существующие авторские позиции отражают лишь отдельные фрагменты сложной системы обеспечения конфиденциальности доступа. Современная теория управления

информационной безопасностью требует интегративной модели, сочетающей техническую защищенность, правовое соответствие, организационные процессы и цифровую культуру. Только при их синтезе можно говорить о полноценной управленческой стратегии в сфере образовательных веб-ресурсов.

Таким образом, эволюция проблемы конфиденциальности и доступа к сайтам образовательных организаций проходит путь от простого информационного сопровождения до системного управленческого инструмента, требующего комплексного регулирования и научного осмысления. Историография данной проблемы наглядно демонстрирует, что ее развитие обусловлено не только техническим прогрессом, но и изменением управленческих парадигм в образовании, а также ужесточением правовых требований к обращению с цифровыми данными. В этой связи под обеспечением конфиденциальности и доступа к сайту образовательной организации следует понимать систему организационно-технических и правовых мер, направленных на обеспечение защищенного, регламентированного и целесообразного обмена информацией между участниками образовательной среды посредством официального веб-ресурса, с учетом принципов информационной безопасности, открытости и персонализированного подхода к пользовательскому взаимодействию.

1.2 Формы, средства и методы обеспечения конфиденциальности доступа к сайту образовательной организации

Изучение и разработка эффективных форм, средств и методов обеспечения конфиденциальности и регламентированного доступа к сайту образовательной организации является необходимым направлением современной управленческой практики в условиях цифровой

трансформации образования. Эта проблема носит комплексный характер, так как затрагивает как технические, так и нормативно-организационные, педагогические и социально-психологические аспекты. Применение целенаправленных форм управления доступом и защитой информации позволяет повысить уровень защищенности образовательной среды, сохранить доверие со стороны участников образовательных отношений, а также обеспечить выполнение требований действующего законодательства в сфере защиты персональных данных [11].

Формы обеспечения конфиденциальности доступа включают в себя совокупность организационных, правовых и технологических решений, реализуемых на уровне образовательного учреждения. Эти формы варьируются в зависимости от целей сайта, его функционального наполнения, категории пользователей и технических возможностей организации. К числу наиболее устойчиво применяемых можно отнести регламентированные административные процедуры, автоматизированные средства защиты, а также специализированные обучающие мероприятия. Формы могут быть как индивидуализированными (например, назначение персонализированных прав доступа к разделам сайта), так и системными (например, внедрение комплексной политики информационной безопасности учреждения) [11].

Л. Н. Бокова подчеркивает значимость регламентирующих форм как основы правомерного и безопасного функционирования цифровой среды образовательной организации. В частности, она указывает на необходимость локальных нормативных актов, регулирующих порядок предоставления доступа, разграничения полномочий, хранения логов активности и обработки персональных данных. Такие формы позволяют четко определить, кто и в каком объеме имеет право взаимодействовать с различными разделами сайта, что особенно важно при размещении документов, содержащих сведения ограниченного распространения [7].

Автоматизированные формы защиты информации, по мнению В. В. Сухостат и И. Н. Васильевой, являются важнейшим инструментом обеспечения конфиденциальности в условиях постоянно возрастающих киберугроз. Авторы акцентирует внимание на необходимости многофакторной аутентификации пользователей, регулярного обновления CMS и плагинов, а также использования сквозного шифрования. Реализация таких форм позволяет технически ограничить возможность несанкционированного вмешательства в структуру сайта и минимизировать риски утечки персональных данных [53].

Психолого-организационные формы, рассматриваемые Л. Л. Тимофеевой, направлены на развитие у работников образовательной организации устойчивой установки на соблюдение принципов информационной безопасности. Автор предлагает внедрение систематических семинаров, тренингов и инструктажей, где работникам объясняются последствия небрежного отношения к защите информации, а также практикуется распознавание потенциальных угроз, таких как фишинг, подмена страниц или социальная инженерия [55].

Существенное внимание в современных работах, в том числе у М. Ю. Корчагиной, уделяется формам, направленным на формирование у обучающихся цифровой ответственности. Предлагаются включение в образовательные программы модулей по цифровой этике, базовой кибербезопасности, а также проведение учебных кейсов и симуляционных ситуаций, в которых обучающиеся учатся различать уровни конфиденциальной информации и корректно действовать в цифровой среде. Эти формы способствуют формированию компетентных пользователей, снижающих нагрузку на систему администрирования сайта [34].

Необходимо выделить, что наиболее эффективными являются интегративные формы, сочетающие правовые регламенты, технические меры и образовательную деятельность. Такую позицию занимает Е. В. Вострецова, которая в своих работах акцентирует внимание на

необходимости формирования целостной модели информационной безопасности, в которую включены стандартизированные формы контроля доступа, протоколы взаимодействия между пользователями и администраторами, а также механизмы мониторинга и анализа инцидентов [12].

Выбор выше указанных форм обеспечения конфиденциальности и доступа обусловлен многоуровневой структурой сайта образовательной организации, в которой сосуществуют открытые и закрытые сегменты информации, разнородные группы пользователей (обучающиеся, родители, педагоги, администрация), а также повышенные требования к сохранности персональных данных. Эффективность форм напрямую зависит от их соответствия контексту учреждения, его цифровой зрелости и наличия подготовленного персонала.

Средства обеспечения конфиденциальности и регламентированного доступа к сайту образовательной организации представляют собой совокупность инструментов, технологий и процедур, направленных на защиту цифровой образовательной среды от несанкционированного вмешательства, утечек персональных данных и искажений информации. В условиях цифровизации образования сайт становится центральной точкой взаимодействия между всеми участниками учебного процесса – администрацией, педагогами, обучающимися, родителями и внешними аудиториями. Это придает особую значимость выбору и грамотной реализации эффективных средств защиты информации, размещаемой на веб-ресурсе учреждения.

Средства обеспечения конфиденциальности и доступа классифицируются по их функциональному назначению:

– технические;

– программные;

– организационно-правовые;

– образовательные.

Каждая группа средств выполняет конкретную задачу в общей системе информационной безопасности и требует комплексного применения. Необходимость их внедрения обусловлена как внутренними управленческими задачами, так и внешними нормативными требованиями – прежде всего, положениями Федерального закона № 152-ФЗ «О персональных данных», а также методическими письмами Минобрнауки России, рекомендациями Рособрнадзора и стандартами цифровой безопасности [42].

Среди технических средств, обеспечивающих конфиденциальность, особое значение имеют системы шифрования данных, межсетевые экраны, фильтры трафика, средства резервного копирования и контроля целостности информации. В работе М. Б. Ефремова подчеркивается, что физическая безопасность серверов, надежная настройка хостинга и защита административной панели сайта составляют первую линию обороны от внешних угроз. Эти средства, при грамотной настройке, предотвращают попытки вмешательства, подмены данных и кражи учетных записей [25].

Программные средства включают в себя системы управления доступом (RBAC), многофакторную аутентификацию, логирование действий пользователей, регулярные обновления CMS и плагинов, а также системы антивирусной и антиспам-защиты. Н. Ф. Богаченко отмечает, что наличие программной архитектуры, поддерживающей разграничение прав доступа для разных категорий пользователей (администрация, педагоги, родители, обучающиеся), является неотъемлемым элементом устойчивого и безопасного функционирования образовательного сайта. Эти средства позволяют обеспечить избирательность в отображении информации, соответствие содержания целевым группам пользователей, а также возможность быстрого реагирования в случае инцидента [6].

Организационно-правовые средства включают разработку и внедрение локальных актов образовательной организации: политики конфиденциальности, положения об обработке персональных данных,

инструкции по ведению сайта и регламентов по управлению учетными записями. Согласно исследованиям Н. В. Москвитиной, наличие документированной базы, регулирующей поведение пользователей и администраторов в цифровой среде, существенно снижает риск произвольных действий и способствует юридической защищенности учреждения в случае проверок или инцидентов. Такие средства должны регулярно актуализироваться в соответствии с изменениями законодательства и технического ландшафта [40].

Отдельную группу составляют образовательные средства – инструменты формирования цифровой грамотности и культуры информационной безопасности у сотрудников и обучающихся. Г. У. Солдатова подчеркивает, что даже самая совершенная техническая защита может быть нейтрализована низким уровнем цифровой компетентности пользователей. В связи с этим используются информационные тренинги, инструкции, тестирования на знание основ ИБ, курсы повышения квалификации для администраторов сайта и ответственных за информационную политику учреждения. Такие средства направлены на профилактику нарушений конфиденциальности, ошибочного распространения закрытых сведений и неосторожного обращения с персональными данными [51].

Особого внимания заслуживают интеграционные средства, которые объединяют технические, программные и организационные решения в рамках единой платформы. К ним относятся системы мониторинга безопасности, автоматизированные модули журналирования действий пользователей, адаптивные системы управления правами доступа, реагирующие на изменение роли пользователя (например, переход ученика в статус выпускника), а также панели централизованного администрирования. Эти средства активно внедряются в современных цифровых платформах образования и позволяют не только управлять

безопасностью, но и анализировать поведенческие модели пользователей для предотвращения потенциальных угроз [26].

Следует отметить, что выбор и реализация указанных средств должна основываться на учете специфики конкретного образовательного учреждения, его ресурсных возможностей, уровня подготовки персонала, структуры сайта и объема обрабатываемых данных. Важно понимать, что эффективность средств обеспечения конфиденциальности и доступа не определяется их количеством или технической сложностью, а степенью их согласованного взаимодействия и регулярного обновления.

В условиях стремительной цифровизации, перехода к электронным формам взаимодействия, хранения и передачи информации вопрос защиты персональных данных, размещаемых на сайтах образовательных организаций, приобретает стратегическое значение. Применение научно обоснованных методов позволяет не только минимизировать риски цифровых угроз, но и сформировать устойчивую и предсказуемую модель информационного поведения как со стороны сотрудников, так и обучающихся.

Методы обеспечения конфиденциальности и доступа представляют собой совокупность приемов, алгоритмов и действий, направленных на реализацию конкретных форм защиты информации в рамках сайта. Они варьируются от технических до административных и поведенческих, охватывая как системный уровень управления, так и индивидуальный уровень пользователя. Их выбор зависит от характера информационных потоков, архитектуры веб-ресурса, целей использования и объема обрабатываемых персональных данных. К методам относятся как превентивные меры, направленные на предупреждение угроз, так и корректирующие действия, позволяющие оперативно реагировать на инциденты [12].

Научные труды А. Р. Карачаева демонстрируют значение технических методов защиты, включающих в себя внедрение шифрования,

протоколов HTTPS, настройку ролевых политик доступа и использование антивирусных фильтров. Автор подчеркивает, что только при комплексной защите серверной части, базы данных и интерфейса возможна стабильная работа сайта, исключающая несанкционированный доступ к чувствительной информации. Среди технических методов он выделяет многоуровневую аутентификацию, сегментацию доступа, установку CAPTCHA и систем логирования действий пользователей, что позволяет не только ограничить вход, но и отслеживать подозрительную активность [31].

В работах Т. Б. Ершовой обоснована эффективность организационно-управленческих методов, направленных на регламентацию доступа и формализацию ответственности. К таким методам относятся утверждение должностных инструкций, локальных актов по информационной безопасности, а также назначение ответственных лиц за ведение и модернизацию сайта. Эти методы обеспечивают ясность в распределении полномочий и минимизируют риски, связанные с человеческим фактором. На практике они выражаются в регулярных проверках, аудитах, согласованиях и контроле над соблюдением требований со стороны административной команды учреждения [24].

Е. В. Грохотова исследует методы, связанные с повышением цифровой грамотности персонала и обучающихся. К числу этих методов относятся проведение обучающих вебинаров, тестирование на знание основ цифровой этики и основ безопасной работы в сети. Автор отмечает, что без подготовки конечного пользователя даже самые совершенные технические системы могут быть уязвимыми из-за ошибок или пренебрежения простейшими правилами безопасности. Таким образом, метод обучения – один из ключевых в формировании устойчивой цифровой культуры [20].

Особый интерес представляет метод интеграции с государственными цифровыми платформами, подробно описанный в исследовании Н. А. Мамиконян. Он включает в себя использование валидации доступа через ЕСИА (Единая система идентификации и аутентификации),

авторизацию через сервисы «Госуслуги», а также передачу данных через защищенные каналы связи. Этот метод особенно актуален для школ и колледжей, которые взаимодействуют с ведомственными структурами и обязаны соблюдать строгие протоколы в работе с электронными дневниками, портфолио, заявлениями и запросами родителей [38].

