МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ 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

«РАЗРАБОТКА ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА В УСЛОВИЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ»

Магистерская диссертация
по направлению 44.04.04 «Профессиональное обучение»,
программа магистратуры «Управление информационной безопасности в профессиональном образовании»

Выполнил:
магистрант группы ОФ-209/210-2-1
Падалец Антон Михайлович
Научный руководитель:
к.т.н., профессор кафедры
АТ,ИТиМОТД Руднев В.В.

Проверка на объем заимствований:
99 % авторского текста

Работа рекомендована к защите
« 27 » мая 2020г.
Заведующий кафедрой АТИТиМОТД
_____ В.В. Руднев

Челябинск, 2020

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ 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

Направление подготовки 44.04.04 – Профессиональное обучение

(Управление информационной безопасностью в профессиональном образовании)

З А Д А Н И Е
на выпускную квалификационную (магистерскую) работу

1. Падалец Антону Михайловичу, обучающемуся в группе ОФ-209/210-2-1 по направлению подготовки 44.04.04 «Профессиональное обучение (управление информационной безопасностью в профессиональном образовании)»

Научный руководитель квалификационной работы: к.т.н., профессор кафедры АТ,ИТиМОТД Руднев В.В.

Тема магистерской диссертации: «Разработка электронного образовательного ресурса в условиях обеспечения информационной безопасности образовательной организации» утверждена приказом и.о. ректора Южно-Уральского государственного гуманитарно-педагогического университета № 3424-с.

2. Срок сдачи магистрантом законченной работы на кафедру «1» июня 2020г.

3. Материалы для выполнения магистерской работы:

- Учебная, нормативно-правовая, научно-техническая, педагогическая, методическая литература по теме магистерской работы.
- Материалы преддипломной практики по теме магистерской работы

КАЛЕНДАРНЫЙ ПЛАН РАБОТЫ

Разделы работы (описание основных вопросов, подлежащих разработке, исследованию)	Срок выполнения
ВВЕДЕНИЕ Раскрывается актуальность исследований в рамках данной тематики, указывается степень изученности и научной разработанности, объект, предмет и гипотеза исследования, ставятся цели и задачи работы, методы исследования. Раскрывается научная новизна и практическая значимость исследования.	15 сентября 2019
ГЛАВА 1. Анализ текущего состояния электронных образовательных ресурсов, предъявляемые требования и этапы разработки. Выводы по главе 1.	04 ноября 2019
ГЛАВА 2. Управление информационной безопасностью образовательной организации: нормативно-правовые основы, управление ИБ базы исследования и меры защиты информационной безопасности. Выводы по главе 2.	14 января 2020
Разработка электронного образовательного ресурса: проектирование, сбор материалов, компоновка, тестирование.	25 января 2020
ГЛАВА 3. Разработка электронного образовательного ресурса и анализ эффективности защиты информационной безопасности конечного программного продукта. Выводы по главе 3.	01 марта 2020
ЗАКЛЮЧЕНИЕ	30 апреля 2020

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ Законы и нормативные акты, международные правовые документы, государственные стандарты, международные стандарты, монографии, научные издания, научные статьи электронные ресурсы.	30 апреля 2020
ПРИЛОЖЕНИЯ (вспомогательные материалы)	30 апреля 2020
ПРЕЗЕНТАЦИЯ (НАГЛЯДНЫЕ МАТЕРИАЛЫ) предоставляется в виде слайдов рекомендаций Microsoft Power Point, 10-12 слайдов, раскрывающих содержание выпускной квалификационной (магистерской) работы, либо схемы, таблицы, графики, диаграммы – в виде раздаточного материала	28 мая 2020
ПРЕДВАРИТЕЛЬНАЯ ЗАЩИТА	29 мая 2020
СДАЧА МАГИСТЕРСКОЙ ДИССЕРТАЦИИНА КАФЕДРУ	1 июня 2020

Дата выдачи задания « 10 » июня 2019 года

Задание выдал _____ В.В.Руднев, к.т.н., профессор
Подпись научного руководителя — Фамилия, Имя, Отчество, ученое звание и степень

Задание принял _____ А.М. Падалец
Подпись магистранта — Ф.И.О. магистранта

Заведующий кафедрой _____ В.В. Руднев, к.т.н., доцент
Подпись заведующего кафедрой — Ф.И.О., ученое звание и степень

АННОТАЦИЯ

Падалец А.М. Разработка электронного образовательного ресурса в условиях обеспечения информационной безопасности образовательной организации. - Челябинск: ЮУрГГПУ, 2020, 113 стр. машинописного текста, 16 рисунков, 8 листингов, список использованной литературы 84 наименований, приложений – 2 (2 стр. машинописного текста)

Ключевые слова: Электронные образовательные ресурсы, электронное обучение, персональные данные, диверсионный анализ, информационная безопасность.

Исследования в рамках данной тематики актуально, так как применение элементов электронного обучения становится все более распространенным явлением в образовании. В то же время, обучение должно происходить в безопасных для обучающихся условиях, а также применяемые учебные материалы должны быть достоверными и безопасными.

Магистерская выпускная квалификационная работа состоит из введения, трех глав, разделенных на параграфы, заключения, библиографического списка и приложений.

В первой главе рассматриваются текущее состояние развития электронных образовательных ресурсов, тенденции их развития, требования, которым должны соответствовать электронные образовательные ресурсы, а также этапы их разработки.

Во второй главе рассматривается нормативно-правовое регулирование в области обеспечения информационной безопасности образовательных организаций, проанализирована структура управления информационной безопасностью «Челябинского института путей сообщения» и рассмотрены основные типы атак на информационные ресурсы, которые базируются на интернет-технологиях.

Третья глава основывается на разработанном электронном образовательном ресурсе «Хранилище учебных материалов ЧИПС УРГУПС». Ресурс разрабатывался для применения в соответствующей образовательной организации. Разработка осуществлялась с учетом дидактических, эргономических, психолого-педагогических, методических, структурных и технических требований. В главе описывается разработанный ресурс, применявшиеся в процессе разработки инструменты, предпринятые меры защиты информационной безопасности и анализ эффективности этих мер. Анализ производился по диверсионному методу с учетом специфики информационных технологий. В результате анализа сделаны выводы об эффективности защиты и предложены меры по закрытию найденных уязвимостей и снижения потенциальных отрицательных последствий их эксплуатации.

В заключении диссертационной работы сделаны основные выводы по результатам исследования.

Магистрант _____ А.М. Падалец

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность:

Одной из главных целей всех педагогических наук считается изучение процесса развития человека, его закономерностей и связей внутри этой целостной структуры. Проявления развития технологической сферы отражается на все сферы жизни общества. Начиная от способов коммуникации с другими людьми и заканчивая такими сферами как здравоохранение или экономика. Во всех сферах общества появляются все новые технологические средства, так или иначе меняющие нашу жизнь. К примеру, рынок смартфонов за последние 10 лет, по приблизительным оценкам вырос в 10 раз. Также, многократно выросла и их вычислительная мощность. Большое развитие получили интернет-технологии, подавляющее большинство людей пользуются различными социальными сетями, мессенджерами и другими сервисами. Появились технологии дополненной и виртуальной реальностей, которые позволяют в некоторой степени «погрузить человека» в виртуальное пространство. Сфера образования не является исключением. Достижения технологической сферы начали повсеместно интегрироваться в образовательный процесс. Они позволяют не только разнообразить этот процесс, но и способны в значительной мере его улучшить. Цифровые технологии способны повлиять на многие аспекты образования. Посредством технологий можно повысить степень наглядности при обучении, преобразить формы, методы и технологии обучения, усовершенствовать организацию образовательного процесса таким образом, чтобы повысить эффективность образовательного процесса для обучающихся, и упростить работу преподавателя. Упрощение работы преподавателя проявляется в снижении количества времени, расходуемого на побочную работу, а также снижение сложности взаимодействия с техникой и программным обеспечением.

В связи с развитием технологий возникла потребность общества в модернизации образования из-за чего государственная политика в сфере образования также требовала изменений. В законе «Об образовании в Российской Федерации» закреплены требования использования электронных ресурсов при реализации образовательных программ, в том числе дистанционных. Согласно приказу министерства образования РФ №816 утверждается порядок применения электронного обучения и дистанционных образовательных технологий. Концепция развития образования РФ до 2020 г [6]. Она появилась в следствие необходимости формирования инновационной экономики. Среди прочего, концепция устанавливает задачи создания доступности качественного образования для людей с ограниченными возможностями здоровья. Стратегическая цель политики этой концепции состоит в повышении доступности качественного образования, которое соответствует требованиям инновационного развития экономики и современным потребностям общества.

Внедрение современных технологий, и в частности электронных информационно-образовательных ресурсов, имеет побочный эффект, состоящий в развитии у обучающихся ИКТ-компетенции. На текущий момент эта компетенция одна из важнейших. Она характеризуется способностью к работе с распространенными аппаратными и программными комплексами. Эта компетенция формирует базис для формирования других компетенций, в частности, связанных с профессиональной деятельностью.

К электронным информационно-образовательным ресурсам применяются те же требования, что и к другим электронным информационным ресурсам. Это, также, касается хранения данных субъектов образования, их взаимодействие с информационными ресурсами, документооборот и т.д. Любой программный или программно-аппаратный комплекс должен соответствовать предъявляемым требованиям, в том числе к информационной безопасности, что позволяет обеспечить безопасную и эффективную работу. Вместе с технологическим прогрессом, развиваются и

методы работы злоумышленников по обходу защиты программных продуктов. К примеру, по данным Генпрокуратуры, за первые 8 месяцев 2019 года произошло на 67% больше киберпреступлений в сравнении с аналогичным периодом прошлого года [78]. По мнению многих экспертов, это связано с приростом количества устройств, использующих интернет-технологии. Именно поэтому возникает необходимость постоянной поддержки программных продуктов с целью защиты от вредоносных действий злоумышленников.

Степень изученности и научной разработанности:

В наше время активно ведутся исследования, связанные с педагогической и технической стороной вопроса о разработке электронных образовательных ресурсов в условиях информационной безопасности в контексте образовательных организаций. Научно-технический прогресс также не стоит на месте, таким образом, сфера образования на постоянной основе имеет спрос на исследования в рамках данных тематик из-за специфики целей и задач образования, которые среди прочего включают необходимость в повышении эффективности осуществления образовательного процесса. Безопасность обучающихся – фундаментальная задача. Из нее необходимость обеспечения информационной безопасности, обусловленная информатизацией организации образовательного процесса и сферы в целом.

На постоянной основе ведутся исследования, связанные решением актуальных проблем, связанных с отдельными аспектами вопроса об электронных образовательных ресурсах. Они исследуются в рамках научно-практических конференций, результатом которых являются научные и обзорные статьи. С технической стороны это выражается в стандартов, рекомендаций, а также различных алгоритмов. Существуют ГОСТы, которые описывают терминологию и общие положения: ГОСТ Р 52653-2006, ГОСТ Р 52657-2006, ГОСТ Р 53620-2009. Другие стандарты предъявляют требования к разработке электронных образовательных ресурсов: ГОСТ Р 52657-2006,

ГОСТ Р 55751-2013. Со временем была произведена структуризация требований в рамках единых требований к электронным образовательным ресурсам на основе международных стандартов и открытых спецификаций [21, 22, 23, 24].

Инструменты для разработки на языках HTML, JavaScript, PHP имеют свои документации по работе в рамках технологии и взаимодействию между ними. В значительной части, работа ведется с использованием протокола передачи данных в виде гипертекстовых документов HTTP, который также имеет свою спецификацию, текущая версия спецификации – RFC 7540 [52].

В различных диссертационных работах рассмотрены такие аспекты темы, как особенности подготовки преподавателей к самостоятельной разработке авторских электронных образовательных ресурсов, развитие методической системы обучения для эффективного применения электронных ресурсов, а также особенности содержания ресурсов с учетом специфики конкретной предметной области.

В монографии А.И. Башмакова и В.А. Старых «Принципы и технологические основы создания открытых информационно-образовательных сред» представлены фундаментальные основы методологии создания информационно-образовательных сред открытого типа, где с прикладной точки зрения раскрыты принципы построения открытых систем [31]. В монографической работе на тему «Использование инновационных технологий в образовательном процессе» Е.Н. Рогановской, Л.Н. Порядиной и П.В. Никитина рассмотрены методы и технологии применения инновационных технологий, с целью формирования и развития творческого мышления обучающихся [35].

В учебном пособии «Инновационные технологии педагогической деятельности» Б.Р. Манделя кроме общей теоретической составляющей описан иностранный опыт применения инновационных технологий, а также рассмотрены различные подходы к образовательной деятельности [36].

В фундаментальной работе на тему «Теоретические основы педагогического проектирования личностно-ориентированных электронных образовательных ресурсов и сред» В.В. Гура рассмотрены парадигмы проектировочного этапа разработки электронных образовательных ресурсов и сред, а также предложены модели многоуровневых адаптивных личностно-ориентированных электронных образовательных ресурсов и сред [32].

На основе анализа изложенной выше литературы, можно сделать вывод о том, что тема разработки электронных образовательных ресурсов является актуальной, исследователями изучены вопросы, касающиеся педагогической составляющей, проектировочной деятельности, стандартов и непосредственно процесса разработки электронных образовательных ресурсов. В нашем исследовании мы объединим несколько сторон разработки электронных образовательных ресурсов в контексте применения в образовательных организациях СПО, а также расширении методов защиты внутреннего состояния электронных образовательных ресурсов.

Объектом исследования являются электронные образовательные ресурсы как средство достижения целей образования.

Предметом исследования является процесс разработки электронного образовательного ресурса в условиях обеспечения политики информационной безопасности в образовательной организации СПО.

Цель настоящей работы – разработка электронного образовательного ресурса для образовательной организации СПО в контексте обеспечения информационной безопасности.

Гипотеза исследования: Применение методов обеспечения информационной безопасности позволят электронному образовательному ресурсу быть устойчивым к большинству попыток злоумышленников изменить внутреннее состояние программы или получить доступ к защищенной информации.

Задачи исследования:

1. Определить педагогические аспекты применения электронных образовательных ресурсов, требования, которые к ним предъявляются и этапы разработки электронного образовательного ресурса;

2. Изучить правовое регулирования обеспечения информационной безопасности образовательных организаций

3. Изучить систему управления информационной безопасностью базы исследования.

4. Проанализировать программные меры защиты информационной безопасности.

5. Разработать электронный образовательный ресурс в соответствии с предъявляемыми требованиями, описать разработанный продукт и проанализировать степень обеспечения информационной безопасности.

Методы исследования:

Общенаучные: абстрагирование, конкретизация, анализ, синтез, сравнение;

Теоретические: анализ литературы, документов и электронных ресурсов, построение гипотез, метод аналогий;

Эмпирические: описание, измерение, тестирование, изучение и обобщение опыта.

Методологическая и теоретическая основы исследования:

1. Научно-методические работы по проблемам информатизации образования и применения ЭОР в учебном процессе: Башмаков А.И., Беляев М.И., Гриншкун В.В., Краснова Г.А.;

2. Научно-методические работы по проблемам обеспечения безопасности: Альтшуллер Г.С, Злотин Б.Л, Зусман А.А.;

3. Стандарты: ГОСТ Р 52657-2006, ГОСТ Р 52653-2006, ГОСТ Р 55751-2013, ГОСТ Р 53620-2009, ГОСТ Р ИСО 9241-1-2007;

4. Законодательные акты РФ.

Научная новизна работы состоит в применении комплекса методов защиты электронных образовательных ресурсов:

1. Авторизация с применением пароля;

2. Защита от доступа к внутреннему состоянию программы путем ввода инвалидных данных;

3. Двойная аутентификация, с целью защиты аккаунта пользователя от несанкционированного доступа;

4. Защита от межсайтовых сетевых атак типа CSRF.

Практическая значимость:

1. Разработан электронный образовательный ресурс для хранения учебных материалов, интерфейс которого адаптирован для использования на компьютерах, планшетах и смартфонах;

2. Реализована валидация вводимых данных, авторизация, двойная аутентификация, хэширование паролей, защита от межсайтовых сетевых атак типа CSRF;

3. Проведен инверсионный анализ эффективности защиты разработанного электронного образовательного ресурса.

Результаты исследования могут быть применены на всех этапах разработки подобных информационных ресурсов образовательной организации. Результаты исследования валидны для любых подлежащих защите информационных ресурсов.

База исследования:

ГБПОУ СПО «Челябинский институт путей сообщения», г. Челябинск.

Структура работы состоит из введения, трех глав, заключения и списка литературы, состоящего из 84 наименований. Работа содержит 16 рисунков и 8 листингов. Общий объем работы составляет 113 страниц.