Ряд авторов, включая О. Ю. Губареву, обращает внимание на методы анализа рисков, в том числе регулярную диагностику уязвимостей и моделирование угроз. Применение данных методов позволяет предвидеть потенциальные точки доступа для несанкционированного вторжения и своевременно вносить изменения в архитектуру сайта, внося правки в код, ограничивая открытые порты и совершенствуя резервное копирование [21].

Таким образом, обеспечение конфиденциальности регламентированного доступа к сайту образовательной организации представляет собой сложную и многоплановую управленческую задачу, решение которой требует использования разнообразных и взаимодополняющих форм, средств и методов. Комплексный подход, включающий технические, программные, организационно-правовые и образовательные компоненты, позволяет создать устойчивую и безопасную цифровую инфраструктуру, соответствующую современным вызовам и требованиям. Эффективность таких мер определяется не только уровнем используемых технологий, но и степенью их интеграции в общую управленческую политику учреждения, а также качеством подготовки персонала и зрелостью цифровой культуры. В условиях роста объемов персональных данных, активного использования цифровых платформ и усиления киберугроз именно сбалансированная комбинация управленческих решений, технической защиты и просветительских инициатив может гарантировать высокую степень защищенности информационного пространства образовательной организации и стабильность функционирования ее ключевых цифровых ресурсов.

1.3 Условия обеспечения конфиденциальности и доступа к сайту образовательной организации

Как было показано ранее, в условиях цифровой трансформации образования вопросы конфиденциальности и регламентированного доступа к сайту образовательной организации приобретают особую значимость. Современный образовательный сайт – это не просто визитная карточка учреждения, а сложный информационно-коммуникационный ресурс, включающий элементы документационного сопровождения, персонализированного взаимодействия и онлайн-обслуживания различных категорий пользователей. От того, насколько грамотно организована система доступа к размещенной информации, зависит не только эффективность управленческих процессов, но и соблюдение норм действующего законодательства в сфере защиты персональных данных. Образовательные организации все чаще становятся объектами внимания со стороны регуляторов, общественности и внешних информационных угроз, что требует от их администрации разработки и внедрения продуманных, научно обоснованных условий, способствующих формированию устойчивой и безопасной цифровой среды.

Условия обеспечения конфиденциальности и доступа представляют собой совокупность организационно-правовых, технологических, педагогических и управленческих мер, направленных на защиту информации и создание прозрачной, но при этом контролируемой цифровой инфраструктуры. Эти условия должны быть не только формально зафиксированы в локальных нормативных актах, но и практически реализуемы в повседневной деятельности образовательной организации. Эффективность таких условий напрямую зависит от системности подхода, согласованности действий всех участников образовательного процесса и

соответствия принятых решений современным вызовам информационного общества.

Ранее мы рассмотрели формы, средства и методы обеспечения конфиденциальности и доступа к сайту образовательной организации, при этом важный инструмент обеспечения конфиденциальности и доступа представляют собой и определенные условия. К таким условиям мы отнесли:

1. Разработана политика информационной безопасности сайта образовательной организации, включающая регламент регулярных аудитов, четкое распределение ролей и ответственности за управление правами доступа, а также внедрение процедур реагирования на инциденты.

Разработка политики информационной безопасности сайта образовательной организации как управленческого условия основывается на совокупности теорий, отражающих различные аспекты цифровой устойчивости, институционального контроля и поведенческой управляемости. Научные подходы А. Ю. Павлюкевича, Ю. С. Сенника, С. А. Петренко, Н. В. Скабцова, Д. Феррайоло и Р. Куна формируют методологический фундамент, позволяющий рассматривать политику безопасности не как формальность, а как живую систему, интегрированную в общий контур образовательного управления. Такая система становится неотъемлемым элементом цифровой трансформации учреждения и условием его соответствия современным вызовам в области информационной безопасности.

Теоретическое обоснование управленческого условия, заключающегося в разработке и внедрении политики информационной безопасности сайта образовательной организации, предполагает обращение к ключевым положениям современной управленческой, правовой и информационно-коммуникационной теории. Сформулированное условие отражает необходимость системного подхода к защите цифрового пространства образовательной организации, в рамках которого

регламентируются аудиты безопасности, устанавливаются четкие роли и зоны ответственности за управление доступом, а также внедряются процедуры оперативного реагирования на инциденты. В условиях усложнения цифровой инфраструктуры и растущих рисков информационных нарушений формирование внутренней политики безопасности становится неотъемлемой частью управленческого цикла и требует научного осмысления.

Опорной концепцией данного условия служит теория институционального управления, в рамках которой политика безопасности интерпретируется как инструмент нормализации и формализации поведения участников информационного обмена. Как указывает А. Ю. Павлюкевич, формирование регламентов и инструкций в образовательной организации создает институциональную основу для устойчивого функционирования ИТ-среды, снижает степень неопределенности и позволяет выстроить эффективную модель взаимодействия между пользователями и администраторами. При этом именно четкое закрепление зон ответственности позволяет избежать дублирования функций и правовых конфликтов в случае информационных инцидентов, что, по мнению исследователя, является важным условием управляемости цифровыми рисками в образовательной сфере [43].

Теория жизненного цикла информационной системы, разработанная в белорусской научной школе под руководством Ю. С. Сенник, также служит методологической базой при внедрении политики безопасности. В соответствии с этой концепцией, любой образовательный сайт рассматривается как комплексный информационный объект, проходящий стадии проектирования, внедрения, эксплуатации и модернизации. На каждом из этапов, по мнению автора, необходимо разрабатывать конкретные регламентные процедуры: от начального аудита до механизмов инцидент-менеджмента. Политика безопасности, как элемент сопровождения жизненного цикла, обеспечивает нормативную связность

между техническими компонентами сайта и организационными процессами в учреждении [49].

Важный вклад в развитие понимания роли процедурного реагирования на инциденты внес С. А. Петренко, исследовавший механизмы киберустойчивости веб-платформ. В своих работах он подчеркивает, что инцидент – это не просто технический сбой, а индикатор слабости системы управления. По его мнению, политика информационной безопасности должна предусматривать не только регламент действий в случае утечки или взлома, но и систему постинцидентного анализа, направленного на извлечение управленческих уроков и корректировку внутренних процедур. Это позволяет образовательной организации не только устранить следствия угрозы, но и усилить свою цифровую устойчивость в долгосрочной перспективе [44].

С позиций теории управленческой отчетности (Р. Коплан, Д. Нортон, В. Э. Керимов, Н. А. Адамов, В. Ф. Палий, И. Е. Мизиковский и др.) регулярный аудит сайта как обязательный элемент политики безопасности выполняет функцию обратной связи между системой управления и текущим состоянием информационной среды. Н. В. Скабцов указывает, что только систематическая проверка на уязвимости, соответствие законодательным требованиям и анализ логов активности пользователей может стать основанием для принятия обоснованных управленческих решений в области цифровой безопасности. Внедрение регулярных аудитов позволяет не только идентифицировать нарушения, но и своевременно предупреждать возможные угрозы, корректируя стратегию развития сайта [50].

Концепция ролевой модели управления доступом, подробно изложенная в работах Д. Феррайоло и Р. Куна, обеспечивает методологическую поддержку распределения функций в рамках политики безопасности. Согласно данной модели, эффективное разграничение прав должно основываться на предварительно описанных ролях, каждая из которых соответствует конкретной категории пользователей сайта

(администратор, преподаватель, родитель, ученик, приглашенный специалист и др.). Такая модель, как показывает практика, снижает риск случайных или намеренных нарушений, а также способствует стандартизации доступа к защищенным разделам ресурса [23].

2. Функционирование сайта сопровождается участием обучающихся в проектах по оценке информационных рисков и защите от SQL-инъекций.

Теоретическое обоснование управленческого условия, заключающегося в участии обучающихся в проектах по оценке информационных рисков и защите от SQL-инъекций, опирается на ключевые положения современной информационно-образовательной парадигмы и теории деятельностного подхода в обучении, в соответствии с которыми образовательный процесс должен быть ориентирован на практическую значимость получаемых знаний, формирование профессиональных умений и развитие навыков критического цифрового мышления.

Одним из фундаментальных источников является концепция деятельностного обучения А. Г. Асмолова, в которой подчеркивается необходимость формирования у студентов способности действовать в условиях неопределенности и самостоятельно принимать решения в сложных информационных ситуациях. По мнению исследователя, образовательная среда должна моделировать реальные профессиональные сценарии, стимулирующие обучающихся к анализу рисков, самостоятельному поиску решений и оценке последствий своих цифровых действий. Участие студентов в проектах по оценке уязвимостей и защите сайта образовательной организации становится важнейшим фактором развития их информационной компетентности и ответственности за цифровую безопасность [2].

Теоретические основания вовлечения обучающихся в практико-ориентированные проекты в сфере информационной безопасности можно найти и в концепции профессионально-ориентированного образования,

предложенной Э. Ф. Зеер. Согласно его исследованиям, реализация учебных задач через проектную деятельность способствует формированию устойчивых профессиональных установок, развитию исследовательской активности и адаптации к быстро меняющимся условиям цифровой среды [28]. Именно в таких проектах, как выявление и предотвращение SQL-инъекций, обучающиеся, на наш взгляд, осваивают прикладные инструменты тестирования безопасности веб-приложений, учатся работать с базами данных, анализировать поведение запросов и разрабатывать стратегии их фильтрации и защиты.

Особую роль в обосновании данного условия играет теория формирования цифровой грамотности, развитая П. Гилстером. В его трудах подчеркивается, что цифровая грамотность не ограничивается умением пользоваться ИКТ, а включает в себя способность осознавать риски цифровой среды, оценивать достоверность информации, противодействовать техническим и социальным угрозам. Проекты, направленные на анализ уязвимостей сайтов, позволяют формировать у обучающихся навыки критической оценки источников данных, понимание принципов SQL-инъекций как одного из наиболее распространенных видов атак, а также развивают правовую и этическую ответственность в киберпространстве [16].

С точки зрения методологии практико-ориентированного обучения, участие студентов в проектах по выявлению уязвимостей сайта образовательной организации согласуется с идеями конструктивистской педагогики, изложенными в работах Ж. Пиаже и С. Каплана. Исходя из принципа активного конструирования знаний в процессе решения реальных задач, такие проекты позволяют студентам выходить за рамки абстрактных теоретических схем и формировать знания через конкретную цифровую практику. Процесс сканирования сайта, моделирования SQL-инъекций, анализа уязвимых входов и формирования отчетов становится не только

образовательной, но и личностно-значимой деятельностью, формирующей ощущение профессиональной полезности и ответственности [4].

Современные исследования в области информационной безопасности также поддерживают важность вовлечения студентов в работу с реальными кейсами. Например, в трудах А. В. Логиновой подчеркивается необходимость интеграции в образовательную среду таких задач, как аудит веб-приложений, разработка моделей угроз и тестирование на проникновение, с целью приближения обучения к реальным условиям функционирования цифровых систем. Она указывает, что только при наличии реального объекта анализа и практических задач возможно формирование у студентов навыков, соответствующих требованиям современного цифрового общества и информационного рынка труда [37].

Важно отметить, что участие обучающихся в проектах по оценке рисков и защите от SQL-инъекций способствует не только формированию индивидуальных профессиональных компетенций, но и развитию коллективного взаимодействия. Согласно позиции Е. А. Вохменцевой, проектная деятельность в малых группах создает условия для развития коммуникативных умений, обмена знаниями, формирования командной ответственности и практики совместного принятия решений. В ходе таких проектов обучающиеся осваивают принципы этичного взаимодействия в сети, соблюдения конфиденциальности данных и уважения к чужой цифровой собственности, что особенно значимо в образовательной среде, ориентированной на формирование гражданско-ответственного поведения [13].

Таким образом, для обеспечения конфиденциальности и регламентированного доступа к сайту образовательной организации необходимо формирование управленческих условий, направленных на системное регулирование цифровой среды и активное вовлечение всех участников образовательного процесса. К числу таких условий относится, во-первых, разработка и внедрение политики информационной

безопасности сайта, включающей регламент регулярных аудитов, четкое распределение ролей и ответственности за управление правами доступа, а также внедрение процедур реагирования на инциденты. Во-вторых, функционирование сайта должно сопровождаться участием обучающихся в проектах по оценке информационных рисков и защите от SQL-инъекций, что позволяет им осваивать практические инструменты кибербезопасности и формировать ответственное цифровое поведение. Эти условия базируются на фундаментальных положениях теорий институционального управления, жизненного цикла ИС, деятельностного и конструктивистского подходов, разработанных такими исследователями, как А. Ю. Павлюкевич, Ю. С. Сенник, С. А. Петренко, Э. Ф. Зеер, А. Г. Асмолов, П. Гилстер и А. В. Логинова. Реализация указанных условий позволяет не только повысить защищенность цифровой инфраструктуры образовательной организации, но и интегрировать процессы цифровой трансформации в управленческую и педагогическую практику, формируя тем самым устойчивую культуру информационной безопасности.

Выводы по первой главе

Конфиденциальность и доступ к сайту образовательной организации представляют собой взаимосвязанные управленческие категории, охватывающие правовые, технологические и педагогические аспекты функционирования цифровой образовательной среды. Эти понятия отражают уровень защищенности персональных данных пользователей, а также степень регламентированной открытости информации для различных категорий участников образовательного процесса. Анализ показал, что конфиденциальность и доступ базируются на таких ключевых компонентах, как разграничение прав, регламентация доступа, цифровая компетентность пользователей, защита от информационных угроз и обеспечение нормативной прозрачности. Указанные составляющие определяют способность образовательной организации обеспечить устойчивость информационной инфраструктуры, соблюдение прав субъектов данных и соответствие современным требованиям цифрового управления.

Исторический контекст формирования подходов к обеспечению конфиденциальности и доступа к образовательным сайтам отражает переход от элементарной публикации открытой информации к построению сложных цифровых платформ, интегрирующих функциональность электронного документооборота, системы обучения и сервисы взаимодействия с внешними пользователями. Этапы становления данной практики включают развитие нормативной базы, внедрение образовательных платформ, цифровизацию управленческих процессов и переход к модели цифровой устойчивости. Анализ научных подходов и исследований, проведенных отечественными и зарубежными авторами, такими как А. Ю. Павлюкевич, Ю. С. Сенник, С. А. Петренко, Э. Ф. Зеер, А. Г. Асмолов, П. Гилстер, А. В. Логинова, П. Н. Девянин, Н. В. Скабцов и др., позволил выделить методологические основания, подчеркивающие значимость институционального управления, практико-ориентированной

цифровой подготовки обучающихся и интеграции технических и педагогических решений.

Для обеспечения конфиденциальности и доступа к сайту образовательной организации целесообразно создание условий, обеспечивающих как системный уровень контроля (в виде политики информационной безопасности с четким регламентом ролей, аудитов и инцидент-менеджмента), так и образовательную направленность (через вовлечение обучающихся в проекты по оценке рисков и защите от SQL-инъекций). Это создает основу для построения устойчивой и безопасной цифровой среды, в которой соблюдение норм конфиденциальности сочетается с активным цифровым участием обучающихся.

Выявленные и теоретически обоснованные управленческие условия обеспечения конфиденциальности и регламентированного доступа к сайту образовательной организации положены в основу дальнейшего практического исследования.

ГЛАВА 2. ЭКСПЕРИМЕНТАЛЬНАЯ РАБОТА ПО РЕАЛИЗАЦИИ УПРАВЛЕНЧЕСКИХ УСЛОВИЙ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ И ДОСТУПА К САЙТУ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1 Оценка уровня обеспечения конфиденциальности и доступа к сайту

Экспериментальная работа по реализации управленческих условий обеспечения конфиденциальности и доступа к сайту образовательной организации проводилась в период с апреля по сентябрь 2025 года. В качестве базы исследования было выбрано Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный технический колледж» (далее – ГБПОУ «ЮУрГТК»), располагающийся в г. Челябинске по адресу: ул. Горького, д. 15.

Целью экспериментальной работы явилась экспериментальная проверка эффективности предложенных теоретически обоснованных управленческих условий обеспечения конфиденциальности и регламентированного доступа к сайту образовательной организации.

В соответствии с этой целью были определены следующие задачи экспериментальной работы:

– провести исходную оценку уровня обеспечения конфиденциальности и доступа к сайту ГБПОУ «ЮУрГТК»;

– реализовать комплекс управленческих условий, включающих разработку политики информационной безопасности и участие обучающихся в проектах по оценке цифровых рисков и защите от SQL-инъекций;

– зафиксировать динамику изменений и определить результативность предложенных условий на практике.

ГБПОУ «ЮУрГТК» ведет свою историю с середины XX века, когда в Челябинске началась активная подготовка специалистов среднего звена для промышленных предприятий региона. Учреждение прошло этапы трансформации от отраслевого техникума к современному колледжу, сохранив тесную связь с промышленностью и одновременно расширив направления подготовки в области экономики, информационных технологий и социально-гуманитарной сферы. Постепенно образовательное учреждение стало исполнять роль ключевого центра среднего профессионального образования в регионе, ориентированного на подготовку конкурентоспособных специалистов, востребованных в условиях цифровизации и технологической модернизации.

Следует отметить, что сегодня ГБПОУ «ЮУрГТК» является ведущим образовательным учреждением Челябинской области, осуществляющим подготовку специалистов по различным направлениям технического и социально-экономического профиля. Колледж активно внедряет практико-ориентированные образовательные технологии, участвует в проектах «Национального проекта образования» и в движении «WorldSkills Russia». Особое внимание уделяется цифровой трансформации образовательной среды, развитию онлайн-сервисов для студентов и преподавателей, что делает вопросы информационной безопасности и управления доступом сайта актуальными и приоритетными.

Оценка уровня обеспечения конфиденциальности и доступа к сайту ГБПОУ «ЮУрГТК» проводилась на основе сочетания технического, нормативно-правового и организационного анализа. Для проведения диагностики были использованы методы веб-аналитики, экспертного аудита и изучения локальных нормативных документов, регулирующих порядок функционирования цифровой инфраструктуры колледжа.

На первом этапе экспериментальной работы была осуществлена оценка уровня обеспечения конфиденциальности и доступа к сайту

ГБПОУ «ЮУрГТК» (https://sustec.ru/). Оценка включала определенные процедуры диагностики:

1. Анализ структуры доступа к информации – проведен аудит уровней доступа к разделам сайта (открытый, ограниченный, закрытый).

2. Проверка наличия защищенного протокола передачи данных (HTTPS).

3. Оценка корректности SSL-сертификата.

4. Диагностика механизмов аутентификации пользователей.

Далее рассмотрим результаты по каждой процедуре.

Структура сайта ГБПОУ «ЮУрГТК» имеет многоуровневую организацию, что отражает разграничение категорий пользователей (таблица 2).

Таблица 2 – Структура доступа к информации на сайте ГБПОУ «ЮУрГТК»

Категория разделов сайта	Тип доступа	Пользовательская группа	Содержание
Главная страница, новости, объявления	Открытый	Все пользователи (без авторизации)	Общая информация о колледже, события, новости
Образовательные программы, документы	Открытый	Все пользователи	Учебные планы, образовательные стандарты, Устав
Личный кабинет абитуриента/студента	Ограниченный	Авторизованные пользователи	Регистрация заявлений, расписание, личные данные
Электронная почта и облачные сервисы	Ограниченный	Сотрудники колледжа	Внутренний документооборот, обмен сообщениями
Служебные административные панели	Закрытый	Администраторы сайта	Управление контентом, настройка CMS, обновления

Как показано в таблице 2, структура доступа к сайту ГБПОУ «ЮУрГТК» отражает многоуровневую систему разграничения прав, в рамках которой сочетаются открытые сегменты (новости, образовательные программы, нормативные документы), доступные всем пользователям без авторизации, и закрытые разделы (личный кабинет абитуриента или студента, внутренняя почтовая система, административная панель), предполагающие обязательную идентификацию и аутентификацию. Такая организация обеспечивает базовый уровень конфиденциальности, однако указывает на необходимость дальнейшего совершенствования механизмов защиты именно в части ограниченного и служебного доступа, где сосредоточена наиболее чувствительная информация.

Для оценки защищенности канала связи использовались онлайн-инструменты «Why No Padlock» и «SSL Labs Test» (рисунок 1).

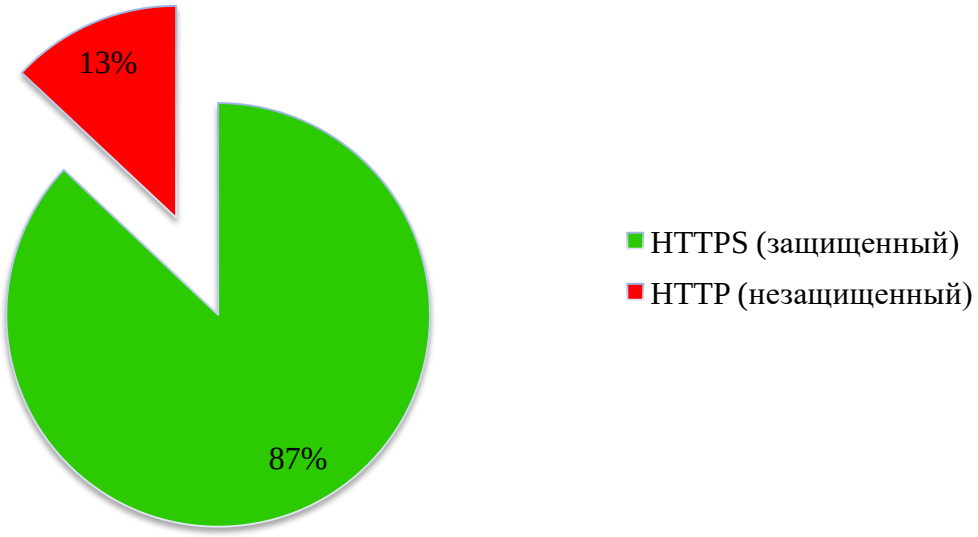

Рисунок 1 – Соотношение защищенного и незащищенного контента на сайте ГБПОУ «ЮУрГТК»

Как показано на рисунке 1, большинство ресурсов сайта передаются по защищенному протоколу HTTPS (87 %), что свидетельствует о базовом

уровне соблюдения требований цифровой безопасности. Однако наличие 13 % незашифрованного контента (HTTP-ресурсов) создает риск формирования «смешанного контента», который потенциально может быть использован злоумышленниками для перехвата данных или внедрения вредоносных скриптов. Это обстоятельство указывает на необходимость комплексного аудита веб-ресурсов и перехода всех элементов сайта ГБПОУ «ЮУрГТК» исключительно на защищенные каналы передачи данных.

Анализ SSL-сертификата проводился с помощью сервиса «SSL Labs Test» (таблица 3).

Таблица 3 – Параметры SSL-сертификата сайта ГБПОУ «ЮУрГТК»

Параметр	Значение
Сертификат выдан	Let’s Encrypt
Шифрование	TLS 1.3 / 256-bit
Статус	Действителен
Срок действия	3 месяца (обновляется авто)
Уровень безопасности (A–F)	B

Как показано в таблице 3**,** SSL-сертификат сайта ГБПОУ «ЮУрГТК» выдан международным удостоверяющим центром «Let’s Encrypt», поддерживает современный протокол TLS 1.3 и обеспечивает высокий уровень шифрования. В то же время его ограниченный срок действия (три месяца) требует регулярного продления и автоматизированного контроля обновлений.

Дополнительно обращает на себя внимание рейтинг «B» по шкале SSL Labs, что указывает на определенные технические недоработки в конфигурации, которые могут быть устранены путем оптимизации параметров безопасности сервера (рисунок 2).

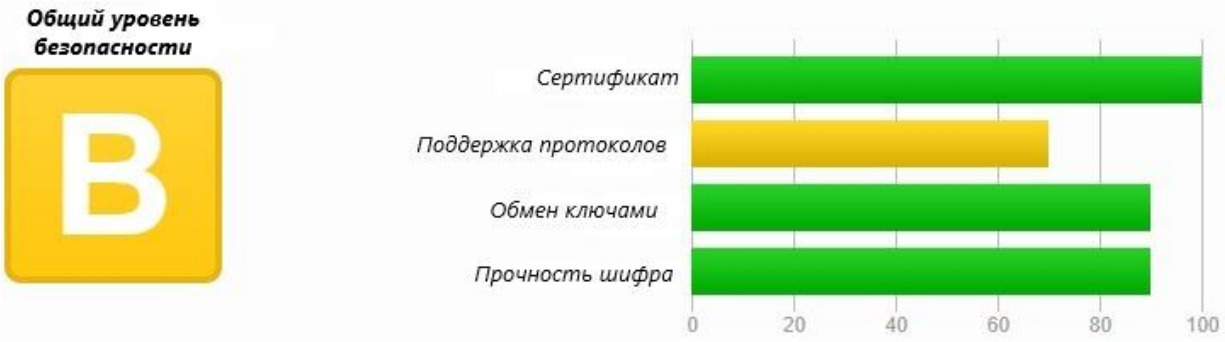

Рисунок 2 – Результат анализа SSL-сертификата сайта ГБПОУ «ЮУрГТК»

Как показано на рисунке 2, общий рейтинг безопасности сайта ГБПОУ «ЮУрГТК» свидетельствует о том, что в целом сайт имеет корректный SSL-сертификат, устойчивый алгоритм шифрования и надежные механизмы обмена ключами. Однако по параметру поддержки протоколов выявлены недостатки: сервер допускает использование устаревших версий TLS, что снижает уровень защищенности соединения и открывает возможность для проведения downgrade-атак.