ГЛАВА 1

1.1. Текущее состояние и тенденции развития электронных образовательных ресурсов

В соответствии с стандартной документацией (ГОСТ Р 52653-2006), под понятием электронный образовательный ресурс подразумевается ресурс, который представлен в электронно-цифровой форме и включает в себя структуру, предметное содержание и метаданные о них [21]. Согласно ЮНЕСКО, применение ЭОР представляет собой обучение посредством интернет-технологий и мультимедиа. Электронные образовательные ресурсы – это фундаментальный компонент информационной образовательной среды, а также основа для применения в процессе обучения новых форм и методов обучения, таких как электронное обучение, сетевое обучение, мобильное обучение, автономное обучение, смешанное и совместное обучение [37].

Прямое назначение электронных образовательных ресурсов заключается в решении задач образования, связанных с необходимостью:

– Увеличения доли самостоятельного обучения за счет снижения доли аудиторных часов;

– Расширения базы учебной и научной литературы;

– Обеспечения обучающихся необходимыми в процессе обучения учебно-методическими материалами;

– Экономии площадей учебного пространства;

– Автоматизации образовательных процессов (статистика, контрольно-оценочные мероприятия и т.д.);

– Расширения контингента обучающихся;

– Обеспечения большей доступности и гибкости образовательного процесса.

На практике, стоит отметить, доступность и гибкость образовательного процесса тесно взаимосвязана с удобством структуры, организации и бесперебойностью работы непосредственно информационной среды [34].

На данный момент ведутся активные исследования и разработки, основными задачами который являются достижение большей эффективности процесса образования. Их практическим результатом являются различного рода электронные образовательные ресурсы, которые в той или иной мере способствуют решению вышеописанных задач современного образования. Обобщенно, все множество электронных образовательных ресурсов можно подразделить на несколько основных классов: мультимедиа материалы, электронные документы, а также симуляторы и тренажеры. При этом существуют гибридные варианты [45].

За время существования электронных образовательных ресурсов каждый из описанных классов прошел множество преобразований, связанных со всеми этапами его создания, используемыми техническими средствами, выполняемыми функциями и общим обликом конечного результата. Это неизбежно, так как развитие любых программных средств неразрывно связано с развитием технических средств и программного обеспечения. Все эти преобразования, также, обусловлены необходимостью обеспечения максимально эффективного результата, чем в данном случае является степень эффективности применения ЭОР.

Развитие мультимедийных ЭОР связано не столько с качеством материалов продукта (качеством изображения, видео или звука), сколько с развитием интерактивности этих материалов. Интерактивность позволяет добиться лучшей активности обучающихся, их вовлеченности в занятие и, соответственно, воспринимаемости материала. Примером таких средств могут служить, к примеру, интерактивные видео, в процессе воспроизведения которых можно осуществлять обратную связь, контроль,

получать дополнительную информацию или рассмотреть визуальный предмет изучения с других ракурсов. Это достигается путем размещения на необходимых моментах видео активных зон, с которыми обучающиеся могут взаимодействовать. Кроме того, уже существуют средства взаимодействия аудитории с интерактивным видео посредством смартфонов, на которых обучающиеся может взаимодействовать с материалом как индивидуально, так и в группах. В качестве такого взаимодействия могут выступать ответы на вопросы, игры по типу викторин, создание графических материалов и т.д. Интерактивность видео также можно задать с помощью объединения видео с интерактивной доской, при помощи которой можно путем наложения нарисованного изображения на видео производить более наглядное объяснение материала. Уже даже необязательно устанавливать программное-обеспечение ЭОР, так как широко распространено размещение таких материалов в сети интернет как в комплексе с другими материалами, так и отдельно.

Работа с электронными документами как никогда актуальна, если раньше мы могли лишь читать электронную литературу и располагали скудным набором инструментов для видоизменения оформления документа, то сейчас существуют программные средства, которые представляют собой не просто учебники, а целые обучающие среды, охватывающие широкий круг необходимых для усвоения предмета материалов. К примеру, комплекс для изучения информатики, кроме самого учебника может содержать справочную информацию, включая, связанную со смежными областями науки, мультимедиа материалы, контрольные материалы и т.д. Таким образом, можно добиться более комплексного усвоения материала [46]. Также, стоить отметить развитие программного обеспечения для воспроизведения простых электронных книг. На данный момент некоторые компании выпускают программы, которые кроме воспроизведения документа прилагают широкий инструментарий для аннотирования документа, что позволяет значительно повысить эффективность работы с документами.

Примером такой программы служит PDF - XChange Viewer, она имеет такие функции как: выделение текста цветом, вставка изображений, схем, нанесение изображений поверх документа, изменение самого содержимого документа, распознание отсканированного текста и т.д.

Необходимо отметить, что для повышения эффективности использования, современные электронные образовательные ресурсы носят гибридный характер, то есть могут носить в себе функционал других классов.

Текущими тенденциямив области электронных образовательных ресурсов является введение социального компонента, это распространяется как на в общем на среду, так и на содержание образования. Социальный компонент проявляется в интерактивном взаимодействии с группой других обучающихся впроцессе решения учебной задачи. Это может быть представлено в виде дискуссии по обсуждению материала, в виде электронной лабораторной работы или проведением экспериментальных исследований. Такое возможно посредством виртуальной симуляции необходимых для работы условий. Кроме обучающихся в обучающей среде может находится также и преподаватель, в роли консультанта или стороннего наблюдателя. Социальная составляющая несет в себе также и стимулирующую роль, наличие других участников обучения стимулируют конкуренцию среди участников, что также повышает эффективность деятельности. Хотя обучение и происходит в группах, каждый из участников имеет индивидуальный прогресс всего процесса обучения, что позволяет более гибко организовать учебную деятельность.

К этому можно добавить еще одну тенденцию – распространение и развитие дистанционного обучения. Дистанционные технологии снимают географические ограничения вследствие того, что доступ к «занятию» обучающийся может получить посредством интернет-технологий. Формат дистанционного обучения можно адаптировать под независимость обучающихся от времени занятий, это возможно, к примеру, если весь материал заранее записан, а необходимая интерактивность осуществляется в

более широких временных рамках. Обучающийся просматривает видео-лекцию, выполняет практические задания, в случае возникновения затруднений ему доступен чат, где менеджеры курса готовы ответить на поставленные вопросы. Для дистанционного обучения также характерны возможности социальной интерактивности, которые описаны выше. Таким образом, обучающая среда становится платформой для совместного обучения в более широких рамках возможностей ввиду материально-технических, географических, финансовых и других ограничений.

Еще одной быстроразвивающейся тенденцией является геймификация учебного процесса. Под понятием геймификация понимают внедрение игровых приемов и закономерностей в неигровые процессы. Такая тенденция характерна не только электронному образованию, также она применима и к традиционному обучению, корпоративному взаимодействию и даже пользовательскому взаимодействию с профессиональными программами.

Основными игровыми приемами, обеспечивающими геймификацию процесса обучения, являются: сторителлинг, дробление, элементы соревнования, поощрения и общение. Сторителлинг представляет собой повествование истории, в которое обернуто смысловая нагрузка полезного материала. Под дроблением подразумевается такое структурирование материала, чтобы каждый отдельный элемент был посилен для человека, и общая структура всего материала имела тематические линии, по которым передвигается пользователь в процессе обучения. Таким образом, обучающемуся не будет казаться непосильным весь подлежащий усвоению материал. Элементы соревновательности проявляются в ограниченных условий в которых пользователю необходимо выполнить задание. Поощрения – это постоянные стимуляции пользователя за успешно законченные элементы обучения. Если система предусматривает общение внутри платформы, то это дает пользователю ощущение, что он не один, у него есть единомышленники, такие же игроки, как и он сам [60].

Активно развиваются и приемы интерактивности во взаимодействии обучающегося с ЭОР. Ярким примером этого служит интерактивное видео, их главная особенность – это нелинейность и вариативность в освоении материала.

На рис. 1.1 представлен пример реализации блока интерактивного взаимодействия. Как вы можете видеть, сначала зритель просматривает фрагмент теоретического материала, затем ему предлагается ответить на вопрос путем выбора одного из предложенных вариантов и в зависимости от сделанного выбора просмотреть комментарий лектора. В данной ситуации не дается оценка верности выбранного варианта в первую очередь потому, что на данном этапе не стоит задача контроля знаний. Основная цель интерактивного видео-взаимодействия – предоставить возможность лектору заочно обратиться к обучающимся, а обучающимся – ответить лектору и, получив его комментарий, закрепить или скорректировать полученные знания. Цель такого занятия - научить, во многом благодаря совершаемым ошибкам и их анализу.

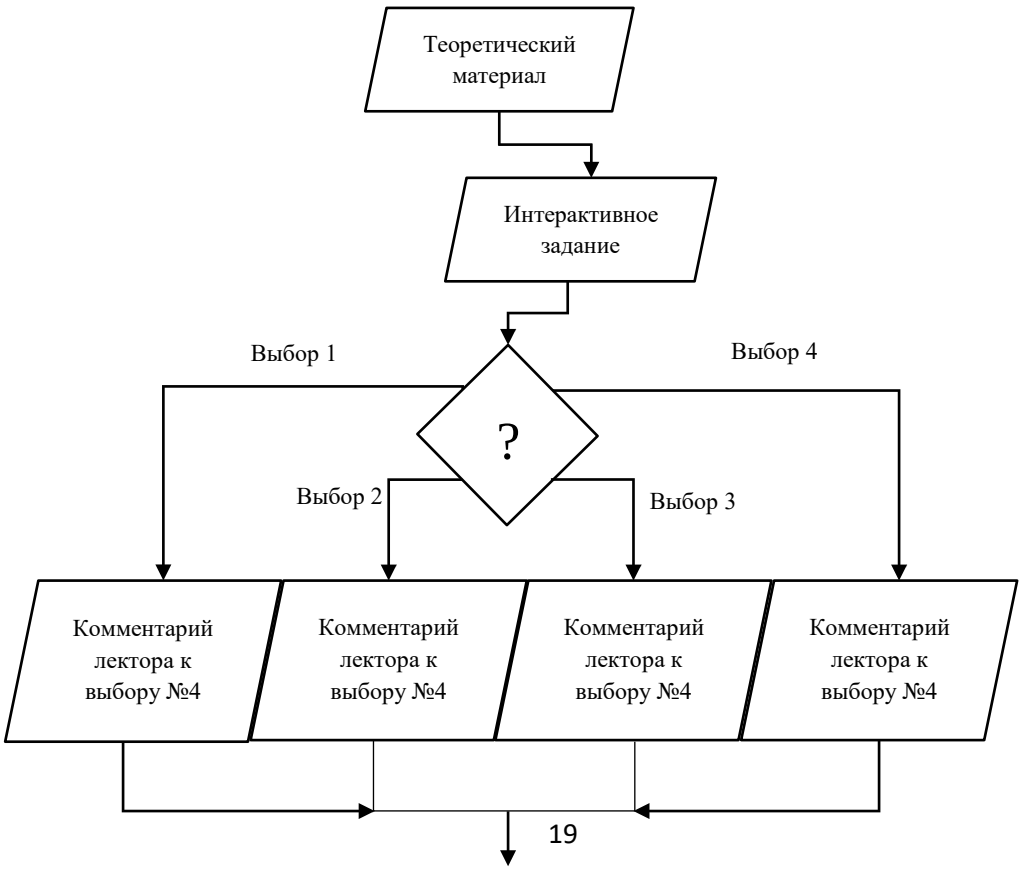

Рис. 1.1 – Пример алгоритма взаимодействия с интерактивным видео

Схожим образом реализуются виртуальные симуляции лабораторных работ. Выделяются следующие задачи, решаемые в ходе такого взаимодействия:

1. Наблюдение и практическое подтверждение ранее изученных теоретических положений;
2. Приобретение и закрепление практических навыков работы с инструментами и приборами;
3. Изучение и закрепление схемы выполнения технологических операций.

Каждая из этих задач может обеспечиваться лабораторной работой индивидуально или в разных комбинациях. Для виртуализации наиболее трудной из них оказывается вторая задача, так как зачастую для эффективной работы с инструментами и приборами необходимо разработать индивидуальную моторику мышц, а также опыт использования материалов или симулирование явлений, плохо поддающихся моделированию (например, запахи или тепловое излучение). Однако виртуализация на уровне реализации только принципов работы с инструментами и приборами вполне осуществима.

Хотя тенденции развития образования и носят технологический характер, их некорректное применение может ни только не принести положительного эффекта, но и отрицательно сказаться на качестве обучения. Поэтому необходимо понимать - как, где и при каких условиях использовать инструмент воздействия на образовательный процесс.

Ключевым фактором интеграции информационных технологий в образование является необходимость в расширении доли самостоятельной работы обучающихся, причиной чего является необходимость в

непрерывном образовании. В современных условиях изменения носят стремительный характер, что также связано с развитием многих отраслей деятельности, а также технологий и науки в целом. А выходом из ситуации как раз служит электронное обучение, в рамках которого, обучающийся может повышать степень своей квалификации без значительных ограничений во времени, месте и т.д. Таким образом, преобразования, связанные с самостоятельной работой обучающихся, является еще одной тенденцией развития образования. Туда входят не только изменения, связанные с техникой и программным обеспечением, туда нужно отнести и изменения в концепции взаимодействия преподавателя и обучающихся. Возможности, которые предоставляют информационные технологии, способствуют росту творческой составляющей в работе преподавателя. Постепенно происходит переход к преимущественно дискуссионной форме взаимодействия. Ярким примером этого служит платформа организации обучения Moodle, которая позволяет преподавателю достаточно просто сформировать курс обучения. Платформа позволяет варьировать степень самостоятельности и предоставляет контроль за успеваемостью каждого из обучающихся. Moodle предусматривает социальное взаимодействие участников внутри курса в виде чатов и форумов. Кроме того, ролевой состав субъектов обучения расширяется за счет введение ассистентов курса, задача которых - помощь преподавателю и обучающимся, а также видоизменение курса.

Одним из актуальных процессов, происходящих в обществе на данный момент, является постепенное формирование информационного общества. Одним из первых актов, регламентирующих обязанности государства и международных организаций по подготовке человека к жизни в информационном обществе является документ «Рекомендации о развитии и использовании многоязычия и всеобщем доступе к киберпространству», разработанный ЮНЕСКО [37].

Электронные образовательные ресурсы также представлены отраслевыми педагогическими библиотеками, вектор развития этой сферы

сводится к формированию единого научно-информационного потенциала, который должен соответствовать современным информационным возможностям и тенденциям, куда входит также расширение национального информационно-образовательного пространства, повышение эффективности использования научно-информационных ресурсов и активизация информационного сотрудничества [22, 39].

Высокая потребность в современной педагогической литературе, а именно содержащихся в ней данных о новых проблемах, идеях, рекомендациях, научных и методических концепциях, а также решениях прикладных задач образования, возникает из необходимости:

— Совершенствовать отбор и структурирование специализированной литературы, многовариантные способы ее представления, включая переводы с других языков;

— Оптимизации способов размещения, хранения и цифрового доступа к литературным ресурсам.

Перед создателями электронных образовательных ресурсов постоянно возникают проблемы, связанные с процессом создания, методической составляющей, учебным материалом и т.д. Для решения этих проблем создаются интегрированные системы педагогической информации, которые постоянно накапливают и обновляют информацию, отечественные и зарубежные информационные ресурсы, а также специализированные научные базы.

Таким образом, складывается необходимость и возможность создания единого информационно-образовательного пространства. ЕИОП можно определить, как совокупность информационных баз данных, хранилищ учебной и научной информации, систем управления этими хранилищами, информационно-коммуникационных систем и сетей, а также методик их разработки для обеспечения информационного взаимодействия пользователей в образовательных целях.

Кроме образовательных задач перед интегрированными информационными системами стоит вопрос информационной безопасности. В рамках государственной программы «Электронная Россия» формируется национальная стратегия «Россия в информационном веке» и разработана Доктрина информационной безопасности Российской Федерации. Согласно документу, ИБ предполагает обеспечение безопасности корпоративных серверных платформ, а также защиту информации в процессе ее хранения [10].

Исходя из доктрины, можно выделить несколько аспектов обеспечения информационной безопасности информационных систем:

1. Требования регулирующих органов по обеспечению информационной безопасности;
2. Подход разработчиков технологий к обеспечению информационной безопасности на протяжении всего жизненного цикла;
3. Построение комплексной системы информационной безопасности;
4. Специализированные решения обеспечения информационной безопасности.

1.2. Требования, предъявляемые к электронным образовательным ресурсам

Достижения в сфере ИКТ оказывают влияние на все сферы жизни общества, и образование не становится исключением. На данный момент можно считать электронные средства обучения неотъемлемой частью образовательного процесса ввиду положительного эффекта, который они оказывают, при умелом использовании, на качество образования. Существует множество примеров применения ИКТ в образовании, от проекторов или интерактивных досок, до интерактивных систем дистанционного обучения с применением игровых механик.