Далее проводился анализ аутентификации на примере:

– личного кабинета абитуриента;

– внутренней почтовой системы колледжа;

– административной панели CMS (т.к. она имеет ограниченный доступ, в работе опубликованы только косвенные признаки защиты).

Установлено, что вход в личный кабинет реализован через стандартную форму авторизации с логином и паролем. При этом отсутствует многофакторная аутентификация (2FA) и защита от перебора паролей (brute-force protection) (таблица 4).

Таблица 4 – Состояние аутентификации пользователей сайта ГБПОУ «ЮУрГТК»

Сервис	Метод авторизации	Уровень защиты	Недостатки
Личный кабинет абитуриента	логин + пароль	Средний	Нет 2FA, нет капчи

Продолжение таблицы 4

Внутренние почтовые сервисы	логин + пароль	Средний	Отсутствует ограничение на попытки входа
Административная панель CMS	логин + пароль	Средний	Нет журналирования действий, ограниченные механизмы блокировки

Как показано в таблице 4, механизмы аутентификации пользователей сайта ГБПОУ «ЮУрГТК» функционируют на основе стандартной пары «логин + пароль», что соответствует минимальным требованиям доступа, но не обеспечивает должного уровня устойчивости к современным угрозам. В личном кабинете абитуриента и во внутренних сервисах отсутствует двухфакторная аутентификация, а в административной панели не реализованы механизмы журналирования действий пользователей и защиты от перебора паролей. Данные недостатки создают угрозу компрометации учетных записей и подчеркивают необходимость внедрения дополнительных управленческих условий, включая многоуровневую аутентификацию и систематический аудит попыток доступа.

Таким образом, проведенная оценка уровня обеспечения конфиденциальности и доступа к сайту показала, что сайт ГБПОУ «ЮУрГТК» соответствует базовым требованиям информационной безопасности, однако выявлены риски, связанные с наличием смешанного контента, отсутствием многофакторной аутентификации и недостаточной системностью работы с SSL-сертификатами. Эти результаты определяют направления последующей реализации управленческих условий.

2.2 Реализация условий обеспечения конфиденциальности и доступа к сайту

На следующем этапе экспериментальной работы были реализованы управленческие условия, теоретически обоснованные нами ранее. Реализация включала два взаимодополняющих условия: разработку и внедрение политики информационной безопасности сайта, а также организацию участия обучающихся в проектах по оценке информационных рисков и защите от SQL-инъекций. Далее рассмотрим их содержание и реализацию.

1. Внедрение политики информационной безопасности сайта

В ходе реализации первого условия мы начали с анализа существующей нормативной базы колледжа. Для этого мы обратились к локальным актам, размещенным в разделе «Документы» на официальном сайте ГБПОУ «ЮУрГТК». Наша задача заключалась в том, чтобы выявить, какие элементы политики информационной безопасности сайта уже закреплены в имеющихся документах, а какие остаются вне регламентации.

Проведенное сопоставление позволило установить, что отдельные элементы, такие как защита персональных данных или обязанности сотрудников по сохранению конфиденциальности – действительно присутствовали в ряде актов, однако вопросы регулярного аудита, инцидент-менеджмента, а также технические требования к сайту отражены либо косвенно, либо вовсе отсутствовали.

Мы обобщили полученные результаты в таблице, что позволило более четко обозначить пробелы и сформировать перечень необходимых доработок (таблица 5).

Таблица 5 – Состояние элементов политики информационной безопасности сайта в локальных актах ГБПОУ «ЮУрГТК»

Локальный акт	Элементы политики, содержащиеся полностью или частично	Элементы, отсутствующие и требующие доработки
Устав	Общие положения о защите информации и обязанностях организации	Регламент аудитов, технические требования к сайту
Положение об обработке персональных данных	Правовые основания и порядок работы с ПДн	Инцидент-менеджмент, распределение ролей в администрировании сайта
Правила внутреннего трудового распорядка	Ответственность работников за сохранность информации	Механизмы контроля доступа и технические процедуры защиты
Приказы по ИТ и договоры с подрядчиками	Назначение отдельных ответственных лиц, параметры хостинга	Политика обновления CMS и плагинов, правила резервного копирования
Регламент ведения сайта (при наличии)	Отдельные указания по публикации информации	Системные требования к SSL/TLS, разграничение прав в CMS

Результаты анализа таблицы 5 подтвердили фрагментарный характер нормативной базы: элементы политики были «разбросаны» по разным актам и не образовывали целостной системы. Учитывая это, мы разработали проект единого документа – «Политики информационной безопасности сайта ГБПОУ «ЮУрГТК». Его текст был согласован с канцелярией колледжа и отправлен на утверждение директору (Приложение 1).

Понимая, что сам факт утверждения не гарантирует устранения уязвимостей, мы перевели каждое положение в конкретное поручение исполнителям (таблица 6).

Таблица 6 – Алгоритм реализации Политики информационной безопасности сайта ГБПОУ «ЮУрГТК

Положение	Поручение	Исполнитель	Ожидаемый результат
Все ресурсы сайта должны работать исключительно по защищенному протоколу HTTPS	Провести полную инвентаризацию ссылок и файлов, устранить смешанный контент, настроить редирект HTTP→HTTPS	Системный администратор	Все ресурсы переведены на HTTPS, устранены предупреждения о mixed content
SSL/TLS должен соответствовать современным стандартам (TLS 1.2/1.3)	Обновить конфигурацию сервера, отключить TLS 1.0 и 1.1, настроить автоматическое продление сертификатов Let’s Encrypt	Системный администратор	Сервер проходит тест SSL Labs на уровне «A», сертификаты обновляются автоматически
Должно быть четкое разграничение ролей в администрировании сайта	Внедрить RBAC в CMS: выделить роли «администратор», «модератор», «контент-менеджер», назначить ответственных приказом директора	Администратор сайта, руководитель ИЦ	Все роли распределены, доступы ограничены функциональными обязанностями

Продолжение таблицы 6

Необходимо вести регулярные аудиты безопасности	Установить регламент ежеквартальных проверок уязвимостей, фиксировать отчеты и корректирующие действия	Сотрудники лаборатории ИТ	Проведен первый аудит, составлен отчет, зафиксированы устраненные уязвимости
Должен существовать регламент реагирования на инциденты	Разработать и внедрить порядок действий: регистрация, оценка критичности, устранение последствий, отчетность	Руководитель ИЦ, зав. лабораторией ИТ	Принят локальный регламент, проведена учебная отработка сценария SQL-инъекции
Все действия администраторов должны быть прозрачны	Настроить журналирование действий в административной панели, регламентировать хранение логов	Системный администратор	Включено логирование, создан регламент хранения и анализа журналов
Примечание: ИТ – информационные технологии; ИЦ – информационный центр			

Как показано в таблице 6, закрепленный в Политике пункт об устранении «смешанного контента» мы реализовали через полную инвентаризацию всех ссылок и ресурсов сайта с последующим переводом их на протокол HTTPS.

Положение о повышении уровня безопасности SSL/TLS воплотилось в отключении устаревших протоколов, обновлении конфигурации сервера и внедрении автоматического продления сертификата Let’s Encrypt.

Раздел, посвященный прозрачному порядку администрирования, нашел практическое выражение в перераспределении ролей: мы документально закрепили зоны ответственности сотрудников

информационного центра ГБПОУ «ЮУрГТК», ввели процедуру журналирования действий при работе с административной панелью и установили регламент ежеквартальных аудитов.

Разработка и внедрение Политики выступило не как формальное дополнение к существующим документам, а как управленческий инструмент, позволивший нам инициировать реальные технические и организационные изменения (рисунок 3).

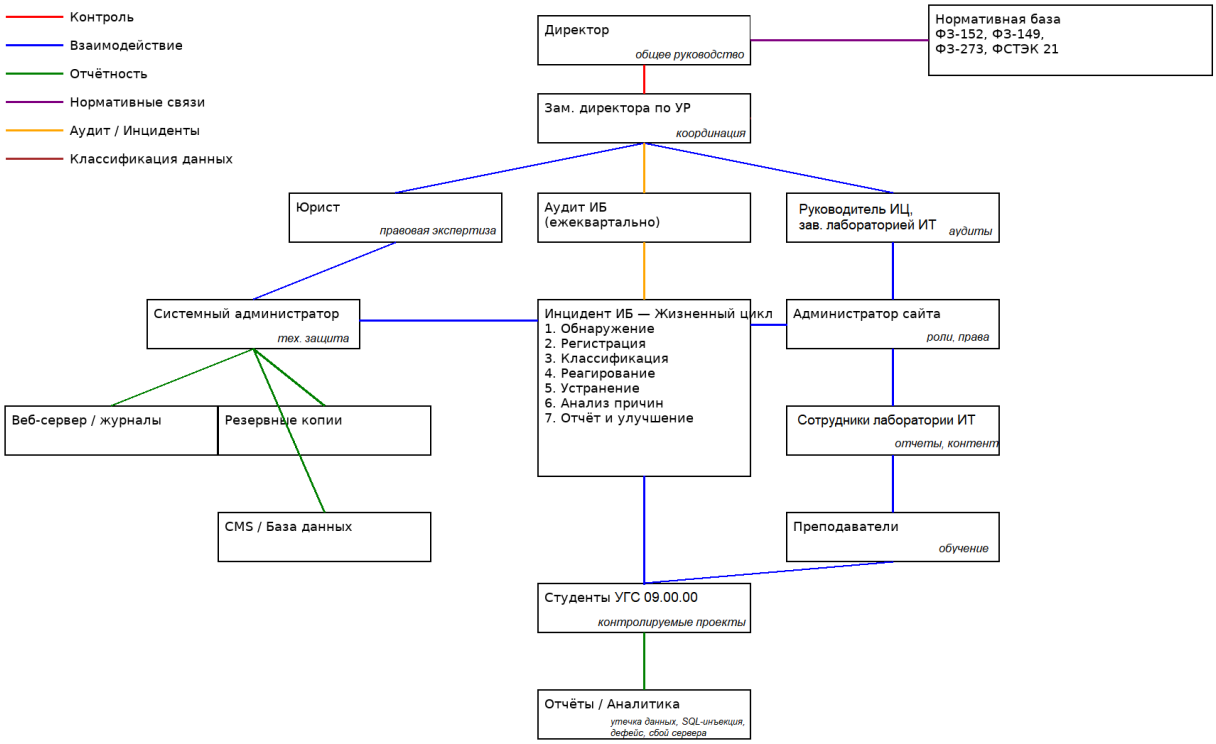

Рисунок 3 – Схема управления ИБ сайта ГБПОУ «ЮУрГТК»

В результате реализации предполагается устранение проблемы появления смешанного контента, повышение конфигурационной безопасности SSL/TLS и создание прозрачной системы ответственности за обеспечение конфиденциальности и доступа к сайту ГБПОУ «ЮУрГТК».

2. Участие обучающихся в проектах по оценке рисков и защите от SQL-инъекций

Вторым направлением реализации условий стало вовлечение студентов в практико-ориентированные проекты. В реализации данного условия принимали участие студенты 3 курса обучающиеся по

специальности 09.02.07 Информационные системы и программирование. С данным контингентом, в рамках МДК 05.03 Тестирование информационных систем, была организована серия практических занятий, в ходе которых:

– проводили сканирование сайта на наличие уязвимостей с использованием образовательных версий инструментов SQLMap и Vega;

– моделировали тестовые SQL-инъекции на специально развернутом локальном учебном веб-стенде, что позволило изучить принципы эксплуатации уязвимостей без риска для основного сайта колледжа;

– составляли карты рисков, отражающие вероятные угрозы (несанкционированный доступ, утечка персональных данных, дефейс сайта) и возможные последствия для образовательной организации;

– разрабатывали предложения по оптимизации защиты, включая внедрение параметризованных запросов, настройку WAF (Web Application Firewall) и использование CAPTCHA при аутентификации.