Общегосударственная тенденция, направленная на применение информационно-коммуникационных технологий обусловлена не только технологическим прогрессом. В соответствии с законом «Об образовании в Российской Федерации», образовательным организациям необходимо использовать в своей деятельности информационные ресурсы, что требуется для эффективной организации образовательного процесса. Также эти тенденции обусловлены государственной стратегией модернизации и развития системы образования, как приоритетного направления государственной политики [14]. Исходя из вышеописанного и общемировых тенденций развития технологий, возникает необходимость стандартизировать электронные информационные ресурсы образования с целью обеспечения разработчиков данными необходимыми для создания безопасного, эффективного и доступного электронного информационного ресурса. В рамках нашего исследования не будут затронуты требования, связанные с оборудованием, так как это напрямую не относится к конечному состоянию электронного образовательного ресурса. Акцент будет направлен в сторону программной составляющей ЭОР. Среди требований к электронным образовательным ресурсам можно выделить следующие категории: психолого-педагогические, дидактические, методические, структурные и технические. Именно от этих категорий требований в большей степени зависит качество ресурса.

В первую очередь имеет смысл рассмотреть требования, напрямую влияющие на эффективность применения ЭОР в учебном процессе. Требования к структуре описаны в ГОСТ Р 53620-2009. Согласно стандарту, структура материалов, предметное содержание и метаданные ресурса должны соответствовать функциональному назначению в процессе образования. Совместно использующиеся блоки учебной информации рекомендуется хранить в соответствии со структурой исходных материалов. Это необходимо с целью многократности использования одних и тех же блоков информации в рамках разных проектов электронных образовательных

ресурсов [3]. К электронным образовательным ресурсам полностью применимы общие дидактические требования, по той причине, что содержание обучения ЭОР подвергается всем закономерностям обучения. К дидактическим относятся требования научности, проблемности, доступности, системности, наглядности, сознательности обучения, самостоятельности, последовательности, а также единства обучающих, развивающих и воспитательных функций [23, 33].

Электронные ресурсы, применяемые в образовании, во многом отличаются от традиционных средств обучения, для образования наибольший интерес имеют изменения, которые связаны с новой функциональностью и возможностями, что предоставляют ЭОР. К этим изменениям предъявляются определенные требования. Ресурс должен быть адаптивен к индивидуальным особенностям пользователя, среди которых индивидуальные психологические особенности, уровень знаний и умений. Пользователю необходимо иметь возможность осуществлять интерактивное взаимодействие с системой в целях достижения образовательных целей. Показательным примером интерактивности во взаимодействии с ЭОР может послужить обучающая игра, где для достижения результата пользователю необходимо взаимодействовать с игрой, а она в свою очередь реализует обратную связь. Таким образом, посредством цепочек взаимодействий пользователь достигает результата, качество которого зависит от принимаемых пользователем решений. В зависимости от назначения электронные образовательные ресурсы могут обладать функциональностью для тренировки и развития теоретических, алгоритмических и наглядно-образных способностей мышления. Электронный образовательный ресурс должен быть рассчитан на обеспечение полного дидактического цикла в рамках одного целостного сеанса использования.

Требования методики обучения состоят в учете специфики отдельных предметных областей, в контексте которых ресурс используется. В основе процесса обучения должна лежать взаимосвязь теоретико-образной

информации и практического опыта взаимодействия. Понятийный аппарат внутри содержания ЭОР должен быть выстроен в строгом соответствии с уровнем освоения конкретной предметной области целевыми пользователями. Для измерения эффективности применения ЭОР и закрепления материала пользователями, система должна иметь блоки контрольных заданий и итогового контроля [21].

Технические требования подразделяются на несколько категорий: требования к компонентам и интерфейсам, требования к интерактивности, требования к мультимедийности, требования к качеству мультимедиа компонентов и требования к совместимости с веб-браузерами [25].

Требования к интерфейсу и графической составляющей регламентируют визуальную составляющую и общий опыт взаимодействия пользователя с ресурсом. В стандарте ИСО 9241-10 регламентирует общие принципы ведения взаимодействия человек – информационная система. Согласно документу, общие механизмы взаимодействия пользователя с интерфейсом должны быть ясны при поверхностном ознакомлении. Другими словами, интерфейс должен быть максимально интуитивен. Навигационный интерфейс должен быть выстроен так, чтобы пользователь, посреди использования ресурса, мог понять, в каком месте структуры системы он находится. Система навигации должна быть минимально достаточной для полноценной навигации внутри системы, и при этом иметь альтернативные навигационные пути. Интерфейс должен быть прогнозируемым, т.е. элементы интерфейса должны выполнять ровно те задачи, которые от него ожидает неосведомленный пользователь. Интерфейс должен предусматривать некорректное поведение пользователя и реагировать на это, в соответствии с предусмотренными сценариями. Это необходимо в целях предупреждения программного сбоя системы. Доступность предполагает адаптивность интерфейса по отношению к интерактивным возможностям пользователя. Это касается как технических возможностей, так и ограниченных возможностей здоровья пользователя. С технической стороны

это выражается возможности взаимодействия пользователя с системой посредством нестандартного набора устройств ввода, к примеру, пользователь должен иметь возможность пользоваться ресурсом исключительно при помощи мыши или исключительно клавиатуры. На практике, устройством ввода может быть сенсорный экран, тачпад, трекбол, электронное перо или даже устройства считывающие движения глаз. В случае ограничений возможностей по здоровью, требования, в основном, определяют возможность адаптации визуальной составляющей ресурса к зрительным возможностям пользователя. Это проявляется в изменении цветов или размеров элементов страницы. Для слабовидящих предусматривается изменение интерфейса в сторону более контрастных цветовых переходов и увеличении размеров текста. Реже применяется адаптация для дальтоников. Реализация доступности контента для дальтоников проявляется в обеспечении контраста между фоном и текстом, не допускается использование смежного использования цветов, находящихся в одном цветовом спектре или оттенки одного цвета. То же относится к динамическим изменениям цвета элемента. Для полностью незрячих предусматривается возможность звукового воспроизведения контента страницы. Для пользователей со слуховыми ограничениями предусматривается вывод звуковой информации в визуальной форме, чаще всего это проявляется в субтитрах к видео или аудиозаписям [26, 43].

Система должна обучать пользователя в плане взаимодействия с интерфейсом. Наиболее часто это выражается в помощи в выполнении наиболее распространенных задач взаимодействия или объяснении задач, которые часто вызывают затруднение у пользователей. При этом необходимо предусматривать различную скорость обучения пользователей [26].

Дополнительные принципы, согласно ГОСТ Р ИСО 14915-1-2010, вводятся для мультимедийных приложений. Согласно документу элементы интерфейса, также, как и мультимедийны приложения в целом должны предоставлять пользователю информацию в таком виде, чтобы человеческий

мозг мог наиболее легко и эффективно воспринимать информацию. К этому относятся и требования к графическим составляющим пользовательского интерфейса. Контраст цветов внутри интерфейса должен позволять легко различать отдельные составляющие объекты интерфейса, как между собой, так и в сочетании с оформлением в целом. Аудио- и видеоматериалы должны иметь такое качество, чтобы контент легко воспринимался человеком. В случае с видеозаписями показателями качества, к примеру, являются качество видеоряда, качество звука, его громкость и т.д. Составные части комплексных элементов мультимедиа или интерфейса должны быть легкоразличимы. Текст должен иметь контрастность наиболее близкую к сочетанию белого и черного цветов. Шрифт должен быть удобочитаем, в случае, если текст анимирован, то скорость анимации должна быть достаточной для легкого прочтения. Рекомендуется, чтобы схожие элементы интерфейса различных крупных блоков имели однообразную стилистику и подобие в управлении. Информация, предоставляемая пользователю не должна быть избыточной, но при этом не противоречить принципу полноценности информации. Для изучения визуально сложных учебных элементов рекомендуется предоставлять возможность изучения под разными углами обзора. Хорошим примером этого может служить 3D-модель объекта, которую можно вращать на 360 градусов во всех осях [25, 26].

Система не должна предоставлять слишком большой объем информации в рамках одной области видимости, даже если эта информация представлена в одной форме представления. Если материал предоставляется по частям с определенной периодичностью, то пользователь должен располагать достаточным временем для полноценной проработки каждой части материала.

Во время восприятия материала на пользователя не должны воздействовать отвлекающие факторы, так как это отрицательно сказывается на качестве усвоения материала. В ходе эволюции человеческий мозг научился обрабатывать зрительную информацию значительно лучше

слуховой, осязательной и т.д. Человек стал способен не только на представление зрительных образов, но и на оперирование ими в процессе решения какой-либо задачи [41]. Рекомендуется, чтобы система учитывала различные возможности восприятия информации пользователями. Это достигается введением альтернативных форм представления информации, что позволяет компенсировать различия. В выборе форм представления информации следует руководствоваться принципом полноценности информации, то есть форма представления должна быть способна полноценно отразить всю необходимую информацию.

Последняя рассматриваемая категория – это требования к обеспечению безопасности информационных ресурсов. Важность этих требований состоит в необходимости защиты конфиденциальной информации, информации подпадающей под защиту авторских прав, целостности и доступности информации, а также защиты от любого несанкционированного доступа. На государственном уровне главным регламентирующим документов является закон «О персональных данных». Одним из требований закона является необходимость размещения в ресурсе раздела, содержащего политику конфиденциальности. Обработка персональных данных может осуществляться только с согласия субъектов персональных данных [2, 3].

Таким образом, разработка ЭОР регулируется широким спектром требований, содержащихся в законодательных актах, стандартах и научной литературе. Регулируются все стороны жизненного цикла ЭОР и, конечно, его содержание. Были рассмотрены такие категории как психолого-педагогические, методические, структурные, требования к интерфейсу и графической составляющей, а также требования к безопасности информационного ресурса. Все требования и принципы должны соблюдаться в целях создания безопасного, эффективного и информативного ресурса, который будет качественно выполнять поставленные перед ним задачи образования.

1.3. Этапы разработки электронных образовательных ресурсов

Процесс разработки ЭОР носит комплексный характер и подвергается влиянию множества объективных и субъективных факторов. Неизбежно производятся изменения непосредственно в процессе разработки из-за того, что невозможно предусмотреть все аспекты идеи готовящегося ресурса и возникающие в процессе создания проблемы, но все же обобщенно можно выделить два основных этапа разработки: подготовительный и компоновки.

Название первого этапа ясно отражает его суть. На этом этапе, после того как идея сформулирована, необходимо произвести сбор материалов, которые будут положены в основу содержания ресурса. Требуется изучить стандарты, для корректной обработки собранных материалов, так как они регламентируют структуру и содержание электронного ресурса. Стандарты затрагивают как содержательную, так и техническую составляющую электронного образовательного ресурса. Собранные материалы необходимо проанализировать и сделать выборку информации, которая войдет в конечный электронный ресурс, после чего на основе выборки необходимо структурировать материал и разработать сценарий работы с электронным ресурсом. Сценарий представляет собой логически выстроенную систему путей освоения пользователем материала образовательного ресурса. Далее требуется преобразовать содержание, чтобы обеспечить реализацию разработанного сценария и сформировать систему разделов. Под содержанием на данном этапе подразумевается смысловое содержание, текст, содержащий учебную информацию. И теперь, необходимо преобразовать это содержание в наиболее подходящие для усвоения формы, применяя элементы мультимедийности, такие как видео, аудио или разновидности графики графика.

Очевидно требование, связанное с соответствием содержания электронного образовательного ресурса специфике и уровню получаемого

образования, что направлено на формирование установленных образовательным стандартом компетенций.

Структура электронных образовательных ресурсов подобна структуре учебника в своем традиционном виде. Она состоит из вводной и основной частей. Основная часть подразделяется на разделы, главы и темы. В вводной части описывается необходимость содержания данного ресурса, его структура, порядок работы с ресурсом, а также для какого уровня образования и для какой аудитории предназначен ресурс. Часто рекомендуется разделять основное содержания на обязательную и вариативную части. Вариативная часть предназначена для углубленного изучения материала и необязательна к освоению. Структура ЭОР предполагает обязательное наличие глоссария, списка рекомендуемой литературы и интернет-ресурсов [77].

Для большей целостности, следует отметить, что помимо вышеописанного содержания подготовительного этапа, в него входит подбор и приобретение программного обеспечения общего назначения, к которому относятся офисные и графические программы, математические редакторы, программы для работы с анимацией, видео- и аудиоматериалами.

Второй этап – компоновки, можно охарактеризовать преобразованием результатов подготовительного этапа в электронную форму в виде целостного приложения.

В начале второго этапа необходимо осуществить разработку архитектуры будущего ресурса. Необходимо выбрать, создавать ресурс по готовым конструкторам или осуществить полный цикл разработки программного продукта. При выборе в сторону создания ресурса с помощью конструкторов, или по-другому инструментальных комплексов, то большинство задач, в рамках этапа, уже будет решено и автору не придется решать проблемы, связанные с программной архитектурой. Обобщенно, в таком случае, разработчику необходимо посредством интерфейса конструктора собрать функциональность приложения и поместить в него

учебные материалы. Можно выделить две подкатегории таких инструментальных комплексов: общего и специального назначения. К первой относится всем известный продукт Microsoft PowerPoint, который широко применяется в большинстве компаний для создания мультимедийных презентаций. Возможности этого программного обеспечения выходят далеко за рамки мультимедийной презентации, при этом, PowerPoint располагает функционалом для создания простых игр, имеет возможности для создания интерфейса взаимодействия внутри контента файла, а также имеет возможности для создания анимационных роликов, подобных мультфильмам. Кроме того, современные версии PowerPoint имеют хорошую интеграцию с другими офисными программами, такими как Excel или Word.

Инструментальные комплексы специального назначения отличаются большей специфичностью создаваемых ресурсов, но это позволяют иметь более подходящий функционал для решения конкретных задач в рамках создания образовательных ресурсов, рассчитанных на применения в образовательном процессе. Часто такие комплексы имеют встроенный функционал, позволяющий автору создавать анимации, графики, таблицы, изображения, работать с видео и аудио форматами или математическими данными. Основной особенностью инструментальных комплексов специального назначения является наличие стандартных шаблонов различных видов учебной деятельности, например, работа с учебником, контроль успеваемости, игра и т.д. Другой важной отличительной чертой является возможность автоматизации контроля использования ресурса, другими словами, система может иметь возможность собирать статистику использования образовательного ресурса, как с целью контроля успеваемости, так и для улучшения самого ресурса, путем сбора обратной связи. Применение комплексов специального назначения для создания авторского электронного образовательного ресурса не требует особых навыков и всегда располагают подробной документацией по работе с системой. Часто обучающая документация представлена как электронный

образовательный ресурс, созданный при помощи этого самого инструментального комплекса.

Примером инструментального комплекса специального назначения служит система Moodle. Она известна как виртуальная обучающая среда и представляет собой веб-приложение, которое позволяет создавать интернет-ресурсы в виде курсов для проведения дистанционного онлайн-обучения. Moodle является бесплатным решением для создания электронных ресурсов, что является ее явным достоинством. Платформа предполагает модульное построение иерархической структуры курса, что позволяет быстро и удобно сконструировать полноценный курс. Причем в качестве смысловых модулей могут выступать текстовые страницы, изображения, интернет-страницы, аудио- и видеозаписи. Также система Moodle имеет интеграцию с платформой для проведения вебинаров eTutorium, что позволяет встроить в структуру курса занятия в режиме реального времени. Система располагает модулями для создания чатов и форумов, которые необходимы для обсуждения учебных вопросов и поддержки слушателей курса. Обслуживать курс преподаватель может как в одиночку, так и с привлечением людей, что реализовано разнообразием пользовательских ролей внутри системы. Moodle имеет функционал для постоянного мониторинга за деятельностью слушателей курса и их достижениями. Встроенная система тестирования имеет широкий ряд разнообразный видов заданий: задания на выбор одного или нескольких ответов, на приведение рядов в соответствие, задания на краткий или развернутый ответ, эссе и т.д. Таким образом, платформа Moodle предоставляет широкие возможности для удобного создания курсов удовлетворяющих требованиям для реализации авторских сценариев [54].

Обобщенная схема процесса разработки электронного образовательного ресурса представлена на рис. 1.2 [75].