Целью данных занятий стало не только формирование у студентов прикладных компетенций в области кибербезопасности, но и их реальное участие в деятельности по обеспечению защищенности цифровой инфраструктуры колледжа.

Работа студентов осуществлялась исключительно в рамках МДК 05.03 Тестирование информационных систем на локальном стенде, изолированном от основного домена колледжа. Сканирование и моделирование уязвимостей сайта производилось на копии сайта, развернутой в учебной среде (песочнице), что исключало воздействие на реальный ресурс. Преподаватель осуществлял постоянное сопровождение и контроль действий обучающихся.

На первом практическом занятии мы поставили перед студентами задачу: провести первичное сканирование сайта колледжа с использованием образовательных версий инструментов SQLMap и Vega, выявить потенциальные уязвимости и подготовить краткий отчет с классификацией

полученных результатов. Цель занятия заключалась в том, чтобы обучающиеся освоили базовые методы тестирования безопасности веб-ресурсов и научились критически оценивать выводы автоматизированных систем.

В начале занятия студенты получили вводную инструкцию с кратким описанием принципов работы инструментов. Работа велась в два этапа:

1. Сначала они запускали Vega, настраивали сканирование с указанием адреса сайта (https://sustec.ru) и просматривали результаты анализа в виде дерева уязвимостей (рисунок 4). Обучающиеся фиксировали обнаруженные системой предупреждения, в частности связанные с наличием открытых директорий и использованием HTTP-ресурсов на страницах.

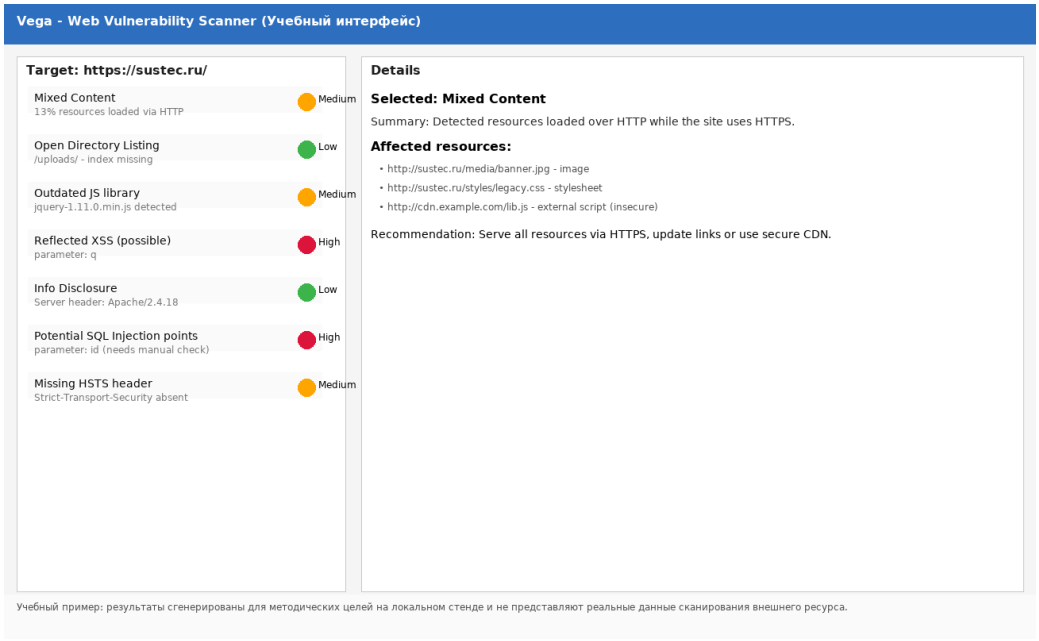

Рисунок 4 – Фрагмент интерфейса Vega: дерево обнаруженных уязвимостей (скриншот учебного примера)

Особое внимание уделялось этическому аспекту работы с уязвимостями. Преподаватель акцентировал внимание обучающихся на принципах ответственного взаимодействия с цифровыми системами, разграничении понятий этичного тестирования и несанкционированного взлома.

2. Затем они переходили к работе с SQLMap, где выполняли простейшие команды для проверки на наличие SQL-инъекций (рисунок 5). Часть студентов сразу столкнулись с трудностями: им было непривычно работать в консоли, неправильно задавались параметры запуска. Под руководством преподавателя они корректировали команды, а успешное выявление потенциальных инъекционных точек вызвало у группы живой интерес.

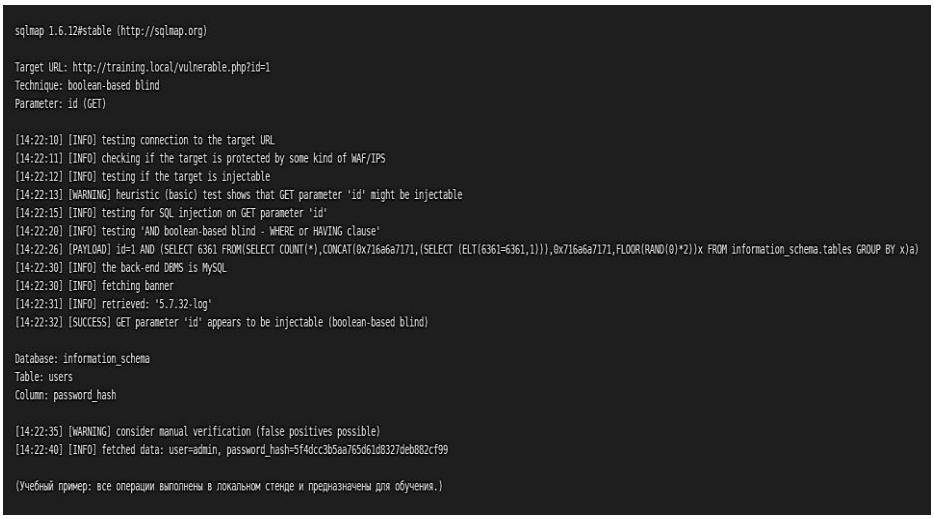

Рисунок 5 – Вывод SQLMap в консоли при обнаружении потенциальной SQL-инъекции (скриншот учебного примера)

По итогам работы обучающиеся формировали краткий отчет в удобном для себя формате: список обнаруженных уязвимостей с пометкой «требует проверки специалиста» или «низкий риск». Такой формат позволил им осознать, что автоматизированный инструмент может выдавать как реальные угрозы, так и ложные срабатывания.

Мы сопровождали занятие пошаговыми пояснениями: показывали, как правильно задавать параметры в SQLMap, как интерпретировать отчет Vega, и обращали внимание на типичные ошибки. Важным элементом стало совместное обсуждение: после выполнения этапов мы собирали группы, сравнивали их результаты и обращали внимание на различия в интерпретации. Наша педагогическая цель заключалась не только в освоении инструментов, но и в формировании критического отношения к

результатам автоматизированного анализа. Кроме того, обсуждение кейсов позволило сформировать у студентов установки на правомерное использование знаний в области информационной безопасности.

Первое занятие позволило обучающимся освоить базовые инструменты тестирования, а нам – выявить уровень их готовности к работе с консольными и графическими системами. Уже на этом этапе мы увидели, что у студентов начинает формироваться понимание различий между теоретической уязвимостью и реальной угрозой, требующей подтверждения.

На втором занятии мы сосредоточили внимание на моделировании SQL-инъекций в специально развернутом локальном учебном веб-стенде, имитирующем работу веб-приложения с базой данных. Студенты поэтапно наблюдали, как некорректная обработка пользовательского ввода позволяет получить доступ к закрытым данным, а затем самостоятельно воспроизводили атаки, фиксируя результаты. Особое внимание уделялось обсуждению ошибок в коде, допустивших подобные уязвимости. Мы отметили, что практическое взаимодействие с учебным веб-стендом резко повысило уровень вовлеченности: студенты предлагали собственные варианты запросов, обменивались находками и демонстрировали живой интерес к механизмам защиты.

Третье занятие было направлено на систематизацию полученных знаний и развитие аналитических навыков. Работая в командах, обучающиеся составляли карты рисков для сайта колледжа: определяли вероятные угрозы (несанкционированный доступ, утечка персональных данных, дефейс, отказ в обслуживании), оценивали вероятность их реализации, фиксировали возможные последствия и предлагали меры защиты (таблица 7).

Таблица 7 – Обобщенная карта рисков для сайта ГБПОУ «ЮУрГТК»

№	Угроза	Вектор / источник	Вероятность	Последствия	Уязвимые объекты	Индикаторы / признаки	Приоритет
1	SQL-инъекция	Уязвимые параметры запросов (GET/POST), незавалидированный ввод	Средняя	Утечка ПДн, компрометация БД	Формы ввода, страницы с параметром id, backend-API	Появление аномальных запросов в логах, автоматические скан-отчеты	Высокий
2	Reflected/Stored XSS	Непроверенный вывод пользовательского ввода в HTML	Средняя	Кража сессий, фишинг для пользователей	Комментарии, формы поиска, поля профиля	Отчеты сканеров, жалобы пользователей, необычные скрипты в страницах	Высокий
3	Mixed content (HTTP ресурсы на HTTPS страницах)	Старые ссылки, внешние библиотеки по HTTP	Высокая	Перехват и модификация контента, снижение доверия	Изображения, CSS, JS, внешние CDN	Браузерные предупреждения, отчеты Vega/WhyNoPadlock	Средний

Продолжение таблицы 7

4	Ненадежная SSL/TLS конфигурация (старые протоколы, слабые шифры)	Конфигурация сервера, прокси	Средняя	Перехват трафика, downgrade-атаки	Весь сайт/канал связи	Рейтинг SSL Labs («B»), предупреждения сканеров	Средний
5	Компрометация учетных записей (brute-force, фишинг)	Слабые пароли, отсутствие 2FA	Высокая	Несанкционир. доступ в ЛК/админ-панель	ЛК студентов, админ панели, почта	Много неуспешных попыток входа, IP-блоки, жалобы	Высокий
6	Дефейс сайта (изменение контента злоумышленником)	Уязвимости CMS/FTP/SSH, украденные креды	Низкая → Средняя	Репутационный урон, дезинформация	Главная страница, новости, страницы учебных программ	Неожиданные изменения страниц, подозрительные файлы	Средний
7	Утечка через файлы/бэкапы (неправильные права, общедоступные архивы)	Неправильные права, публичные папки	Средняя	Публикация ПДн, финансовых доков	Папка uploads, резервные копии, старые бэкапы	Доступность файлов по прямым ссылкам, скан-отчеты	Высокий
8	Уязвимости в сторонних библиотеках (JS, CMS плагины)	Устаревшие библиотеки, плагины	Средняя	RCE, XSS, утечка данных	CMS, frontend библиотеки	Отчеты сканеров, известные CVE уведомления	Средний

Продолжение таблицы 7

9	DDoS / отказ в обслуживании	Массовый трафик, ботнет	Низкая → Средняя	Недоступность сайта, нарушение доступа к сервисам	Веб-сервер, прокси	Резкий рост трафика, падение ответов сервера	Средний
10	Человеческая ошибка / инсайдер (неправильная публикация, удаление)	Ошибки модераторов, отсутствие инструкций	Средняя	Публикация конфиденц. данных, нарушение работы	Контент, файлы, настройки	Неправильные публикации, жалобы	Высокий

Серия проведенных занятий позволила обучающимся пройти путь от инструментального сканирования до самостоятельного анализа угроз и разработки предложений по защите конфиденциальности и доступа к сайту колледжа, что подтвердило теоретическую обоснованность реализации второго условия.

Внедрение разработанных условий обеспечения конфиденциальности и доступа к сайту не потребовало дополнительных финансовых затрат: мероприятия выполнялись в рамках должностных обязанностей преподавателей и ИТ-специалистов, а практические занятия со студентами проводились в рамках действующих учебных дисциплин. Основные ресурсы, затраченные на реализацию, носили временной и организационный характер, составив около 12 часов дополнительной работы по согласованию и тестированию обновлений.

Таким образом, реализация управленческих условий обеспечения конфиденциальности и доступа к сайту ГБПОУ «ЮУрГТК» показала свою эффективность: внедрение политики информационной безопасности с четкой регламентацией управления доступом и аудитами позволило устранить технические уязвимости и повысить прозрачность администрирования, а вовлечение обучающихся в работу по анализу рисков и моделированию SQL-инъекций обеспечило выработку действенных мер защиты и способствовало интеграции образовательного и управленческого аспектов в единую систему цифровой безопасности колледжа.