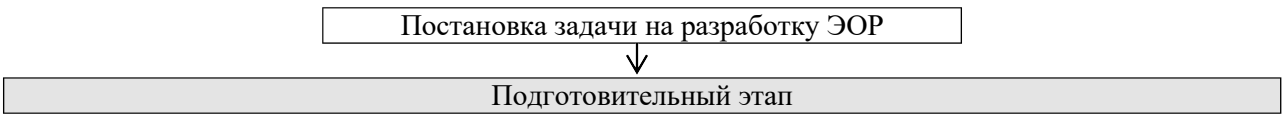

Рис. 1.2 – Процесс разработки ЭОР

Если пойти по пути осуществления полного цикла разработки, то первое, что необходимо сделать - это определить, какую функциональность должен содержать будущий ресурс. На основе этого составить иерархическую схему, из каких частей будет состоять электронный ресурс. На основе схемы необходимо произвести подбор технологий, которые требуются для реализации электронного ресурса. Под технологиями подразумеваются языки программирования, а также сопутствующие инструменты, которые необходимы в основном для решения задач автоматизации и хранения данных. Для обеспечения качества будущего ресурса, необходимо произвести изучение стандартов для технической стороны ресурса. К этому относится визуальное оформление, элементы мультимедиа, интерактивность, компоненты управления и обеспечения безопасности ресурса. Далее требуется осуществить непосредственную разработку в соответствии со всеми требованиями на основе результатов первого этапа, результатом чего будет электронный образовательный ресурс. Вариант создания электронного образовательного ресурса путем реализации полного цикла разработки позволяет реализовать практически любые идеи по использованию дидактических методик в рамках электронного ресурса. В противовес этому достоинству, нельзя не затронуть существенные недостатки такого подхода. К ним относятся значительно высокая трудоёмкость процесса разработки, необходимость привлечения профессиональных программистов и невозможность последующего изменения ресурса без их участия. Главным недостатком такого подхода

является его дороговизна, в плане покупки необходимого для разработки программного обеспечения и оплаты труда самих разработчиков.

ВЫВОДЫ К ПЕРВОЙ ГЛАВЕ

Электронные образовательные ресурсы – это основа для применения в процессе обучения новых форм и методов обучения, таких как электронное обучение, сетевое обучение, мобильное обучение, автономное обучение, смешанное и совместное обучение. Развитие мультимедийных ЭОР связано с развитием интерактивности этих материалов. Интерактивность позволяет добиться лучшей активности обучающихся, их вовлеченности в занятие и, соответственно, воспринимаемости материала. Социальный компонент современных ЭОР проявляется в интерактивном взаимодействии с группой других обучающихся в процессе решения учебной задачи. Развивается тенденция геймификации образования.

Требования к ЭОР затрагивают множество сторон разработки, проектирования и поддержки проекта. При проектировании необходимо учитывать цели и сценарии взаимодействия пользователей с ЭОР. Необходимо обеспечивать доступность ресурса к использованию пользователей с ограниченными возможностями здоровья. Важна и внешняя сторона ЭОР, необходимо обеспечить хорошую читаемость, достаточную плотность материалов на экране, удобство интерфейса и навигации, так как этого напрямую зависит эффективность применения ЭОР. Для лучшего восприятия материала, необходимо подбирать такую форму представления, которая обеспечит наиболее простое восприятие.

Процесс разработки ЭОР носит комплексный характер и подвергается влиянию множества объективных и субъективных факторов. Выделяют два основных этапа разработки ЭОР: подготовительный и компоновочный. Первый этап состоит в сборе и обработке материалов в соответствии с требованиями, а также подборе инструментов разработки, которые

понадобятся на следующем этапе. Второй этап состоит в преобразовании результатов первого этапа в программную форму.

ГЛАВА 2

Деятельность образовательных организаций характеризуется активным взаимодействием с информацией. В рамках образовательной деятельности ее субъекты на постоянной основе осуществляют различные операции с информацией. В качестве ее источников могут выступать сеть интернет, локальная сеть организации, программное обеспечение, базы данных, архивы, договоры и т.д. Часть информационной среды организации носит также и организационный характер, куда в том числе входит конфиденциальная информация. Следовательно, подобная информация нуждается в защите. Согласно законодательству, в обязательном порядке защите подлежат следующие группы информационных ресурсов:

1. Персональные данные обучающихся, работников и преподавателей, оцифрованные архивы;
2. Предметы интеллектуальной собственности;
3. Структурированная учебная информация, обеспечивающая образовательный процесс.

Информационная безопасность любых данных строится на трех основополагающих принципах: доступности, целостности и конфиденциальности информации. Под доступностью понимается гарантированное и беспрепятственное получение авторизированным

пользователем полноценного доступа к необходимой информации в требуемые сроки в соответствии с правами доступа [19, 20, 68]. Временные рамки в данном принципе носят ключевой характер. Каждый пользователь при работе с информационной системой преследует определенные цели, к примеру, желает получить необходимую ему информацию или услугу. Система должна быть способна своевременно выполнить свои функциональные задачи и предоставить результат необходимый пользователю. Если пользователь не получил результат в требуемые сроки или не получил результат вообще – имеет место нарушение доступности информации. К примеру, явным нарушением этого принципа является сбой на сервере электронной библиотеки, где хранятся все оцифрованные архивные документы, в следствие сбоя, у пользователей нет возможности получить доступ к необходимым литературным источникам. За гарантии неизменности информации без санкционированного доступа отвечает принцип целостности. Он отвечает за выявление несанкционированного создания, модификации или удаления информационных ресурсов. К примеру, злоумышленник воспользовался уязвимостью механизма авторизации электронной библиотеки и получил права сотрудника, что дало ему возможность управлять внутренним состоянием ресурсов библиотеки. Принцип конфиденциальности представляет собой гарантии доступа к информации только того круга лиц, которые авторизированы иметь к ней доступ. Этот принцип самый важный с точки зрения потенциальных последствий его нарушения. Нередки ситуации, когда в открытом доступе в сети интернет появляются базы данных компаний, которые содержат конфиденциальную информацию. Они могут содержать номера телефонов, паспортные данные, общую информацию о человеке или круге лиц, информацию составляющую коммерческую тайну или данные, на которые распространяется авторское право. К примеру, в начале 2020 года, специалисты компании IntSights обнаружили почти две с половиной тысячи скомпрометированных учетных данных пользователей сервиса

видеоконференций Zoom. Эти данные были опубликованы на хакерском форуме. Они содержали корпоративные логины и пароли, принадлежащие банкам, образовательным организациям, здравоохранительным организациям и разработчикам программного обеспечения.

В более широком смысле информационная среда опосредованно влияет на экономическую, политическую и другие сферы жизни общества. Она оказывает значительное воздействие на младшее поколение, за счет несформированности индивидуального мировоззрения и недостаточной опытности в анализе поступающей извне информации. Вследствие постепенного роста степени интеграции человека в информационное пространство, появляются неизбежные риски, которые связанны с отрицательным влиянием информационного пространства на состояние и развитие личности человека [44].

В рамках контекста образовательных организаций мы, естественно, имеем дело с информационно-образовательной средой (ИОС). Согласно ФГОС, под информационно-образовательной средой понимается совокупность условий, обеспечивающих взаимодействие пользователя с информационными ресурсами в образовательных целях. Она включает комплекс информационно-образовательных ресурсов, совокупность технических средств ИКТ, коммуникационных каналов и системы современных педагогических технологий [31]. Информационно-образовательная среда также несет в себе определенные риски для информационной безопасности образовательной организации, которые могут разнится в зависимости от конкретного звена всей системы. По большей части, проблемы с информационно-образовательной средой являются следствием физических факторов (например, неполадки оборудования), неумышленных действий пользователей информационной среды или программных сбоев. Более серьезные риски при пользовании ИОС появляются при связи ее с сетью интернет. Последствия от нарушения информационной безопасности связанной с сетью интернет, могут нести

самый различный характер. Без грамотного менеджмента информационного пространства образовательной организации, под риск могут попасть конфиденциальные данные. Вышеописанные риски для информационной среды обуславливают острую необходимость менеджмента качества обеспечения информационной безопасности образовательной организации, ее развитие, а также постоянный процесс перекрытия существующих уязвимостей. Эта политика затрагивает не только документальные и технические мероприятия, но и протоколы, регламентирующие взаимодействие работников и обучающихся с ИКТ.

2.1 Правовое регулирование и общие требования к системе обеспечения информационной безопасности образовательной организации.

Одной из важнейших задач управления образовательной организации – обеспечение эффективной информационной системы, частью чего является информационная безопасность. Как говорилось выше, информационная безопасность строится на принципах доступности, целостности и конфиденциальности. При отсутствии или нарушении любого из них, целостная система будет нарушена и не сможет эффективно функционировать. Чтобы гарантированно добиваться необходимого уровня надежности всей системы существуют стандартные документы, законодательные и международные акты, регламентирующие эту сферу деятельности организации.

Согласно Конституции РФ, информация и связь, а также обеспечение внутренней и внешней безопасности государства входит в ведение государства. Каждый человек имеет право на осуществление труда в безопасных условиях, что включает не только физическое, но и психическое здоровье. Это значит, что в современных условиях государству необходимо осуществлять политику, направленную на защиту информационного пространства населения. В нее входят и законодательные меры, которые

обязывают работодателей обеспечивать безопасность информационного пространства, в условиях которого работают его подчиненные, а также, на сколько это возможно ограничивать риски, связанные с косвенными угрозами безопасности, в число которых входит, к примеру, личная информация работников и самого работодателя [8].

Уголовный кодекс (УК) регулирует преступления, в том числе связанные с информационной сферой. Так, к примеру, за создание, распространение или использование программного обеспечения, либо иной компьютерной информации, которая предназначена для несанкционированного и незаконного доступа к информации или нейтрализации средств ее защиты - карается лишением свободы, либо принудительными работами и штрафом. УК регулирует нарушения в области санкционированного хранения и обработки информации, неправомерные воздействия на критическую информационную структуру РФ и т.д. Тяжесть ответственности зависит от фактических и потенциальных последствий от нарушения, а также от умысла и количества связанных с нарушением человек [9].

Федеральный закон «Об информации, информационных технологиях и о защите информации» регулирует отношения, связанные с поиском, получением, передачей, производством и распространением информации, использованием информационных технологий и обеспечением безопасности информационных ресурсов [13]. В этом контексте правовое регулирование основывается на следующих принципах:

1. Свобода обращения информации любым законным способом;

2. Ограничение доступа к информации устанавливается только федеральными законами;

3. Открытость информации о деятельности государственных органов управления всех уровней;

4. Равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5. Обеспечение безопасности РФ при обращении информационных ресурсов;

6. Достоверность информации и своевременность ее предоставления;

7. Неприкосновенность частной жизни и запрет сбора личной информации без согласия ее владельца.

8. Недопустимость законодательного установления преимуществ одних информационных технологий над другими для применения в государственных информационных системах, только если в федеральных законах не установлено требование применения определенных технологий в этих целях.

Доктрина информационной безопасности РФ от 2016 года является официальной системой взглядов, связанных с обеспечением национальной безопасности РФ в информационной сфере. Согласно доктрине, эффективное применение информационных технологий и ресурсов является важным фактором экономического развития государства и формирования информационного общества. В сферу национальных интересов государства входит [10]:

1. Обеспечение и защита конституционных прав и свобод человека в сфере взаимодействия с информационными технологиями и ресурсами, обеспечение поддержки демократических институтов, а также использование современных информационных технологий с целью сохранения духовно-нравственных, культурных и исторических ценностей всех народов проживающих на территории РФ;

2. Обеспечение и поддержание бесперебойности и корректности функционирования национальной информационной инфраструктуры;

3. Развитие информационных технологий и электронной промышленности, совершенствование деятельности организаций, связанных с разработкой средств обеспечения информационной безопасности и оказанием связанных с этим услуг;

4. Применение информационных технологий с целью обеспечения информационной национальной безопасности РФ в области культуры;

5. Осуществление мер, способствующих формированию системы международной информационной безопасности, которая будет направлена на противодействие угрозам нарушения государственной стабильности, на укрепление равноправного партнерства в сфере обеспечения международной информационной безопасности и на защиту суверенитета РФ в цифровой среде.

Федеральный закон «О персональных данных» занимает ведущее место в законодательстве в сфере взаимодействия с персональными данными. Закон основан на положениях конституции и нацелен на защиту неприкосновенности частной жизни, личную и семейную тайну. В нем закрепляются условия реализации контроля и надзора государства над деятельностью, связанной с обработкой и хранением персональных данных, унифицируются правила их сбора и обработки. Кроме того, закрепляются правовые, организационные и технические меры, обеспечивающие защиту прав человека при сборе и обработке конфиденциальной информации. Закон «О персональных данных» учитывает все принципы обработки конфиденциальной информации, принятые Европейским Союзом [12]. В качестве поддержки закона о персональных данных был принят ряд подзаконных актов, представляющих собой постановления правительства РФ [2, 3, 4, 5]:

1. Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных;

2. Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации;

3. Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О

персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами;

4. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных.

Закон «О персональных данных» закрепляет, что обработка персональных данных разрешена только с согласия владельца этих персональных данных. Для законности обработки персональных данный образовательная организация должна иметь цели, которые будут соответствовать законодательству и международным договорам РФ, а также если сама обработка персональных данных необходима исключительно для выполнения возложенных функций на оператора законодательством, договором или для обеспечения защиты интересов владельца персональных данных. Соответственно в образовательных организациях производится сбор письменных согласий владельцев персональных данных с целью их обработки и хранения. Это согласие должно соответствовать требованиям пункта 4 статьи 9 настоящего закона [3].

Среди перечня документов по защите персональных, которые необходимы образовательной организации должна присутствовать модель угроз персональным данным. Она разрабатывается на основании следующих документов, утвержденных Федеральной службой по техническому э экспортному надзору [15, 16]:

1. Базовая модель угроз безопасности персональных данных при их обработке в ИСПДн;

2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» регулирует отношения, затрагивающие защиту детей от информации, которая может нанести им какой-либо вред. В

документе определяется понятие информационной безопасности детей как состояние защищенности, когда отсутствует риск, связанный с причинением информацией вреда физическому или психическому здоровью и духовному или нравственному развитию. Определяет полномочия государственных органов субъектов РФ в обеспечении политики защиты подрастающего поколения от опасных информационных ресурсов, среди которых разработка и реализация региональных программ обеспечения информационной безопасности детей. Кроме прочего документ определяет классификацию информационной продукции в зависимости от возраста. Она включает три возрастные ступени: шесть, двенадцать и шестнадцать лет. Другими словами, чтобы пользователь мог получить доступ к ресурсу, ему необходимо достичь определенного возраста [11].

«Концепция информационной безопасности детей» появилась вследствие повышения роли СМИ и сети интернет в формировании личности подрастающего поколения. Согласно документу, правильное применение СМИ и сети интернет может оказать значительное влияние на укрепление нравственных и патриотических принципов населения, а также развитию системы культурного и гуманитарного просвещения. Выдвигаются принципы, в соответствии с которыми реализуется политика данная государства, среди которых:

1. Ответственность государства за соблюдение законных интересов детей в информационной сфере;

2. Обучение детей медиа-грамотности;

3. Воспитание у детей навыков самостоятельного и критического мышления;

4. Взаимодействие государственных ведомств при реализации стратегии обеспечения информационной безопасности детей.

В соответствии со ст. 28 п. 6 федерального закона «Об образовании в Российской федерации» образовательная организация обязуется

обеспечивать безопасные условия обучения, жизнь и здоровье обучающихся и работников образовательной организации [14].

ГОСТ-Р 50739-95 устанавливает требования к защите средств вычислительной техники (СВТ) от несанкционированного доступа. Согласно документу, защищенность характеризуется доступностью к обработке информации только уполномоченным лицам, либо запущенным ими процессам. Стандарт разделяет требования на три основные группы: требования к разграничению доступа, требования к учету побочной информации и требования к гарантиям, что означает необходимость наличия технических и программных механизмов, которые гарантируют выполнение первых двух групп требований [18].

В группе требований, которые связаны с разграничением доступа определяются показатели защищенности. Они сводятся к тому, что доступ к данным может получить только авторизованное лицо, которое имеет определенный порог доступа к данным. При этом каждая отдельная единица информационных ресурсов обладает набором параметров, которые определяют каким видам обработки информации эта информация может быть подвергнута. Каждая единица информационного ресурса обладает рангом доступа, по которому система принимает решение о доступе к информации, в зависимости от ранга пользователя. Политика безопасности информационного ресурса должна ограничивать спектр возможных операций с данными, чтобы предупредить несанкционированные операции с данными, к примеру, распространение путем копирования на отчуждаемый носитель. Система должна предусматривать механизмы разграничения доступа как для встроенных методов обработки информации, так и «скрытых», то есть с использованием собственных программных или программно-технических средств. Архитектура программы должна предусматривать изоляцию друг от друга участков памяти, отвечающих за процессы, запущенные различными пользователями программы.

Требования к учету определяют показателями защищенности, которые необходимо поддерживать информационному ресурсу, а именно регистрация и маркировка документов. Это означает, что система должна регистрировать и хранить информацию о действиях пользователей внутри самой системы, а также о попытках авторизоваться. Должна хранится информация о всех действиях, произведенных с информацией, а также о конфигурационных операциях, производимых над самой системой, подобные данные обычно называют термином «log», что в переводе с английского означает журнал.

В качестве показателей защищенности группы требований к гарантиям считают наличие надежных средств восстановления целостности системы, комплекса средств защиты, контроль над операциями, направленными на модификацию внутреннего состояния системы и содержащихся в ней информационных ресурсов. В основе системы должна лежать модель защиты, сформированная еще на этапе проектирования. Она должна задавать механизмы управления доступом и принципы его разграничения. Такая модель должна содержать:

1. Непротиворечивые правила разграничения доступа и их изменения;
2. Протоколы работы с устройствами ввода и вывода;
3. Формальную модель механизма управления доступом.

Вышеописанные требования и принципы описывают защиту информационной безопасности средств вычислительной техники, но для его приемки и сертификации необходимы документы, всесторонне описывающие это средство. Пакет документов включает в себя руководство пользователя, руководство по комплексу средств защиты, тестовую документацию и конструкторскую (продуктную) документацию.

Таким образом можно выделить уровни обеспечения информационной безопасности в образовательных организациях:

1. Уровень законодательства;
2. Административный уровень, который заключается в деятельности реализуемой руководством образовательной организации;

3. Процедурный уровень включает конкретные меры безопасности, реализуемые непосредственно персоналом и обучающимися;

4. Программно-технический уровень представлен конкретными средствами защиты информации.

2.2 Составляющие информационной безопасности базы исследования.

Базой нашего исследования является образовательная организация среднего профессионального образования «Челябинский институт путей сообщения», институт является ответвлением от «Уральского Государственного Университета Путей Сообщения». Корпус непосредственной базы исследования располагается отдельно от основного университета, но его структура обеспечения информационной безопасности является частью основной системы университета и построена по тем же структурным принципам.

В соответствии с вышесказанным, систему информационной безопасности базы исследования можно разделить на три основных категории, а именно информационная безопасность технических средств, безопасность персональных данных и защита обучающихся от доступа к информации, которая может отрицательно сказаться на психическом и физическом здоровье.

В распоряжении корпуса имеется 454 компьютера с выходом в сеть интернет и подключенных к внутренней локальной сети института. В читальном зале оборудовано два рабочих места с компьютерами, и одно в приемной комиссии. Доступ в интернет и внутреннюю сеть осуществляется посредством кабельного и беспроводного подключения. К этим ресурсам можно получить доступ только путем однофакторной авторизации, которая является самым распространенным способом доступа в сеть. В распоряжении преподавателей и обучающихся имеется два сторонних электронных образовательных и информационных ресурса и один собственный. Каждый

из этих ЭОР разработан в соответствии с государственными требованиями и требованиями стандартов. Преподаватели и обучающиеся имеют возможность доступа к восьми различным электронным библиотечным системам (ЭБС). В настоящий момент институт реализует проект по интеграции в учебный процесс платформы Blackboard Learn в качестве системы поддержки обучения [84].

На каждый компьютер установлен антивирус Kaspersky с защитой от сетевых атак. Парк компьютеров делится на три категории, к первой относятся компьютеры, предназначенные для обучающихся, ко второй относятся компьютеры, используемые преподавателями, и к последней категории относятся компьютеры управленческого персонала. В наибольшей защите нуждаются управленческие компьютеры, так как на них обрабатываются наиболее ответственные данные, такие как персональные данные обучающихся. Повышенную защиту таких компьютеров обеспечивает сетевой экран с более строгими ограничениями и серьезными настройками защиты. Внутренняя LAN сеть построена по клиент-серверной архитектуре, где сервер выступает в качестве источника ресурсов для компьютеров-абонентов, но при этом сам не использует мощности абонентов. Такая архитектура состоит из следующих основных компонентов [47]:

1. Сервер баз данных. Управляет хранением, доступом и защитой данных, резервным копированием, мониторингом целостности и исполняет запросы с компьютеров-клиентов;

2. Клиент, посылающий запросы к серверу. Реализует пользовательский интерфейс;

3. Сеть и коммуникационное ПО. Предназначены для взаимодействия компьютера-клиента и сервера посредством сетевых протоколов.

Пример принципиальной схемы клиент-серверной архитектуры представлен на рисунке 2.1. Серверы оптимизированы для быстрой обработки сетевых запросов на разделяемые ресурсы и для управления

информационной безопасностью файлов и каталогов. Чтобы справляться с нагрузкой, сеть оперирует двумя серверами. Архитектура сети предусматривает интеграцию сети интернет, что делает систему более гибкой и при этом не требуется наличие подключения дополнительного оборудования к компьютерам-абонентам. Сервера работают на базе операционной системы FreeBSD. При этом на компьютерах-абонентах может использоваться любая совместимая операционная система. В данном случае парк компьютеров использует операционную систему Microsoft Windows 10. Сам сервер обеспечен системами безопасности от физического доступа и системой противопожарной безопасности. Система безопасности сети предусматривает управление распределением ресурсов, контроль прав доступа, защиту данных и файловой системы, а также резервное копирование данных. Контроль прав доступа обеспечивается разграничением ролей пользователей на администраторов, пользователей с повышенными правами и рядовых пользователей. Соответствующие ограничения существуют в файловой системе серверов [66, 67].

Для получения доступа к использованию компьютера, пользователю необходимо авторизоваться в системе по логину и паролю. Политика безопасности операционных систем парка компьютеров настроена таким образом, что рядовые пользователи не могут запускать исполняемые файлы. Это ограничивает пользователей в несанкционированной установке программного обеспечения на компьютеры. При этом существует список допустимого для установки программного обеспечения, в него входят некоторые браузеры и определенные офисные пакеты, распространяемые по лицензии GNU General Public License. Настройки политики безопасности компьютеров ограничивают возможности пользователей во внесении ряда настроек операционной системы. Это необходимо для поддержания работоспособности компьютеров и сетей.

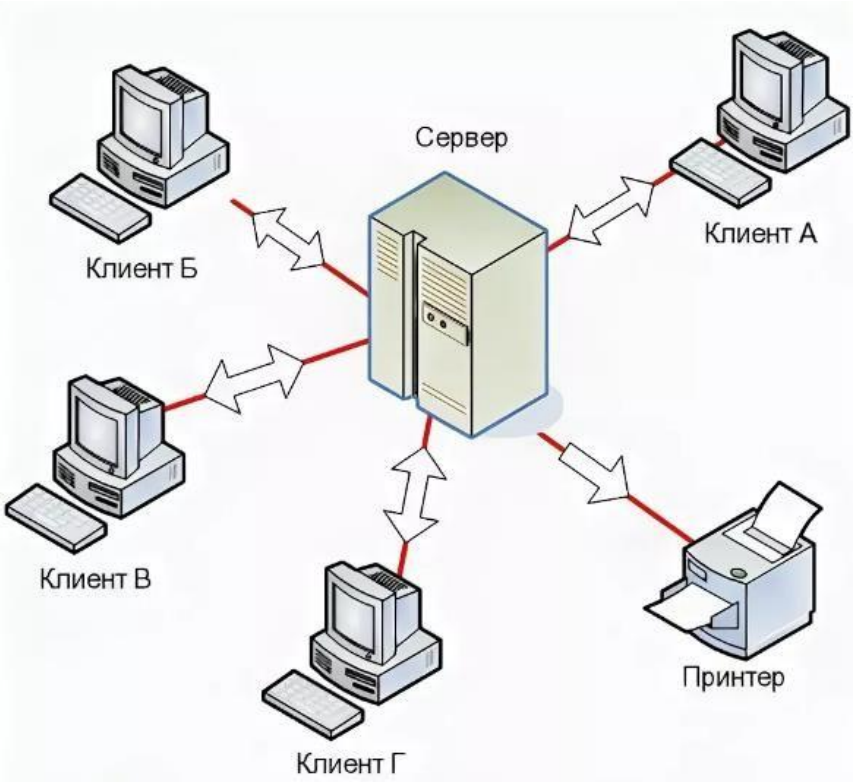

Рис. 2.1. Схема клиент-серверной архитектуры сети.

Кроме технических, требуются и организационные меры по обеспечению информационной безопасности. В институте используется перечень рекомендаций по работе с персональными данными. Кроме общих рекомендаций в состав документа входят действия при получении персональных данных, ведении личных дел, хранении носителей, содержащих персональные данные, предоставлении сведений, отнесенных к персональным данным и использовании средств вычислительной техники в обработке персональных данных. Документ о работе с персональными данными содержит информацию о сборе, обработке и хранении ПДн, информацию о передаче ПДн субъекта, о уничтожении ПДн, меры по обеспечению защиты этих данных, а также особенности организации обработки ПДн, осуществляемых без использования средств автоматизации. В институте разработан перечень обязательных документов, которые

необходимо иметь образовательной организации, весь перечень представлен в приложении 1 [74].

Сайт образовательной организации расположен на поддомене основного сайта университета. Его веб-сервер основан на базе операционной системы FreeBSD и таких технологий как Apache и PHP. Сайт прошел предварительную экспертизу в группе ТЗИ УИ и сетевой группе ОСО УИ [84].

Деятельность пользователей на сайте регламентирована пользовательским соглашением, в него входят следующие разделы:

1. Общие положения;
2. Термины. Регистрация пользователя;
3. Общие условия пользования сервисом;
4. Условия использования аналога собственной подписи;
5. Права и обязанности пользователя;
6. Права и обязанности ассоциации;
7. Персональные данные (соглашение, принципы и настройки уровня конфиденциальности);
8. Ответственность сторон;
9. Заключительные положения.

Политика в области защиты персональных данных изложена в документе «О порядке обработки и защиты персональных данных работников и лиц, обучающихся в Университете». Кроме того, используются следующие документы [74]:

1. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные;
2. Инструкция по обеспечению безопасности эксплуатации сертифицированных средств криптографической защиты информации;
3. Обязательство о неразглашении персональных данных;
4. Согласие на обработку персональных данных работника;
5. Согласие на обработку персональных данных абитуриента;

6. Согласие на обработку персональных данных для родителей.

Абсолютно необходимой стороной системы информационной безопасности образовательной организации является защита подростков от опасной информации, которая может прямо или косвенно навредить их здоровью. В институте используются рекомендации по обращению с информацией из интернет-источников. Периодически проводятся занятия, на которых обучающихся информируют на тему безопасности в интернете, и в общем на тематику интернет-грамотности. На уровне сети используется фильтр трафика, которые ограничивает доступ к ресурсам, которые находятся в базе запрещённых и определены как опасные для восприятия подростками. База постоянно обновляется, что поддерживает корректность работы фильтра. В дополнение к фильтру, действующему на уровне образовательной организации работает фильтрация трафика на уровне интернет-провайдеров. Они блокируют доступ к сайтам, которые содержатся в едином реестре запрещенный интернет-ресурсов, который формируется Роскомнадзором. Наряду с единым реестром используются база данных сайтов Министерства Юстиции РФ, реестр НСОР (не совместимые с образованием ресурсы) и база данных Министерства Образования и Науки РФ [62].

2.3 Основные меры, предпринимаемые для защиты информационной безопасности программных продуктов.

Существует множество методов и приемов произведения атак на веб-сервисы и их пользователей. С каждым днем их количество только увеличивается. Чаще всего атаки возможны благодаря изъянам в структуре самого веб-сервиса, при этом распространены атаки, которые становятся возможными благодаря промежуточным звеньям, соединяющим веб-сервис и страницу, открытую непосредственно в браузере пользователя. Пользователь, также, может являться причиной, позволившей злоумышленникам совершить

атаку. Именно поэтому, меры, необходимые для защиты информационной безопасности, не могут включать в себя только технические мероприятия. Необходимо повышать культуру поведения пользователей в сети интернет и разрабатывать правила безопасности, которыми необходимо руководствоваться при работе за служебным компьютером.

Межсайтовый скриптинг или XSS (Cross-site Scripting) – разновидность атак, связанных с внедрением кода, и представляет собой тип атаки на интернет-ресурс, при котором в получаемую пользователем страницу встраивается вредоносный код, который будет выполнен при открытии страницы в браузере пользователя. Исполнение вредоносного кода может сопровождаться установкой соединения с сервером злоумышленников. Код злоумышленников может быть встроен на страницу через эксплуатацию бреши в безопасность сервера целевого интернет-ресурса или с устройства самого пользователя, в таком случае код злоумышленников должен быть заранее помещен на устройство пользователя. Посредством XSS атак злоумышленники могут использовать систему авторизации целевого ресурса, чтобы получить доступ к ресурсу имея повышенный права пользователя или получить его данные для авторизации [70, 76].

Межсайтовый скриптинг входит в рейтинг уязвимостей веб-приложений, который составляет открытый проект обеспечения безопасности веб-приложений OWASP (Open Web Application Security Project) по состоянию на 2017 год [57]. Даже учитывая распространенность атаки, долгое время она оставалась без должного внимания. Страница или Cookie-файлы могут содержать ответственную информацию, к примеру, это может быть платежные данные или идентификатор сессии. Благодаря такой атаке может стать возможной реализация многих других атак, как пример, это могут быть DoS-атаки.

На данный момент атаки межсайтового скриптинга насчитывают три основных вида [76]:

1. Непостоянные (отраженные);

2. Постоянные (хранимые);

3. Локальные (основанные на объектной модели документа).

Атаки, производимые по непостоянному типу сценария (рис 2.2.) реализуются, когда данные, которые предоставляет браузер пользователя, обрабатываются серверным кодом, чтобы сгенерировать страницу для браузера пользователя. Если передаваемые данные некорректны и содержатся на странице с результатами без кодировки HTML, то это позволяет получить доступ к динамической странице пользователя. Таким образом зараженный код может быть обработан на сервере в результате запроса с устройства пользователя. Подобные атаки могут быть реализованы также в условиях электронной почты. В таком случае, пользователю необходимо нажать на вредоносную ссылку или отправить данные формы, тогда вредоносный код поступает на уязвимый сервер, обрабатывается и поступает обратно на устройство пользователя и обрабатывается.

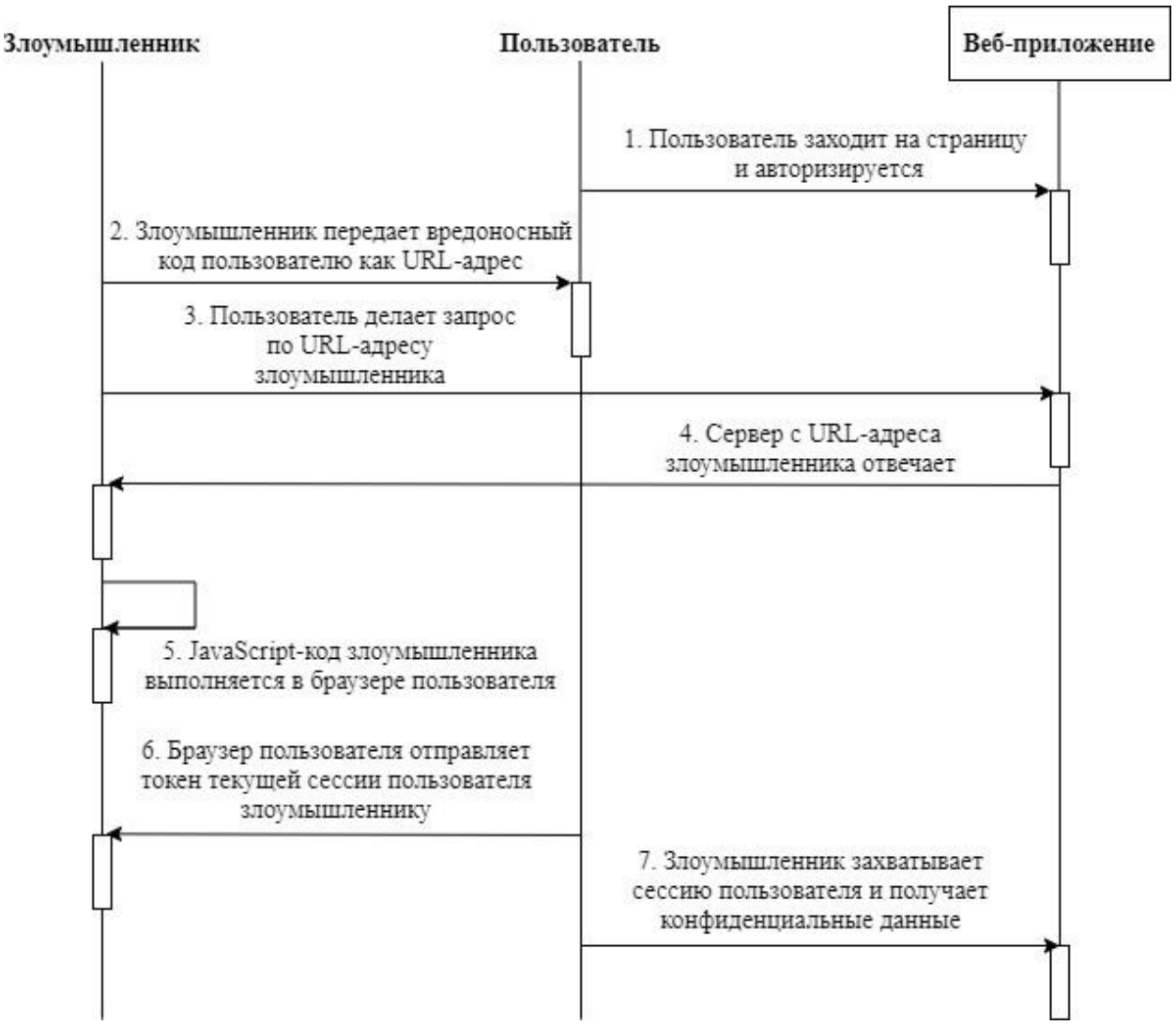

Рис 2.2. Сценарий непостоянной (отраженной) атаки межсайтового скриптинга.