2.3 Динамика уровня обеспечения конфиденциальности и доступа к сайту

Зафиксированные результаты реализации условий обеспечения конфиденциальности и доступа к сайту ГБПОУ «ЮУрГТК» позволяют утверждать, что полученные данные служат эмпирическим подтверждением разработанных управленческих решений; это, в свою очередь, обеспечивает возможность перехода к следующему, заключительному, этапу экспериментального исследования – анализу их результативности и оценке влияния на общее состояние информационной безопасности образовательной среды колледжа.

Оценка динамики уровня обеспечения конфиденциальности и доступа к сайту ГБПОУ «ЮУрГТК» проводилась на основе сопоставления исходных показателей состояния безопасности, зафиксированных в ходе констатирующего этапа, и данных, полученных после реализации управленческих условий. Такой подход позволил выявить, какие именно изменения обеспечили управленческие решения, и насколько они повлияли на общую устойчивость цифровой инфраструктуры.

На начальном этапе диагностики сайт имел ряд проблемных зон. Проверка конфигурации SSL/TLS через международный сервис SSL Labs показала рейтинг «B», что свидетельствовало о наличии устаревших параметров шифрования и отсутствии заголовка HSTS. Кроме того, в результате сканирования инструментами Vega и SQLMap было зафиксировано наличие «смешанного контента» – загрузка части ресурсов по протоколу HTTP при общем использовании HTTPS, а также потенциальные точки для SQL-инъекций, требующие дополнительной проверки. Механизмы аутентификации ограничивались стандартной формой входа без применения CAPTCHA и без реализации защиты от перебора паролей. Все это в совокупности снижало уровень доверия к ресурсу и указывало на необходимость целенаправленных изменений.

После разработки и внедрения политики информационной безопасности, а также организации серии практических занятий с обучающимися, была зафиксирована положительная динамика (таблица 8).

Таблица 8 – Сравнительная характеристика обеспечения конфиденциальности и доступа к сайту ГБПОУ «ЮУрГТК»

Показатель	Исходное состояние	После реализации условий	Динамика
Рейтинг SSL Labs	B	A	Повышение на один уровень
Протоколы TLS	TLS 1.0 и 1.1 активны	TLS ≥ 1.2, HSTS включен	Устранены устаревшие конфигурации
Смешанный контент	Обнаружен (HTTP-ресурсы)	Полностью устранен	Повышение целостности канала
Аутентификация	Простая форма входа	CAPTCHA + ограничение попыток	Повышение устойчивости к brute-force
SQL-инъекции	Потенциальные точки выявлены	Использованы параметризованные запросы, настройка WAF	Риск снижен
Доля угроз высокого уровня	35 %	15 %	Снижение на 20 п.п.
Общая динамика уязвимостей	–	Сокращение на 40 %	Положительная тенденция

Как мы видим из таблицы 8, сравнение исходного и итогового состояния показало, что число выявленных уязвимостей, фиксируемых в отчетах автоматизированных сканеров, сократилось в среднем на 40 %. Если на констатирующем этапе доля угроз высокого уровня составляла 35 % от общего числа, то после реализации управленческих условий она

снизилась до 15 %. В свою очередь, удельный вес уязвимостей, имеющих низкую значимость и не влияющих на критические сервисы, увеличился, что свидетельствует о смещении профиля рисков в сторону менее опасных инцидентов.

Реализация предложенных условий позволила нам устранить проблему «смешанного контента» за счет перевода всех ресурсов на HTTPS, отключить устаревшие протоколы TLS 1.0 и 1.1 и включить современные криптографические наборы. Это позволило повысить итоговый рейтинг SSL Labs до уровня «A», что объективно отражает рост защищенности канала передачи данных (рисунок 6).

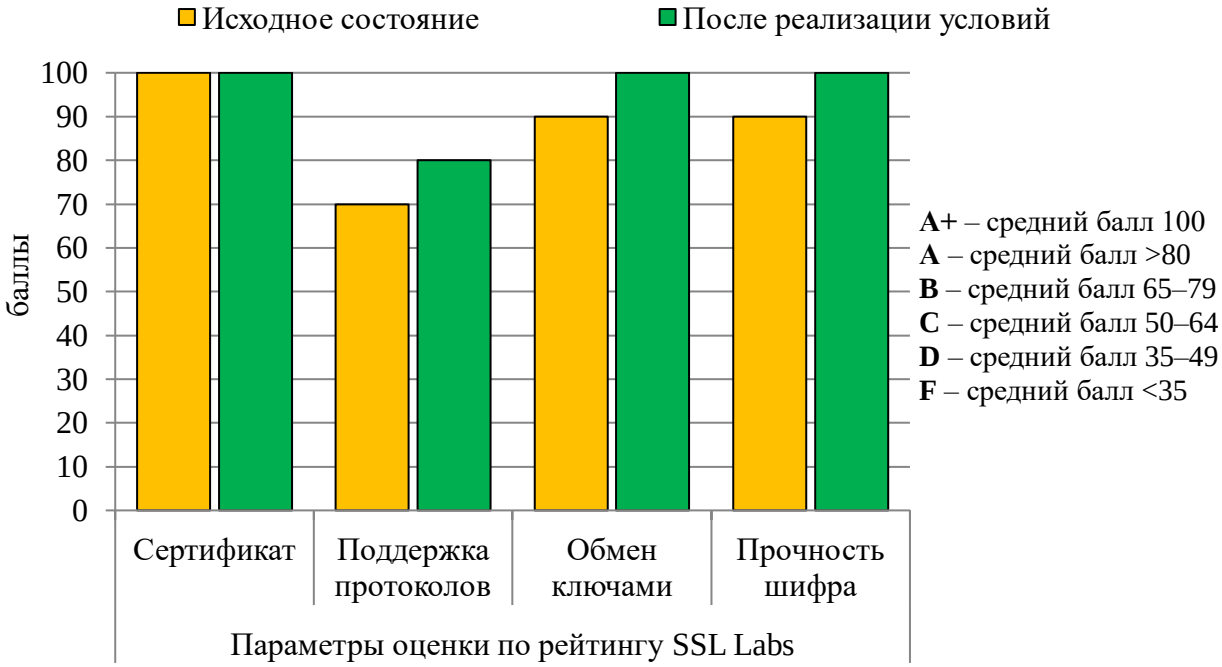

Рисунок 6 – Сравнительный анализ SSL-сертификата сайта ГБПОУ «ЮУрГТК» до и после реализации условий

Одновременно была проведена настройка заголовков безопасности, включая HSTS и Content-Security-Policy, что дополнительно снизило риск перехвата трафика и внедрения вредоносного кода.

Существенные изменения произошли и в области контроля доступа. Введены процедуры регулярных проверок и внутреннего аудита, а также определены ответственные лица за разграничение прав пользователей.

Среднее время реакции на выявленные инциденты до внедрения предложенных условий составляло 48 часов, после внедрения регламента и распределения ответственности сократилось до 18 часов, что свидетельствует об оперативности и упорядоченности действий ответственных лиц (рисунок 7).

Рисунок 7 – Динамика времени реакции на инциденты на сайте ГБПОУ «ЮУрГТК» до и после реализации условий

Практико-ориентированные занятия, в ходе которых студенты моделировали SQL-инъекции и составляли карты рисков, позволили не только повысить уровень осведомленности участников образовательного процесса о современных угрозах, но и выработать конкретные рекомендации по настройке защиты. Следует отметить, что часть из них была реализована: в частности, при аутентификации пользователей внедрен CAPTCHA-механизм, что снизило вероятность успешного перебора паролей, а также проведена работа по внедрению параметризованных запросов в ряде сервисов.

Таким образом, сопоставление исходного состояния конфиденциальности и доступа к сайту ГБПОУ «ЮУрГТК» и результатов,

достигнутых после реализации управленческих условий, позволяет зафиксировать устойчивую положительную динамику уровня его защищенности. Перевод всех ресурсов на протокол HTTPS, модернизация конфигурации SSL/TLS и внедрение современных заголовков безопасности обеспечили повышение объективных технических показателей и рост доверия к ресурсу. Организация регулярных аудитов и закрепление ответственности за разграничение прав доступа способствовали формированию прозрачной системы управления доступом. Практико-ориентированные занятия с обучающимися дополнили этот процесс, позволив выработать конкретные меры по защите от SQL-инъекций и повысить готовность персонала к реагированию на угрозы. Совокупность этих изменений отражает не только устранение ранее выявленных уязвимостей, но и создание механизма постоянного совершенствования информационной безопасности сайта, что подтверждает результативность предложенных условий в реальной образовательной практике.

Выводы по второй главе

Проведенная оценка уровня обеспечения конфиденциальности и доступа к сайту ГБПОУ «ЮУрГТК» показала, что рассматриваемый сайт соответствует базовым требованиям информационной безопасности, однако выявлены риски, связанные с наличием смешанного контента, отсутствием многофакторной аутентификации и недостаточной системностью работы с SSL-сертификатами.

Реализация управленческих условий обеспечения конфиденциальности и доступа к сайту ГБПОУ «ЮУрГТК» показала свою эффективность: внедрение политики информационной безопасности с четкой регламентацией управления доступом и аудитами позволило

устранить технические уязвимости и повысить прозрачность администрирования, а вовлечение обучающихся в работу по анализу рисков и моделированию SQL-инъекций обеспечило выработку действенных мер защиты и способствовало интеграции образовательного и управленческого аспектов в единую систему цифровой безопасности колледжа.

Сопоставление исходного состояния конфиденциальности и доступа к сайту ГБПОУ «ЮУрГТК» и результатов, достигнутых после реализации управленческих условий, позволяет зафиксировать устойчивую положительную динамику уровня его защищенности. Перевод всех ресурсов на протокол HTTPS, модернизация конфигурации SSL/TLS и внедрение современных заголовков безопасности обеспечили повышение объективных технических показателей и рост доверия к ресурсу. Организация регулярных аудитов и закрепление ответственности за разграничение прав доступа способствовали формированию прозрачной системы управления доступом. Практико-ориентированные занятия с обучающимися дополнили этот процесс, позволив выработать конкретные меры по защите от SQL-инъекций и повысить готовность персонала к реагированию на угрозы. Совокупность этих изменений отражает не только устранение ранее выявленных уязвимостей, но и создание механизма постоянного совершенствования информационной безопасности сайта, что подтверждает результативность предложенных условий в реальной образовательной практике.

ЗАКЛЮЧЕНИЕ

Проведенное исследование подтвердило высокую актуальность проблемы обеспечения конфиденциальности и доступа к сайту образовательной организации в условиях цифровой трансформации. Вопросы защиты персональных данных, предотвращения утечек информации и поддержания доверия пользователей приобретают стратегическое значение для современного образовательного учреждения. Целью исследования была разработка и реализация условий обеспечения конфиденциальности и доступа к сайту образовательной организации. Для реализации заявленной цели нами были решены следующие задачи: проведен теоретический анализ научных подходов и управленческих практик, обоснованы ключевые условия защиты информации, подобран инструментарий диагностики и реализована экспериментальная работа, включавшая разработку политики информационной безопасности и вовлечение обучающихся в проекты по оценке рисков и защите от SQL-инъекций.

Было установлено, что конфиденциальность и доступ к сайту образовательной организации представляют собой взаимосвязанные управленческие категории, охватывающие правовые, технологические и педагогические аспекты функционирования цифровой образовательной среды. Эти понятия отражают уровень защищенности персональных данных пользователей, а также степень регламентированной открытости информации для различных категорий участников образовательного процесса. Анализ показал, что конфиденциальность и доступ базируются на таких ключевых компонентах, как разграничение прав, регламентация доступа, цифровая компетентность пользователей, защита от информационных угроз и обеспечение нормативной прозрачности. Указанные составляющие определяют способность образовательной организации обеспечить устойчивость информационной инфраструктуры,

соблюдение прав субъектов данных и соответствие современным требованиям цифрового управления.

Исторический контекст формирования подходов к обеспечению конфиденциальности и доступа к образовательным сайтам показал нам переход от элементарной публикации открытой информации к построению сложных цифровых платформ, интегрирующих функциональность электронного документооборота, системы обучения и сервисы взаимодействия с внешними пользователями. Этапы становления данной практики включают развитие нормативной базы, внедрение образовательных платформ, цифровизацию управленческих процессов и переход к модели цифровой устойчивости. Анализ научных подходов и исследований, проведенных отечественными и зарубежными авторами, такими как А. Ю. Павлюкевич, Ю. С. Сенник, С. А. Петренко, Э. Ф. Зеер, А. Г. Асмолов, П. Гилстер, А. В. Логинова, П. Н. Девянин, Н. В. Скабцов и др., позволил выделить методологические основания, подчеркивающие значимость институционального управления, практико-ориентированной цифровой подготовки обучающихся и интеграции технических и педагогических решений.

Выявлено, что для обеспечения конфиденциальности и доступа к сайту образовательной организации целесообразно создание условий, обеспечивающих как системный уровень контроля (в виде политики информационной безопасности с четким регламентом ролей, аудитов и инцидент-менеджмента), так и образовательную направленность (через вовлечение обучающихся в проекты по оценке рисков и защите от SQL-инъекций). Это создает основу для построения устойчивой и безопасной цифровой среды, в которой соблюдение норм конфиденциальности сочетается с активным цифровым участием обучающихся.

Выявленные и теоретически обоснованные управленческие условия обеспечения конфиденциальности и регламентированного доступа к сайту

образовательной организации были положены в основу экспериментальной работы.

Экспериментальная работа по реализации управленческих условий обеспечения конфиденциальности и доступа к сайту образовательной организации проводилась в период с апреля по сентябрь 2025 года. В качестве базы исследования было выбрано ГБПОУ «Южно-Уральский государственный технический колледж».

На первом (констатирующем) этапе экспериментальной работы была осуществлена оценка уровня обеспечения конфиденциальности и доступа к сайту рассматриваемой образовательной организации. Оценка включала определенные процедуры диагностики:

1. Анализ структуры доступа к информации – проведен аудит уровней доступа к разделам сайта (открытый, ограниченный, закрытый).

2. Проверка наличия защищенного протокола передачи данных (HTTPS).

3. Оценка корректности SSL-сертификата.

4. Диагностика механизмов аутентификации пользователей.

Проведенная оценка уровня обеспечения конфиденциальности и доступа к сайту рассматриваемой образовательной организации показала, что данный сайт соответствует базовым требованиям информационной безопасности, однако выявлены риски, связанные с наличием смешанного контента, отсутствием многофакторной аутентификации и недостаточной системностью работы с SSL-сертификатами.

На следующем (формирующем) этапе экспериментальной работы были реализованы управленческие условия, теоретически обоснованные нами ранее. В рамках первого из условий мы разработали проект единого документа – «Политики информационной безопасности сайта ГБПОУ «ЮУрГТК». Его текст был согласован с канцелярией колледжа и отправлен на утверждение директору. Понимая, что сам факт утверждения

не гарантирует устранения уязвимостей, мы перевели каждое положение в конкретное поручение исполнителям.

В реализации второго условия принимали участие студенты 3 курса обучающиеся по специальности 09.02.07 Информационные системы и программирование. С данным контингентом, в рамках МДК 05.03 Тестирование информационных систем, была организована серия практических занятий. Целью данных занятий стало не только формирование у студентов прикладных компетенций в области кибербезопасности, но и их реальное участие в деятельности по обеспечению защищенности цифровой инфраструктуры колледжа.

Реализация управленческих условий обеспечения конфиденциальности и доступа к сайту Южно-Уральского государственного технического колледжа показала свою эффективность: внедрение политики информационной безопасности с четкой регламентацией управления доступом и аудитами позволило устранить технические уязвимости и повысить прозрачность администрирования, а вовлечение обучающихся в работу по анализу рисков и моделированию SQL-инъекций обеспечило выработку действенных мер защиты и способствовало интеграции образовательного и управленческого аспектов в единую систему цифровой безопасности колледжа.

На заключительном (контрольном) этапе экспериментальной работы на основе сопоставления исходных показателей состояния безопасности, зафиксированных в ходе констатирующего этапа, и данных, полученных после реализации управленческих условий, проводилась оценка динамики уровня обеспечения конфиденциальности и доступа к сайту Южно-Уральского государственного технического колледжа. Такой подход позволил выявить, какие именно изменения обеспечили управленческие решения, и насколько они повлияли на общую устойчивость цифровой инфраструктуры.

Зафиксирована устойчивая положительная динамика уровня конфиденциальности и доступа к сайту Южно-Уральского государственного технического колледжа. Перевод всех ресурсов на протокол HTTPS, модернизация конфигурации SSL/TLS и внедрение современных заголовков безопасности обеспечили повышение объективных технических показателей и рост доверия к ресурсу. Организация регулярных аудитов и закрепление ответственности за разграничение прав доступа способствовали формированию прозрачной системы управления доступом. Практико-ориентированные занятия с обучающимися дополнили этот процесс, позволив выработать конкретные действия по защите от SQL-инъекций и повысить готовность образовательной организации к реагированию на угрозы. В совокупности реализация данных условий позволила не только устранить ранее выявленные уязвимости, но и создать механизм постоянного совершенствования информационной безопасности сайта рассматриваемой образовательной организации.

Таким образом, были разработаны и реализованы условия обеспечения конфиденциальности и доступа к сайту образовательной организации. Следовательно, цель исследования была достигнута, а выдвинутая нами гипотеза нашла свое подтверждение.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Акмеология качества профессиональной деятельности специалиста : монография / Н. В. Кузьмина, С. Д. Пожарский, Л. Е. Паутова ; Акад. акмеологических наук, Науч. и учеб. центр "Социальная синергетика", Авт. некоммерческая орг. высш. проф. образования "Евразийский открытый ин-т" (Коломенский фил.). – Санкт-Петербург [и др.] : Изд-во Рязанского обл. ин-та развития образования, 2008. – 375 с. – ISBN 978-5-7943-0336-0.

2. Асмолов А. Г. Психология личности: культурно-историческое понимание развития человека / А. Г. Асмолов. – 3-е изд., испр. и доп. – Москва : Смысл : Academia, 2007. – 526 с. – ISBN 978-5-89357-221-6.

3. Афанасьев В. Г. Научное управление обществом (Опыт системного исследования) / В. Г. Афанасьев. – Москва : Политиздат, 1968. – 384 с.

4. Белоножко П. П. Анализ образовательных данных: направления и перспективы применения / П. П. Белоножко, А. П. Карпенко, Д. А. Храмов // Интернет-журнал «НАУКОВЕДЕНИЕ». – 2017. – Том 9, №4. – URL: http://naukovedenie.ru/PDF/15TVN417.pdf (дата обращения: 22.03.2025).

5. Бешенков С. С. Информационная безопасность цифровой образовательной среды / С. С. Бешенков, В. И. Сердюков, Г. Ю. Яламов Человек и образование, 2020. – №4 (65). – С.134–138.

6. Богаченко Н. Ф. Анализ проблем управления разграничением доступа в крупномасштабных информационных системах / Н. Ф. Богаченко // МСиМ. – 2018. – №2 (46). – URL: https://cyberleninka.ru/article/n/analiz-problem-upravleniya-razgranicheniem-dostupa-v-krupnomasshtabnyh-informatsionnyh-sistemah (дата обращения: 21.03.2025).

7. Бокова Л. Н. Правовой режим создания безопасной цифровой образовательной среды / Л. Н. Бокова // Вестник РУДН. – Серия: Юридические науки. – 2020. – №2. – URL:

https://cyberleninka.ru/article/n/pravovoy-rezhim-sozdaniya-bezopasnoy-tsifrovoy-obrazovatelnoy-sredy (дата обращения: 21.03.2025).

8. Буданцев Д. В. Цифровизация в сфере образования: обзор российских научных публикаций / Д. В. Буданцев // Молодой ученый. – 2020. – № 27 (317). – С. 120–127.

9. Бурков В. Н. Основы математической теории активных систем / В. Н. Бурков. – Москва : Наука, 1977. – 255 с.

10. Вербицкий А. А. Цифровое обучение: проблемы, риски и перспективы / А. А. Вербицкий // Электронный научно-публицистический журнал "Homo Cyberus". – 2019. – №1(6). – URL: http://journal.homocyberus.ru/Verbitskiy_AA_1_2019 (дата обращения: 18.03.2025).

11. Винник Е. А. Обеспечение защиты информации в образовательных организациях / Е. А. Винник // Молодой ученый. – 2023. – № 7 (454). – С. 3–6.

12. Вострецова Е. В. Основы информационной безопасности / Е. В. Вострецова. – Екатеринбург : Изд-во Урал. ун-та, 2019. – 204 с. – ISBN 978-5-7996-2677-8.

13. Вохменцева Е. А. Проектная деятельность учащихся как средство формирования ключевых компетентностей / Е. А. Вохменцева // Актуальные задачи педагогики : материалы I Междунар. науч. конф. (г. Чита, декабрь 2011 г.). – Чита : Издательство Молодой ученый, 2011. – С. 58–65.

14. Гайдарева И. Н. Информационная составляющая национальной безопасности / И. Н. Гайдарева // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. – 2007. – № 1. – С. 386–392.

15. Гайдарева И. Н. Правовое обеспечение информационной безопасности в России / И. Н. Гайдарева // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия,

история, социология, юриспруденция, политология, культурология. – 2009. – № 1. – С. 174–180.

16. Гилстер П. Навигатор Internet : Путеводитель для человека с компьютером и модемом : [Пер. с англ.] / П. Гилстер; [Вступ. ст. В. Г. Серфа]. – Москва : АОЗТ "Джон Уайли энд санз", 1995. – 735 с. – ISBN 5-88182-025-8.

17. Гриншкун В. В. Современная цифровая образовательная среда: ресурсы, средства, сервисы / В. В. Гриншкун, Г.А. Краснов. – Москва : Издательство «Проспект», 2023. – 216 с. – ISBN 978-5-392-37868-5.

18. Гриншкун В. В. Цифровые инструменты в профессиональной подготовке педагогов / В. В. Гриншкун // Альманах Института коррекционной педагогики. – 2021. – № 43 (1). – С. 1–10.

19. Гриншкун В. В. Тенденции и особенности современного этапа информатизации высшей школы / В. В. Гриншкун, О. Ю. Заславская, М. Л. Левицкий // Вестник Российского университета дружбы народов. Серия: Информатизация образования. – 2022. – Т. 19. – №4. – С. 285–299.

20. Грохотова Е. В. Современный курс компьютерной грамотности с точки зрения нового поколения людей третьего возраста / Е. В. Грохотова, Д. А. Бархатова // Открытое образование. – 2021. – Т. 25. – № 6. – С. 4–12.

21. Губарева О. Ю. Статистический анализ уязвимостей информационной безопасности информационных систем / О. Ю. Губарева, В. В. Пугин // Проблемы техники и технологий телекоммуникаций: Сборник трудов XVI Международной научно-технической конференции – Уфа, 2015. – Т. 3. – С. 175–177.

22. Двуличанская Н. Н. Интерактивные методы обучения как средство формирования ключевых компетенций // Машиностроение и компьютерные технологии. – 2011. – №4. – URL: https://cyberleninka.ru/article/n/interaktivnye-metody-obucheniya-kak-sredstvo-formirovaniya-klyuchevyh-kompetentsiy (дата обращения: 21.05.2025).

23. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками / П. Н. Девянин. – Москва : Горячая линия – Телеком, 2011. – 320 с. – ISBN 978-5-9912-0328-9.

24. Ершова Т. Б. Управленческие решения / Т. Б. Ершова, А. С. Ершов. – Комсомольск-на-Амуре : Изд-во АмГПГУ, 2015. – 223 с. – ISBN 978-5-85094-473-5.

25. Ефремов М. Б. Обеспечение безопасности сайта компании: выпускная квалификационная работа / М. Б. Ефремов; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. – Екатеринбург, 2019. – 83 с.

26. Жиляев А. Х. Управление НСИ в информационных системах / А. Х. Жиляев // Системы управления бизнес-процессами. – 2012. – № 9. – URL: https://journal.itmane.ru/node/823 (дата обращения: 21.03.2025).

27. Захарова И. Г. Информационные технологии в образовании / И. Г. Захарова. – Москва : Акад., 2003. – 187 с.

28. Зеер Э. Ф. Профессионально-образовательное пространство личности / Э. Ф. Зеер. – Екатеринбург : Рос. гос. проф.-пед. ун-т; Нижнетагил. гос. проф. колледж им. Н. А. Демидова., 2002. – 126 с.

29. Информатизация образования: толковый словарь понятийного аппарата / Сост. И. В. Роберт, В. А. Касторнова. – Москва : Изд-во АЭО, 2023. – 182 с. – ISBN 978-5-8323-1121-0.

30. Исследования по общей теории систем: Сборник переводов / Общ. ред. и вст. ст. В. Н. Садовского и Э. Г. Юдина. – Москва : Прогресс, 1969. – С. 23–82.