Рис 2.3. Сценарий постоянной атаки межсайтового скриптинга.

Наиболее широкие возможности использования имеют атаки постоянного сценария (рис 2.3.). В рамках этого сценария, вредоносный код располагается внутри самого веб-приложения, к примеру, в базе данных. При посещении пользователем ресурса - вредоносный код отображается на устройстве пользователя без преобразования специальных HTML символов.

Атаки по сценарию локального типа (рис. 2.4.) – основаны на объектной модели документа (DOM – Document Object Model), и заключаются в подмене данных злоумышленником на стороне пользователя во время запроса страницы с сервера веб-приложения. Если JavaScript код имеет доступ к параметру URL, а также оказывает влияние на HTML код

страницы с использованием исходных данных, то есть не обработанных заменой спецсимволов на безопасные, имеет место потенциальная угроза атаки межсайтового скриптинга (XSS). Так как вносимые изменения будут заново обработаны интерпретатором браузера – атака представляется возможной.

Рис 2.4. Пример локального сценария межсайтового скриптинга.

Основная идея в защите от атак межсайтового скриптинка – не доверять данным, которые поступили от пользователя, включая Cookie-файлы.

Защита от XSS атак на стороне сервера [55]:

1. Преобразование спецсимволов, использующихся в HTML, JavaScript и URL-адресе перед внедрением и обработкой на странице. С этой целью используются htmlspecialchars (преобразует спецсимволы в HTML сущности), strip_tags (удаляет HTML и PHP теги из строки), htmlentities (преобразует символы в HTML сущности), filter_var функции, а также FILTER_SANITIZE_ENCODED (параметр filter_var, кодирует строку в формат HTML) фильтр;

2. Кодирование входных данных с помощью библиотек, к примеру, OWASP Encoding Project, Anti-XSS class, HTML Purfier, htmLawed;

3. Мониторинг кода и регулярный аудит, а также тестирование на проникновение средствами инструментов Nessus, OWASP Zed Attack Proxy и Nikto Web Scanner;

4. Обязательное указание кодировки документа на каждой странице в теге <meta> расположив его в <head>;

5. Конфигурация cookie-файлов с ограничением домена и допустимых путей, где могут использоваться конкретные cookie. Никогда не следует хранить в cookie-файлах ответственные и конфиденциальные данные;

6. Задать HTTP заголовок Content Security Policy (CSP). Он задает перечень приемлемых источников, с которых можно загружать необходимые данные (скрипты, изображения, CSS-стили, данные, JavaScript код и т.д.) и игнорировать данные из прочих источников. Чтобы использовать эту функциональность необходимо настроить сервер приложения на добавление в ответы HTTP заголовка Content-Security-Policy (иногда X-Content-Security-Policy). Также можно занести CSP как атрибут метатега: <meta http-equiv="Content-Security-Policy" …>. Конфигурация CSP формируется из специальных директив:

a. Default-src – обязательная директива, используется для ресурсов, которым не заданы отдельные правила;

b. Script-src – устанавливает доверенные источники JavaScript кода;

c. Img-src – устанавливает доверенные источники изображений;

d. Report-uri – устанавливает адрес отправки отчетов.

Защита от XSS атак на стороне клиента (пользователя):

1. Производители браузеров регулярно ведут поиски уязвимостей безопасности, закрывают их, после чего выпускают обновление. Соответственно появляется необходимость регулярно производить обновление браузера. Многие браузеры поддерживают функцию автоматического обновления в фоновом режиме и при очередном запуске браузера – обновления будут применены. Таким образом пользователям нет необходимости заботится об этом;

2. Установить расширение для браузеров, которые будут производить мониторинг полей форм, URL-адресов, скриптов JavaScript, а также запросы методом POST, на предмет подозрительных скриптов и в случае обнаружения применят фильтры для предотвращения их запуска. Как пример, существует расширение NoScript доступное на большинстве платформ.

SQL-инъекции.

SQL-инъекции – разновидность атак внедрения кода. Это один из самых распространенный приемов атак на веб-сайты, использующие в работе базы данных. Суть инъекции сводится к добавлению в данные, полученные со стороны пользователя, команд, с помощью которых взаимодействуют сервер и база данных. Таким образом, при неправильной работе с введенными пользователем данными, злоумышленник может произвести взаимодействие с базой данных [55, 59].

В зависимости от разновидности системы управления базой данных (СУБД) инъекция может дать возможность воспользоваться интерфейсом сервер – база данных, для таких операций как чтение данных таблиц,

добавление, изменение, удаление данных, чтение или запись файлов непосредственно из файловой системы, а также несанкционированное выполнение команд на уязвимом сервере.

Как упоминалось выше, такие атаки возможны благодаря некорректной обработке данных, полученных от клиента (пользователя), которые могут попасть в запрос к базе данных, поэтому специалистам по работе с базами данных необходимо владеть актуальной информацией о работе SQL-инъекций и мерами противодействия их внедрению.

Распространен подход к формированию содержимого итоговой страницы, при котором в базе данных хранятся данные, составляющие смысловое содержимое страницы. Все подобные данные структурированы внутри базы данных по таблицам, отражающим определенные сущности и их характеристики. Если сайт поддерживает авторизацию, соответственно, в базе данных должны хранится данные пользователей, которые попадают под категорию персональных данных, поэтому необходимо особо ответственно подходить к их защите.

Рассмотрим принцип SQL-инъекции на следующем примере: в стандартной ситуации сервер может использовать данные, которые пользователь передал, к примеру, через форму, как параметры для формирования тела запроса, после чего запрос отправляется в базу данных и код запроса исполняется. Результат возвращается на сервер [59].

```
1.  $id = $_POST['id'];
2.  $res = mysqli_query("SELECT * FROM archive WHERE id = " . $id);
3.
4.  SELECT * FROM archive WHERE id = 5
5.  SELECT * FROM archive WHERE id = -1 OR 1=1
```

Листинг 2.1.

В листинге 2.1. показан стандартный пример: во второй строке формируется SQL запрос данных таблицы archive с указанным идентификатором, внутри которого подставляется значение переменной из первой строки, после чего запрос отправляется. Запрос сработает как ожидается, если он будет как в строке 4, но если после подстановки значения переменной идентификатора запрос станет как в строке 5, то результатом запроса станет доступ ко всем записям таблицы archive, так как после ключевого слова WHERE идет логическое выражение, результатом которого всегда будет истина. Это и есть атака с использованием SQL-инъекции.

Внедрение кода в текстовые параметры основано на предположении, что, получив от пользователя данные, сервер сделает запрос к базе данных, в теле которого они будут содержаться.

```
1.  $search_text = $_POST['search_text'];
2.  $resources = mysqli_query("SELECT id, date, caption, text,
    id_author FROM archive WHERE caption LIKE('%$search_text%')");
3.
4.  SELECT id, date, caption, text, id_author FROM archive WHERE
    caption LIKE('%$search_text %');
5.
6.  SELECT id, date, caption, text, id_author FROM archive WHERE
    caption LIKE('%') and (id_author='1%');
7.
8.  ')+and+( id_author='1
```

Листинг 2.2.

В листинге 2.2. представлен пример использования данных, полученных от пользователя для формирования запроса к базе данных. Сначала пользовательские данные сохраняются (строка 1), после чего, используются как критерий поиска записей в базе данных (строка 2). Но если данные полученные от пользователя содержат SQL код и, при этом, они не были корректно обработаны (строка 6) – результатом может стать успешно произведенная атака. SQL-код злоумышленника может содержать

конструкцию, которая меняет поведение запроса, добавляя в него новые инструкции. Это возможно благодаря устройству синтаксиса языка запросов.

По такому же принципу работают приемы с использованием оператора UNION (листинг 2.3 строка 1), который объединяет запросы в один и возвращает общий результат, за исключением повторов, при их наличии. Представленный запрос выбирает записи только из таблицы admin с полями имен пользователя и паролей.

```
1.  SELECT id, header, body, author FROM archive WHERE id = -1 UNION
    SELECT 1,username,password,1 FROM admin
2.
3.  SELECT author FROM archive WHERE id=-1 UNION SELECT password FROM
    admin/* AND author LIKE ('a%')
4.
5.  12;INSERT INTO admin (username, password) VALUES ('fakeAdmin',
    'foo');
```

Листинг 2.3.

Случается, что после вставки параметров в запрос следует условие, уточняющее запрос. Из-за особенностей синтаксиса языка нельзя использовать прием с использованием UNION. Для преодоления этой проблемы злоумышленники применяют прием экранирования части запроса, следующей за вставкой параметра (листинг 2.3, строка 3). Таким образом, все что после параметра больше не входит в тело запроса.

Злоумышленники могут выполнять более одного запроса за раз. Для этого используется стандартный оператор синтаксиса – точка с запятой, которая разделяет запрос на части (листинг 2.3, строка 5). Эту возможность поддерживают не все вариации языка.

Предупреждение возможности SQL-инъекций включают следующие меры, предпринимаемые на сервере [63]:

1. Самый простой метод защиты – использование специфических названий полей таблиц;

2. Перед тем как поместить данные в БД, их необходимо специальным образом обработать. Все числовые данные должны быть приведены к соответствующему типу. Все остальные данные должны быть обработаны функцией mysql_real_escape_string и помещены в кавычки;

3. Нельзя выводить информацию о базе данных и о ее структуре;

4. Все варианты динамической подстановки имени базы данных, таблицы, поля или SQL оператора должны изначально содержаться в коде и не вставляться в запрос напрямую, а выбираться в зависимости от данных, полученных от пользователя;

5. Если в запрос необходимо передать хотя бы одно внешнее значение, то для его формирования и отправки необходимо использовать подготовленные выражения с подставленными переменными. Особенность подготовленных выражений состоит в том, что база данных получает запрос и необходимые для его исполнения данные отдельно. Это исключает возможность изменения инструкций при запросе. Такая возможность предоставляется библиотеками PDO и MySQLi [55];

a. Библиотека PDO поддерживает позиционные маркеры (листинг 2.4, строка 1), куда можно вставить переменную. Они обозначаются символом вопросительного знака. Также поддерживаются именованные маркеры, для которых порядок не имеет значения (листинг 2.4, строка 2). Перед выполнением необходимо подготовить запрос (листинг 2.4, строка 4). Команда возвращает пустое подготовленное выражение, куда остается внести значения переменных. Они вносятся при команде исполнения запроса – в виде параметра функции (листинг 2.4, строка 5) [73];

b. Библиотека MySQLi реализует подготовленные выражения схоже с PDO. Команда mysqli_prepare подготавливает выражение и определяет недостающие переменные (листинг 2.4, строка 7). Команда mysqli_stmt_bind_param определяет тип данных переменной и вставляет переменные в подготовленное выражение (листинг 2.4, строка 8), а

mysqli_stmt_execute окончательно выполняет запрос (листинг 2.4, строка 9) [83].

```
1.  $sql = "SELECT name FROM categories WHERE id = ?";
2.  $sql = "SELECT name FROM categories WHERE name = :name";
3.
4.  $stmt = $pdo->prepare("SELECT `name` FROM categories WHERE `id` =
    ?");
5.  $stmt->execute([$id]);
6.
7.  $stmt = mysqli_prepare($link, "SELECT item FROM categories WHERE
    name=?")
8.  mysqli_stmt_bind_param($stmt, "s", $categories);
9.  mysqli_stmt_execute($stmt);
```

Листинг 2.4.

Атаки типа Denied of Service (DOS) – отказ в обслуживании, ставят своей целью привести веб-сервис к неспособности выполнять свои функции в обслуживании обычных пользователей. Атака приводит систему к такому состоянию, посредством создания ошибок в программном обеспечении веб-сервиса, экстремальными нагрузками на сетевой канал или систему. В 2017 году Минздрав России был подвергнут распределенной атаке - Distributed Denied of Service (DDoS), в такой атаке участвует множество компьютеров злоумышленников. В самый нагруженный момент количество запросов в секунду достигло 4 миллионов. Чаще всего таким атакам подвергаются финансовые и государственные организации, а их целью становится похищение данных, либо угроза их уничтожения. Согласно статистике киберпреступлений, DDoS атакам подвергается большая часть образовательных организаций [50, 71].

Сама организация атак упростилась, теперь для злоумышленников доступны инструменты автоматической реализации атак, и при этом они не требуют глубоких знаний в этой сфере.

Основные разновидности DDoS атак:

1. Массированные атаки;
2. Атаки на протокольном уровне;
3. Атаки на уровне приложений.

Массированная DDoS атака заключается в отправке большого количества запросов к серверу, таким образом доступный канал заполняется «мусорными» запросами и правомерным пользователям нет возможности воспользоваться сервисом.

Атаки на протокольном уровне производятся путем отправки открытых запросов, в результате чего происходит истощение ресурсов системы и, соответственно, невозможность обработки запросов обычных пользователей. Этот подвид атак на протокольном уровне состоит в отправке множества фрагментированных пакетов, с которыми не в состоянии справиться система.

Domain Name System (DNS) часто становится целью DDoS-атак. DNS оказывает влияние на доступность и производительность ресурса. DNS представляет собой распределенную базу данных, в роботу которой входит приведение в соответствие IP- и URL-адресов. Другими словами, когда пользователь переходит на страницу по URL-адресу, DNS заменяет его на IP-адрес. До половины времени загрузки сайта составляет отправка запроса на DNS сервер и его внутреннюю обработку. Таким образом DNS становится привлекательной добычей для злоумышленников.

DNS подвергается различным видам DDoS-атак. Они могут быть направлены непосредственно на DNS-сервер, или могут использовать лазейки DNS, чтобы произвести атаку на другие элементы интернет-ресурса.

При атаке типа DNS Reflection, DNS-сервер подвергается большому количеству поддельных DNS ответов. Как видно из рисунка 2.5 – для атаки используется большое количество компьютеров-ботов, объединенных в сеть.

Каждый отдельный бот отправляет некоторое количество запросов, но все они используют один и тот же IP-адрес цели. На сервер обрушиваются сотни тысяч запросов. При этом DNS запрос обычно имеет размер меньше 50 байт, но размер ответа уже достигает 500 байт. Так достигается отрицательный эффект атаки.

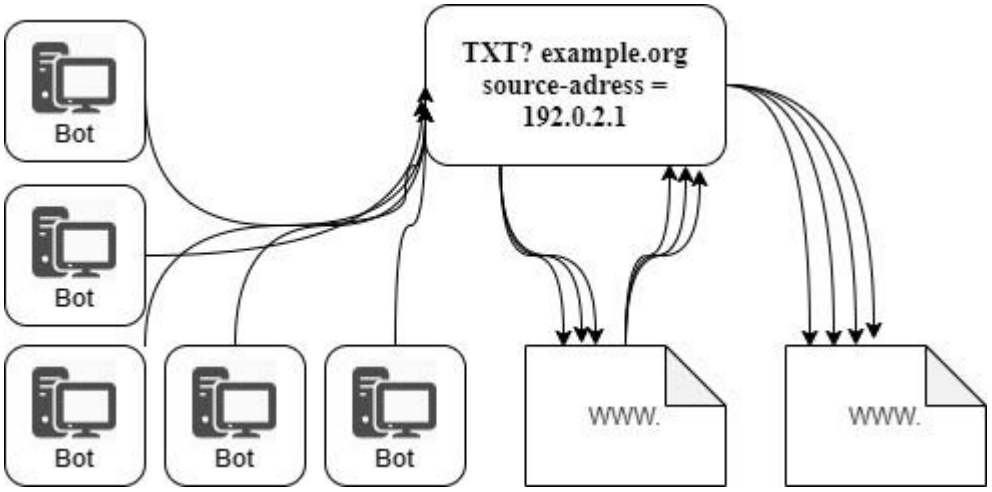

Рис 2.5. Атака типа DNS Reflection.