31. Карачаев А. Р. Методы защиты и технология шифрования данных / А. Р. Карачаев, З. А. Шогенов, Т. К. Курбанов, Ф. Р. Пашаева // Образование и право. – 2022. – №9. – URL: https://cyberleninka.ru/article/n/metody-zaschity-i-tehnologiya-shifrovaniya-dannyh (дата обращения: 21.03.2025).

32. Касперский Е. В. Компьютерные вирусы : что это такое и как с ними бороться? / Е. В. Касперский. – Москва : СК Пресс, 1998. – 288 с.

33. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ N 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // КонсультантПлюс : [сайт]. – 2025. – URL: https://www.consultant.ru/document/cons_doc_LAW_121499/?ysclid=m9sac1u0yg464025189 (дата обращения: 21.03.2025).

34. Корчагина М. Ю. Анализ цифровой грамотности в школе / М. Ю. Корчагина // Молодой ученый. – 2023. – № 46 (493). – С. 387–390.

35. Красильникова В. А. Становление и развитие компьютерных технологий обучения / В. А. Красильникова. – Москва : ИИО РАО, 2002. – 168 с.

36. Краснов А. Е. Детектирование DDoS-атак на основе анализа динамики взаимосвязи характеристик сетевого трафика / А. Е. Краснов, Е. Н. Надеждин, Д. Н. Никольский, Д. С. Репин, В. С. Галяев // Вестник Удмуртского университета. Математика. Механика. Компьютерные науки. – 2018. – Т. 28. – № 3. – С. 407–418.

37. Логинова А. В. Ключевые вопросы и проблемы интеграции технологий в процесс обучения / А. В. Логинова. // Молодой ученый. – 2015. – № 11 (91). – С. 1405–1408.

38. Мамиконян Н. А. Цифровые платформы в государственном управлении / Н. А. Мамиконян // Молодой ученый. – 2023. – № 6 (453). – С. 107–108.

39. Манович Л. Язык новых медиа / Л. Манович ; Перевод Д. Кульчицкой. – Москва : Ад Маргинем Пресс, 2018. – 400 с. – ISBN 978-5-91103-411-5.

40. Москвитина Н. В. Цифровая трансформация государственного управления / Н. В. Москвитина // Социология. – 2021. – № 4. – С. 114–128.

41. Надеждин Е. Н. Задача распределения программных ресурсов информационно-вычислительной сети / Е. Н. Надеждин // Современные наукоемкие технологии. – 2019. – № 12. – С. 89–94.

42. О персональных данных : федеральный закон от 27.07.2006 № 152-ФЗ (в последней редакции) // Справочно-правовая система «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 21.05.2025).

43. Павлюкевич А. Ю. Внедрение цифровой образовательной среды как механизма управления развитием образовательной организации / А. Ю. Павлюкевич // Научно-методическое обеспечение оценки качества образования. – 2022. – №1 (15). – С. 61–67.

44. Петренко С. А. Концепция обеспечения киберустойчивости цифровых платформ индустрии 4.0 / С. А. Петренко, Д. Д. Ступин // XII Мультиконференция по проблемам управления (МКПУ-2019) : материалы XII мультиконференции по проблемам управления (МКПУ-2019): в 4 томах, Дивноморское, Геленджик, 23–28 сентября 2019 года. Том 3. – Дивноморское, Геленджик: Южный федеральный университет, 2019. – С. 200–205.

45. Поличка А. Е. Приемы обучения для развития информационной компетенции и поддержки информационной безопасности личности студента вуза / А. Е. Поличка, Н. П. Табачук // Информационная безопасность личности субъектов образовательного процесса в цифровой информационно-образовательной среде: сб. науч. тр. – Москва: Издательский центр РГУ нефти и газа (НИУ) имени И.М. Губкина. – 2021. – С. 332–342.

46. Роберт И. В. Развитие информатизации образования на основе цифровых технологий: интеллектуализация процесса обучения, возможные

негативные последствия // Наука о человеке: гуманитарные исследования. – 2017. – №4 (30). – URL: https://cyberleninka.ru/article/n/razvitie-informatizatsii-obrazovaniya-na-osnove-tsifrovyh-tehnologiy-intellektualizatsiya-protsessa-obucheniya-vozmozhnye (дата обращения: 21.05.2025).

47. Роберт И. В. Теоретико-методические подходы к обеспечению информационной безопасности личности в условиях цифровой трансформации образования / И. В. Роберт // Информационная безопасность личности субъектов образовательного процесса в современном обществе. – Москва : Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина, 2023. – С. 7–29.

48. Саттарова Н. И. О формировании культуры безопасности обучающихся в информационном пространстве / Н. И. Саттарова // Проблемы современного педагогического образования. – 2018. – № 58-4. – С. 242-245.

49. Сенник Ю. С. Жизненный цикл информационных систем / Ю. С. Сенник, Р. И. Гребенников // Системный анализ и прикладная информатика. – 2015. – №2. – С. 4–9.

50. Скабцов Н. Kali Linux в действии. Аудит безопасности информационных систем /Н. Скабцов. – 2-е изд. – Санкт-Петербург : Питер, 2024. – 384 с. – ISBN 978-5-4461-2154-0.

51. Солдатова Г. У. Цифровое поколение России: компетентность и безопасность / Г. У. Солдатова, Т. А. Рассказова, Е. И. Нестик. – Москва : Смысл, 2017. – 375 с. – ISBN 978-5-89357-363-3.

52. Степанова Т. Ю. Обеспечение безопасности облачных хранилищ / Т. Ю. Степанова, Л. В. Ламонина, О. Б. Смирнова // Инновационные технологии в АПК, как фактор развития науки в современных условиях : сборник всероссийской (национальной) научно-практической конференции, Омск, 29 ноября 2019 года. – Омск: Омский государственный аграрный университет имени П.А. Столыпина, 2019. – С. 613-617.

53. Сухостат В. В. Основы информационной безопасности / В. В. Сухостат, И. Н. Васильева. – Санкт-Петербург : Изд-во СПбГЭУ, 2019. – 103 с. – ISBN 978-5-7310-4634-3.

54. Теория и практика дистанционного обучения : учебник для вузов / под редакцией Е. С. Полат. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2025. – 434 с. – ISBN 978-5-534-13159-8.

55. Тимофеева Л. Л. Организация работы образовательных организаций по обеспечению информационной безопасности детей / Л. Л. Тимофеева // Лидер образования. – 2020. – Вып. 12. – С. 10–41.

56. Хамидуллин Р. Д. Трансформация процессов управления организацией на основе удаленного доступа : диссертация ... кандидата экономических наук : 5.2.6. ; 5.2.3. / Р. Д. Хамидуллин; [Место защиты: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова». – Москва, 2022. – 206 с.

57. Хоббс Р. Состояние медиаграмотности: ответ Поттеру / Р. Хоббс. – Журнал вещания и электронных медиа. – 2011. – № 55 (3). – С. 419–430.

58. Шариков А. В. Глобальное информационное онлайн-пространство в 2020 г.: динамические характеристики / А. В. Шариков // Мониторинг общественного мнения: экономические и социальные перемены. – 2021. №. 2. URL: https://www.monitoringjournal.ru/index.php/monitoring/article/view/1926 (дата обращения: 21.05.2025).

59. Шершакова Т. Л. Когнитивный анализ защищенности информационных ресурсов образовательной организации / Т. Л. Шершакова, Е. Н. Надеждин // Информация и безопасность. – 2018. – Том. 21. – Вып. 1. – С. 48–57.

60. Шинкарев А. А. Ретроспектива развития веб-технологий в создании корпоративных информационных систем / А. А. Шинкарев // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. – 2020. №4. – С. 14–21.

ПРИЛОЖЕНИЕ Политика информационной безопасности сайта ГБПОУ «ЮУрГТК»

ГБПОУ «Южно-Уральский государственный технический колледж» **Система менеджмента качества**	**Политика информационной безопасности сайта ГБПОУ «Южно-Уральский государственный технический колледж»** СМК – …

ПРИНЯТО
Советом колледжа
Протокол № _____
«___» _____ 2025 г.

УТВЕРЖДЕНО
Директор колледжа
_____ И. И. Тубер
от «___» _____ 2025 г.

ПОЛИТИКА
информационной безопасности сайта ГБПОУ «Южно-Уральский государственный технический колледж»
СМК – …

1. Общие положения

1.1 Настоящая Политика информационной безопасности сайта (далее – Политика) определяет цели, задачи, принципы и порядок обеспечения конфиденциальности, целостности и доступности информации, размещенной и обрабатываемой на официальном сайте ГБПОУ «ЮУрГТК» (далее – Сайт).

1.2 Политика является локальным нормативным актом, обязательным для исполнения всеми сотрудниками и обучающимися, имеющими отношение к функционированию и использованию Сайта.

2. Нормативно-правовая база

2.1 Политика разработана в соответствии с:

– Конституцией Российской Федерации (ст. 23, ст. 24);

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Методическими рекомендациями Минцифры России по защите веб-ресурсов образовательных организаций;

– Уставом ГБПОУ «ЮУрГТК» и другими локальными актами колледжа.

3. Ключевые понятия и термины

3.1 В целях реализации настоящей Политики применяются следующие основные понятия:

– информационная безопасность – состояние защищенности информации и инфраструктуры, при котором обеспечиваются ее конфиденциальность, целостность и доступность;

– персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

– конфиденциальность информации – обязательное для соблюдения требование не передавать информацию третьим лицам без согласия владельца;

– аутентификация – процедура проверки подлинности пользователя на основе предъявляемых им учетных данных;

– авторизация – предоставление пользователю прав доступа в соответствии с его ролью;

– SQL-инъекция – тип атаки на веб-приложения, при котором злоумышленник внедряет в запрос к базе данных произвольный SQL-код;

– инцидент информационной безопасности – любое событие, нарушающее или угрожающее нарушением конфиденциальности, целостности или доступности информации;

– аудит информационной безопасности – систематическая проверка состояния защиты информации и соблюдения установленных требований.

4. Цели и задачи Политики

4.1 Цель Политики заключается в создании и поддержании устойчивой системы информационной безопасности Сайта, которая исключает несанкционированный доступ, гарантирует законность обработки персональных данных и обеспечивает прозрачность управления цифровыми ресурсами колледжа.

4.2. Задачи включают:

1. Регламентацию процессов администрирования.

2. Организацию регулярных аудитов.

3. Внедрение процедур реагирования на инциденты.

4. Обеспечение прозрачности действий ответственных лиц и вовлечение обучающихся в практико-ориентированные проекты по безопасности.

5. Принципы реализации Политики

5.1 К принципам реализации Политики относятся:

– законность и соблюдение действующего законодательства РФ;

– комплексность мер защиты;

– разделение ролей и персональной ответственности;

– интеграция образовательного и технического аспектов.

6. Роли и ответственность

6.1 Директор колледжа утверждает Политику, издает приказы о назначении ответственных.

6.2 Системный администратор обеспечивает техническую защиту (SSL/TLS, резервное копирование, мониторинг уязвимостей).

6.3 Администратор сайта отвечает за организацию доступа и функционирование CMS.

6.4 Модераторы контента поддерживают актуальность размещаемой информации.

6.5 Юрист контролирует соответствие Политики законодательству РФ.

6.6 Студенты участвуют в проектах по оценке рисков под руководством преподавателей.

7. Технические требования к Сайту

7.1 Функционирование сайта колледжа возможно только при:

– использовании протокола HTTPS для всех ресурсов;

– наличии действующего SSL/TLS-сертификата уровня не ниже TLS 1.2;

– обязательном обновлении CMS и плагинов;

– организации журналирования действий администраторов;

– проведении резервного копирования и проверки восстановления.

8. Аудиты и контроль

8.1 Аудиты проводятся ежеквартально рабочей группой лаборатории информационных технологий с использованием инструментов анализа веб-уязвимостей.

8.2 Результаты аудитов оформляются отчетом и фиксируются в журнале аудита.

9. Реагирование на инциденты

9.1 В случае выявления инцидента (утечка данных, SQL-инъекция, дефейс, сбой сервера и т.д.) осуществляется регистрация, оценка критичности, устранение последствий и составление отчета. При необходимости уведомляется Учредитель и Роскомнадзор.

10. Образовательные мероприятия

10.1 Преподаватели информатичных дисциплин организуют проекты и практические занятия по выявлению цифровых рисков.

10.2 Студенты, обучающие по специальностям УГС 09.00.00 Информатика и вычислительная техника, участвуют в тестировании учебных веб-стендов, готовят предложения по усилению защиты, результаты включаются в отчеты аудита.

11. Заключительные положения

11.1 Политика утверждается директором колледжа и подлежит пересмотру не реже одного раза в два года либо при изменении нормативной базы.