Имеет место необходимость реализации следующих мер по защите от DDoS-атак и их последствий:

1. На всех этапах разработки и проектирование интернет-ресурса необходимо использовать стандарты касающиеся безопасности сети, а также производить комплексное тестирование модулей. Это необходимо, чтобы закрыть другие распространенные уязвимости на уровне проекта, такие как, к примеру, SQL-инъекции или ошибки в коде;

2. Необходимо предусмотреть возможность отката системы, в случае экстренных обстоятельств и на случай некорректных обновлений;

3. Иметь план восстановления системы к прежнему состоянию. Он должен иметь средства выявления факта самой атаки, контакты для связи с провайдером, а также алгоритм перенаправления намерения решить

проблему выше по иерархии управления системой, при невозможности ее решения на данном уровне;

4. Применения сканеров, которые способны выявить уязвимости системы в целом, и конкретно связанные с возможностью DDoS-атаки. Существует множество различных тестов: OWASP Top 10 – наиболее распространенные уязвимости, системы производящие DDoS-атаки – стресс тесты и слабые места системы, тесты на проникновение. Подобные средства тестирования существует для большинства разновидностей уязвимостей;

5. Иметь в распоряжении возможность изменить схему маршрутизации всего трафика в случае атаки, либо других экстренных обстоятельств;

6. Использовать сеть доставки контента (CDN), что позволяет осуществлять доставку содержимого сайта посредством распределенной сети. Таким образом трафик распределяется, результатом чего становится уменьшение нагрузки на каналы передачи информации;

7. Использовать файрвол (WAF), который будет осуществлять мониторинг трафика между интернет-ресурсом и браузером пользователя для выявления нелегитимных запросов.

Для ослабления последствий DDoS-атак целесообразно предпринять следующие меры:

1. Необходимо производить мониторинг DNS сервера на произведение статистически нестандартного поведения. При этом необходимо постоянно обновлять статистические данные;

2. Ресурсы DNS сервера должны предусматривать возможность обработки статистически повышенных объемов трафика. Необходимо найти баланс в плане запаса, так как слишком маленький запас снижает безопасность, а слишком большой экономически нерационален;

3. Применение DNS Response Rate Limiting позволит снизить вероятность атаки типа DNS Reflection за счет снижения скорости реакции сервера на повторные запросы;

4. Использование резервного сервера позволит снизить вероятность полного отказа, так как в случае отказа одного сервера – нагрузка переключается на резервный;

5. Использование географически распределенной сети – Anycast или Unicast:

а. В Unicast схеме (рис. 2.6.) маршрутизации каждый узел сети (unicast – одноадресная сеть) получает собственный IP-адрес. При вводе пользователем URL-адреса, для исполнения выбирается случайный из доступных адресов. При использовании CDN одноадресной сети трафик будет направляться к конкретному узлу;

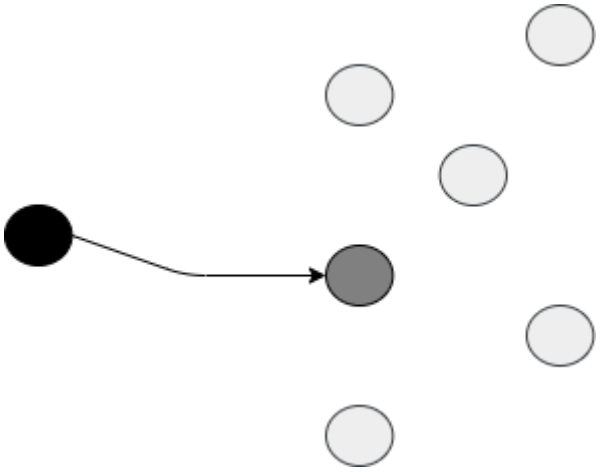

Рис 2.6. Схема маршрутизации Unicast.

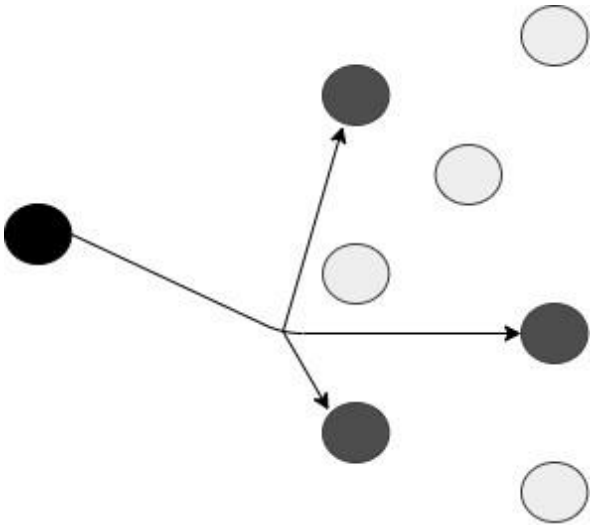

Рис 2.7. Схема маршрутизации Anycast.

b. Маршрутизация по схеме Anycast (рис. 2.7.) направляет запросы на подключение между несколькими узлами обработки. Процесс выбора оптимизируется географически, с целью достижения минимальных временный издержек. При поступлении запросов на один IP-адрес – сеть распределяет их в соответствии с приоритетами. Из-за особенностей топологии сети или ее конфигурации, ближайший узел не обязательно будет ближайшим географически. Схема Anycast предотвращает прерывание обслуживания пользователей, запрашивающих информацию с первоначального сервера. Если емкость сети превышает трафик атаки – воздействие атаки значительно снижается.

ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ

Образовательная организация характеризуется активной информационной средой. Информационная безопасность любых данных строится на трех основополагающих принципах: доступности, целостности и конфиденциальности информации. Отношения в области обращения с информацией регулируются широким спектром документов, начиная с Конституции РФ и заканчивая приказами ФСТЭК и государственными стандартами. Правовое регулирование строится на принципах свободы и достоверности информации, равноправии всех языков и защиты личной информации.

Основная идея в защите от атак межсайтового скриптинга – не доверять данным, которые поступили от пользователя. Для защиты ресурса от XSS атак предпринимаются меры по обработке данных полученных со стороны пользователя, мониторинг и совершенствование кода самого ресурса, а также фильтрация источников данных на уровне HTTP протокола.

SQL-инъекции – разновидность атак внедрения кода. Такие атаки возможны благодаря некорректной обработке данных, полученный от клиента (пользователя), которые могут попасть в запрос к базе данных. Для защиты от SQL-инъекций предпринимаются меры по формированию БД, операциям ввода и вывода данных из базы таким образом, чтобы невозможно было преобразовать назначение запроса.

Атаки типа Denied of Service (DOS) – отказ в обслуживании, ставят своей целью привести веб-сервис к неспособности выполнять свои функции в обслуживании обычных пользователей. Для защиты от DoS-атак и их разновидностей предпринимаются меры по фильтрации входящих запросов, адаптивному изменению их маршрутизации, а также смягчению последствий от подобных атак.

ГЛАВА 3

3.1. Описание разработанного программного продукта

Разработанное нами продукт называется хранилище учебных материалов ЧИПС УРГУПС. Как отражено в названии, продукт разрабатывался для использования в рамках образовательной организации ЧИПС УРГУПС. Оно представляет собой веб-приложение (сайт) и запускается в браузере при переходе по соответствующему URL-адресу. Наше приложение подпадает под категорию электронных образовательных ресурсов, так как оно предназначено для хранения электронных материалов, которые могут понадобится для обеспечения учебного процесса. В качестве материалов могут выступать различные носители учебной информации, такие как схемы, таблицы, электронные учебники, пособия, видеозаписи, презентации, текстовые документы, анимации, необходимое программное обеспечение и т.д. Приложение предназначено для использования как обучающимися, так и преподавателями, и может использоваться в любое время, независимо от местоположения пользователя и текущего времени. К примеру, преподаватель объясняет материал по презентации, а в это время обучающиеся имеют возможность загрузить эту же презентацию на свое устройство. В качестве такого устройства могут выступать компьютеры, планшеты и смартфоны и другие устройства, имеющие доступ в интернет посредством браузера.

Структура приложения проста и состоит из нескольких страниц: авторизации, регистрации, страницы с файлами (главная) и страницы

результатов поиска. Интерфейс каждой страницы строится из трех крупных блоков (рис 3.1.):

1. Главная навигация;
2. Основное содержимое страницы;
3. «Подвал».

В главный навигационный блок входят ссылки на другие страницы и основной портал образовательной организации, поле поиска по сайту, меню авторизации и кнопка переключения страницы в режим для слабовидящих. Главная навигация и «подвал» располагаются на каждой странице сайта, что позволяет пользователям эффективно перемещаться по структуре сайта.

Блок основного содержимого страницы разнится в зависимости от страницы. Он может содержать форму авторизации, форму регистрации, хранилище файлов или результаты поиска. Хранилище файлов представляет собой раскрывающийся список, который состоит из последовательности: предмет, преподаватель, тема и затем файлы. Передвигаясь по списку, пользователи могут найти необходимые файлы и загрузить их на свое устройство. Сам процесс навигации не требует обновления страницы, до любого файла можно добраться за три нажатия клавиш.

Блок «подвала» содержит контактную информацию образовательной организации, ссылку на основной портал ЧИПС УРГУПС и ссылку на соглашение о конфиденциальности, содержащее положения о работе с персональными данными пользователей как основного портала, так и хранилища учебных материалов.

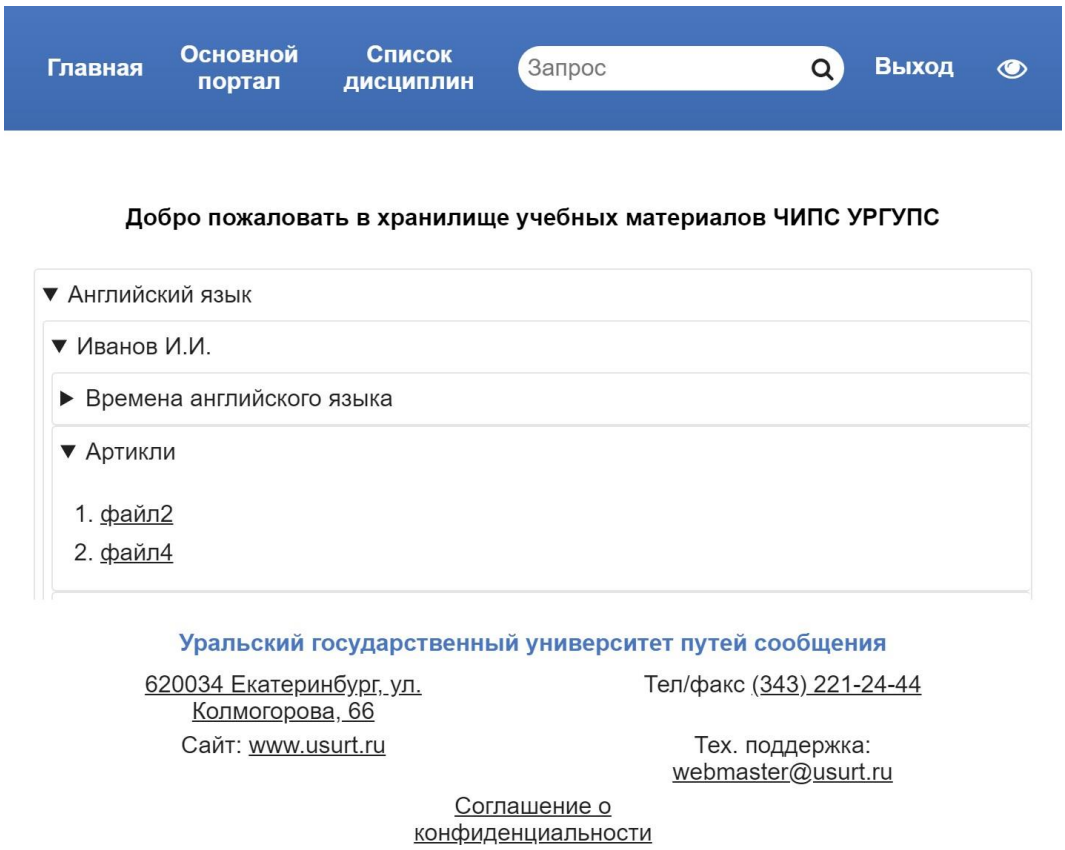

Рис 3.1. Интерфейс главной страницы.

Наш электронный образовательный ресурс поддерживает опциональный режим доступности для слабовидящих. Соответствующий переключатель находится в главном навигационной блоке сайта. При его включении шрифты и навигационные элементы становятся больших размеров и повышается их контраст за счет смены цветовой палитры сайта на наиболее контрастную - сочетание белого и черного цветов.

Сайт также поддерживает доступность интерфейса программ, которые читают текст с экрана. Это достигается использованием семантической разметки, доступной в текущем стандарте HTML, и скрытой разметки. Прием скрытой разметки заключается в добавлении в разметку невидимых на странице заголовочных тегов, которые видны лишь программам (рис 3.2.). Все это помогает программе корректно воспринимать структуру текстового содержимого страницы.

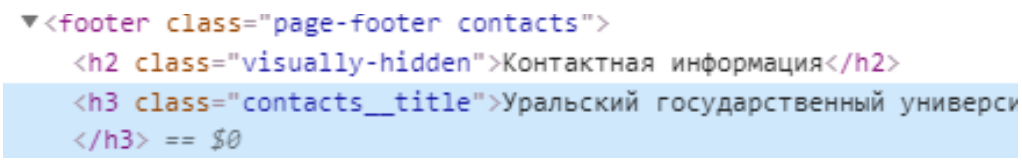

Рис 3.2. Скрытый заголовок

Наш сайт адаптирован для использования на мобильных устройствах (рис. 3.3.). Адаптация заключается в перестройке интерфейса под размеры экранов мобильных устройств. Экраны смартфонов, в отличии от экранов компьютеров, вытянуты вертикально и размеры самих экранов довольно малы. Вследствие этого, появляется неудобство в использовании сайтов для компьютеров из-за горизонтальных интерфейсов. Для мобильных устройств более удобны в использовании вертикальные интерфейсы. Процесс адаптации сайта состоит в преобразовании компьютерного интерфейса в вертикальный мобильный, а также его упрощении и увеличении размеров интерактивных элементов (рис 3.4).

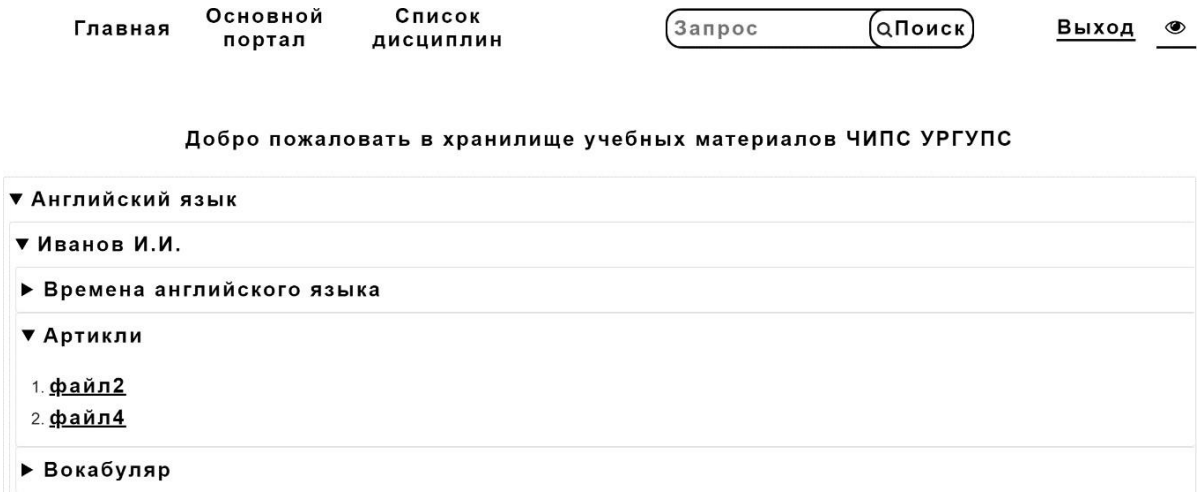

Рис 3.3. Режим доступности для слабовидящих.

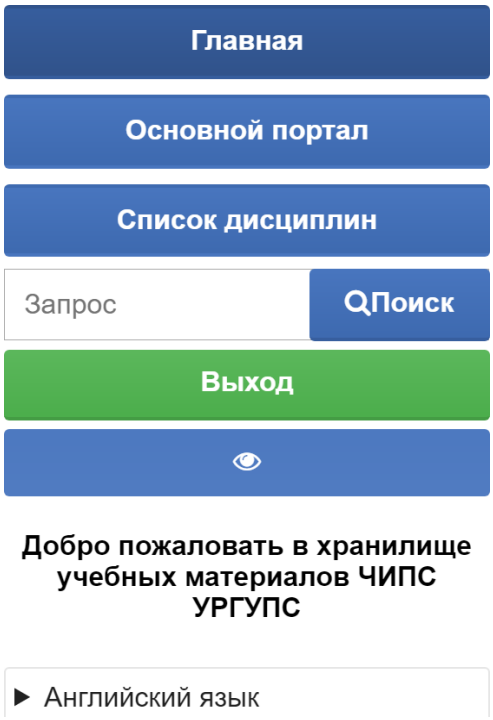

Рис 3.4. Мобильная версия сайта.

Приложение построено при помощи следующих основных технологий: HTML, БЭМ, CSS, SCSS, Gulp, NPM, PHP, Google Authenticator, MySQL.

В процессе разработки использовалось следующее программное обеспечение:

Microsoft Visual Studio Code, XAMPP, PHP, MySQL, phpMyAdmin, Google Chrome, Mozilla Firefox, NodeJS, Adobe Photoshop.

Вторая часть (компоновка) процесса разработки состояла из следующих этапов (тестирование после каждого этапа):

1. Проектирование структуры приложения;

2. Написание HTML разметки основной навигации и «подвала», после чего написание основного содержания каждой отдельной страницы.

3. Написание CSS стилей;

4. Преобразование HTML документов в PHP для шаблонизации и настройки взаимодействия с сервером;

5. Написание PHP сценариев взаимодействия клиент-сервер;

6. Проектирование и создание базы данных, наполнение базы данных;

7. Написание PHP сценариев взаимодействия клиент-сервер-база данных;

8. Обеспечение защиты от CSRF, написание авторизации и двухфакторной аутентификации;

Расстановка этапов выстроена в соответствии с логикой масштабирования функциональности.

База данных приложения построена на базе MySQL под управлением phpMyAdmin. База данных состоит из пяти таблиц: users (пользователи), classes (предметы), tutors (преподаватели), topics (темы) и files (файлы). Схема таблицы представлена на рисунке 3.5. Все таблицы кроме users имеют связи, реализуемые посредством идентификаторов. Таким образом записи в этих таблицах получают принадлежность к соответствующим записям из других таблиц. Например, каждый файл имеет принадлежность к определенной теме, преподавателю и предмету, на это указывают такие поля как topic_id, tutor_id и class_id. Каждое поле таблиц имеет определенный тип допустимых для записи в него данных. Таким образом, обеспечивается экономия пространства базы данных, скорость ее работы и защита от записи несоответствующих данных. Таблица users (пользователи) содержит информацию о пользователях. Она необходима для проведения процедур авторизации и персонализации функциональности и содержимого сайта.

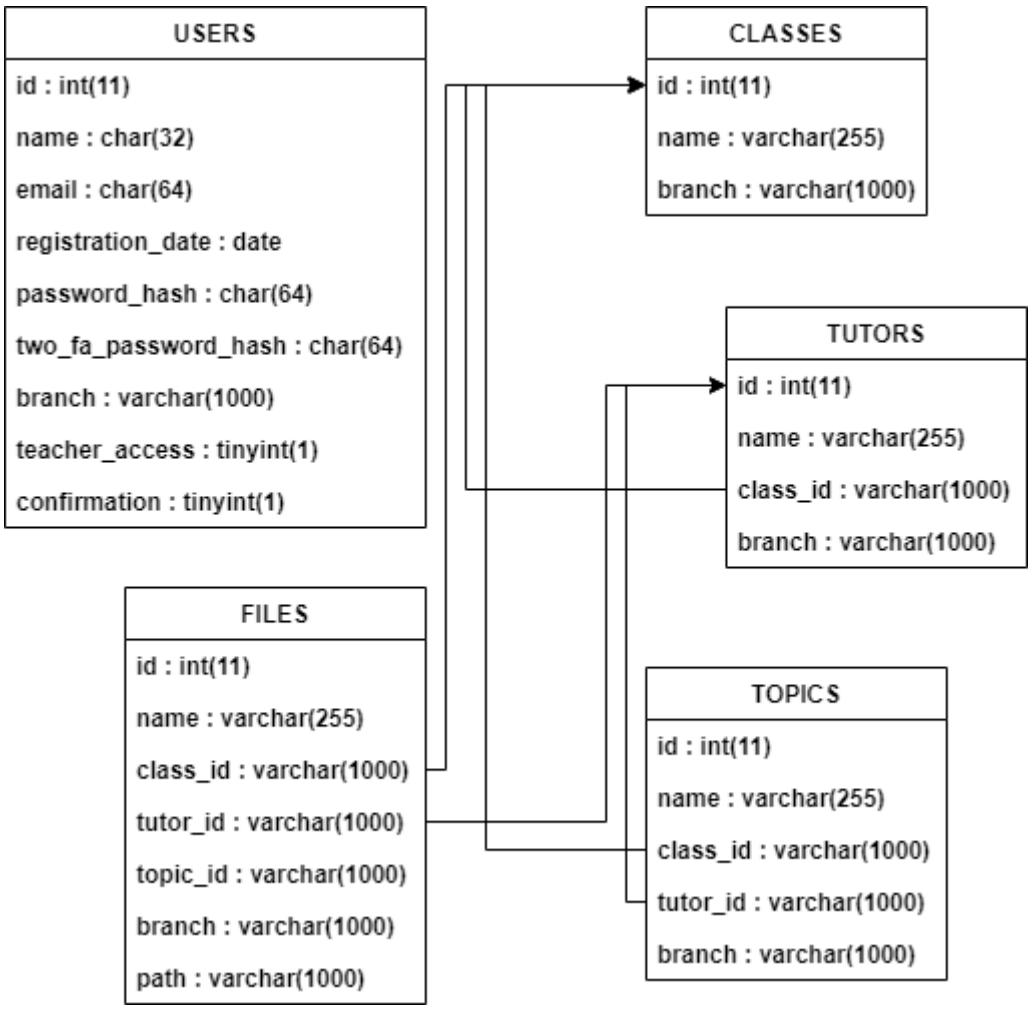

Рис 3.5. Схема базы данных

3.2. Примененные в электронном образовательном ресурсе меры защиты информационной безопасности.

Важной частью процесса разработки любого программного продукта является обеспечение его защиты. На сегодняшний день абсолютно необходимо принимать меры по их защите, так как вместе с развитием приемов злоумышленников - растет тяжесть последствий и масштаб посягательств злоумышленников на информационную безопасность. В базе данных нашего веб-приложении хранятся персональные данные, которые используются для системы авторизации на сайте и персонализации хранящихся в базе учебных материалов в соответствии с направлением

обучения. Персональные данные, согласно законодательству, подлежат обязательной защите от несанкционированного доступа. Важность этого обуславливается потенциальными последствиями от их несанкционированного распространения. Требования и меры по обеспечению информационной безопасности регламентируются в стандартах.

На программном уровне предприняты следующие меры по защите информационной безопасности нашего электронного образовательного ресурса:

1. Валидация ввода на стороне пользователя;
2. Валидация данных полученных от пользователя на сервере;
3. Защита от SQL-инъекций;
4. Защита от межсайтовой подделки запросов;
5. Разделение ролей (иерархия пользователей);
6. Система авторизации с многоразовым паролем;
7. Двухфакторная аутентификация.

Валидация вводимых данных на стороне пользователя, или HTML валидация, представляет собой проверку вводимых пользователем данных непосредственно в браузере. Проверка проводится на предмет соответствия введенных данный указанным в теге атрибутам. Главный из них – type. Он определяет, чем должны являться вводимые данные. Самое распространенное значение этого атрибута – text (текст), но гораздо лучше установить значение атрибута в соответствии с назначением поля. К примеру, для ввода пароля, значением атрибута должно быть – password. В таком случае браузер не будет показывать вводимые символы, но заменит их на символ звездочки. Таким образом, пароль не сможет увидеть злоумышленник как находясь в помещении, так и при использовании снятия изображения с экрана. Существуют также атрибуты, ограничивающие значения полей: maxlength – для строковых полей, max/min – для числовых полей. Можно обязать пользователя заполнить поле, указав атрибут required. Таким образом, форма не отправится, пока поле не будет заполнено

корректными данными. Полный список атрибутов и их значений представлен в спецификации. Клиентскую валидацию нельзя назвать серьезной мерой по обеспечению безопасности, так как при доступе к компьютеру злоумышленник сможет обойти ее при помощи консоли разработчика. По большей части, это необходимо чтобы обезопасить пользователя от ввода некорректных данных, которые могут попасть в систему, где изменить их становится проблемой. На данном этапе наш проект не имеет множества разнообразных полей для ввода, используются поля password, email, text и required [51].

```
1. <form class="sign-in form" action="sign-in.php" method="POST"
   enctype="multipart/form-data">
2. <input class="sign-in input" name="email" type="email" id="email"
   required>
3. <input class="sign-in input" name="password" type="password"
   id="password" required>
4. <input class="sign-in input" name="code" type="password"
   id="password-2fa" required>
```

Листинг 3.1.

В PHP коде данные полученные от пользователя поступают в встроенные массивы $_POST, $_GET, $_COOKIE и $_REQUEST, который объединяет первые три. По умолчанию данные форм передаются методом GET, и попадают в массив $_GET. Можно явно указать метод передачи данных формы. В нашем случае – метод $_POST, так данные будут передаваться в теле HTTP запроса (листинг 3.1. строка 1). Этот метод рекомендуется использовать для внесения изменений во внутреннее состояние приложения. Валидация на сервере - серьезная мера по обеспечению информационной безопасности. При ее отсутствии открывается множество уязвимостей доступных для эксплуатации злоумышленниками, к примеру, SQL-инъекции. В нашем проекте при регистрации используется следующий алгоритм (отрывок):

1. Проверяем метод, по которому получены данные. Нас интересует только метод POST;

2. Проверяем, что все интересующие нас поля заполнены;

3. Убираем из данных все теги функцией strip_tags, удаляем пробелы по концам строк и заменяем специальные символы на веб-безопасные;

4. При помощи функции filter_var с параметром FILTER_VALIDATE_EMAIL проверяем корректность синтаксиса email-адреса;

5. Проверяем не занят ли указанный адрес другим пользователем;

6. Хэшируем пароль при помощи функции password_hash с параметром PASSWORD_DEFAULT;

В проекте для авторизации используются email и многоразовый пароль, введенный пользователем при регистрации. Пароль хэшируется на сервере по алгоритму bcrypt, после чего имеено хэш значение пароля заносится в базу данных. При авторизации пользователя запрашивается хэш пароля из базы данных, после чего сравнивается с введенным пользователем паролем функцией password_verify [82]. Перед сравнением нет необходимости заново хэшировать пароль, так как функция password_hash возвращает также алгоритм хэширования, стоимость (алгоритмическая сложность, 10 по умолчанию) и «соль», как составляющие хэша [81]. Таким образом, даже если произойдет утечка хэша пароля из базы данных – будет большой проблемой произвести его расшифровку. Пароль от аккаунта пользователя нигде не хранится в открытом виде. Если указанный email-адрес существует и введенный пароль совпадает с хэшем (отпечатком) пароля из базы данный, то первый этап авторизации прошел успешно.

Меры защиты от SQL-инъекций представлены в виде обработки данных, полученных со стороны пользователя, и методикой формирования запросов к базе данных, в нашем случае это подготовленные запросы библиотеки mysqli. Информация о подготовленных запросах библиотеки mysqli представлена в предыдущей главе. Подготовленные запросы

применяются во всех случаях, когда необходимо произвести изменение внутреннего состояния базы данных. В нашем случае это процедура регистрации (листинг 3.2.).

```
1.  $sign_up_query = 'INSERT INTO users(name, email, password_hash,
    branch, registration_date, two_fa_password_hash) VALUES (?, ?, ?,
    ?, ?, ?)';

2.  $request_stmt = mysqli_prepare($link, $sign_up_query);

3.  mysqli_stmt_bind_param($request_stmt, 'ssssss',
    $signup_fields_data['username'], $signup_fields_data['email'],
    $signup_fields_data['password'], $signup_fields_data['branch'],
    $current_date, $secret);

4.  $signup_status = mysqli_stmt_execute($request_stmt);
```

Листинг 3.2.

В первой строке составляется запрос с пропусками, где подразумевается наличие данных. Во второй строке запрос подготавливается для передачи в базу данных. В третьей строке сопоставляются параметры запроса с пропусками, причем эти параметры должны соответствовать типам данных, что указаны в подстроке «’ssssss’», где «s» означает строковый тип. В четвертой строке подготовленный запрос отправляется для выполнения драйвером базы данных. Таким образом, параметры и тело запроса отправляются отдельно, что исключает возможность его модификации злоумышленниками.

Подделка межсайтовых запросов (CSRF — Cross Site Request Forgery) представляет собой вид сетевых атак, при котором пользователь непреднамеренно и опосредованно выполняет неблагоприятные действия в интернет-сервисе. Поскольку злоумышленник, в данном случае, не может иметь доступа к ответу на свой запрос — подобные атаки связаны с изменением какой-либо информации [69]. Обычно подобные атаки начинаются с того, что пользователь (жертва) совершает на поддельном сайте какие-либо действия, которые предусмотрены злоумышленником.

Также, атака может быть совершена посредством электронной почты или чата с помощью ссылки. Потенциальные последствия CSRF атак разнятся в зависимости от статуса пользователя (жертвы) — от изменения личной информации, электронной почты или пароля, в случае обычного пользователя, до угрозы всему интернет-сервису, в случае если жертва администратор. CSRF-атаки работают по причине того, что запросы браузера пользователя по умолчанию включают любые данные, связанные с сайтом, такие как cookie-файлы и IP-адрес пользователя. Как следствие, сайт не в состоянии различить оригинальный запрос от специально подделанного [38].

Существует несколько основных методов защиты от CSRF-атак, их можно разделить на две основные категории: методы требующие взаимодействия с пользователем, и условно автономные.

Методы связанные с вовлечением пользователя в обеспечение защиты данных являются наиболее простыми и адаптивными, в сравнении с методами описанными далее. К таким методам относятся повторная аутентификация пользователя и CAPTCHA, представляющая собой интерактивный тест, который позволит выявить что пользователь является человеком или «компьютером». Значительным недостатком подобных методов является их влияние на пользовательский опыт (UX — User Experience). Применение этих методов имеет место, когда необходимо обеспечить безопасность таких операций как перевод денег или смена пароля от аккаунта.

Вторая группа методов уже не требует вовлечения пользователей. Она основана на применении токенов, т.е. специально сгенерированных последовательностей символов. Главной особенностью токенов является их «непредсказуемая» уникальность, достигаемая посредством комплекса математических операций. Защита на их основе является наиболее распространенным и рекомендуемым инструментом достижения безопасности информации. Стоит отметить то, что для всех указанных

методов предполагается, что общие принципы информационной безопасности соблюдены.

Первый метод основан на синхронизации токенов между сервером и пользователем, отсюда его название — Synchronizer Tokens. Этот метод базируется на сохранении информации о сессии на сервере и статусе каждого клиента в процессе множественных запросов. Задействованность в процесс обеспечения безопасности сервера — влечет за собой такие последствия как использование дополнительной памяти сервера и дисбалансу с точки зрения распределения нагрузки между серверами. Как следует из названия этот метод работает по следующей схеме: на стороне сервера генерируется токен (действует только во время текущей сессии), который сохраняется на сервере для последующей проверки и отправляется пользователю как часть ответа на инициирующий запрос. При последующих запросах пользователя на сервер также отправляется токен, где производится его сравнение с исходным токеном. Из идентичности токенов следует вывод об отсутствии CSRF-атаки, в противном случае событие логируется, а запрос отклоняется [56].

Именно метод Synchronizer Tokens используется в нашем проекте. При успешной авторизации для пользователя генерируется токен session_token, при помощи функции random_bytes. Она генерирует криптографически безопасные псевдослучайные байты произвольной длины, но этот параметр можно указать. В нашем случае он равен 32 байта. Далее необходимо перевести получившиеся байты в шестнадцатеричную систему счисления функцией bin2hex. Таким образом, в результате получаем строку длиной 64 символа – это и есть наш токен. В среде Windows функция random_bytes в качестве случайных величин использует CNG-API (Cryptography API: Next Generation) [49]. Готовый токен записывается в новую сессию пользователя (листинг 3.3. строка 1), а также помещается в скрытое поле каждой формы на сайте (листинг 3.3. строка 3). Срок жизни сессии по умолчанию составляет 1440 секунд (24 минуты). Теперь, при каждом запросе сервер будет проверять наличие и идентичность токенов. Если в запросе нет токена или он

не идентичен токену в сессии – значит, что запрос произведен не из доверенного источника. В таком случае это событие записывается в журнал и сервер возвращает ошибку.

```
1.  $_SESSION['user']['session_token'] = bin2hex(random_bytes(32));
2.
3.  <input name="session_token" type="hidden" value="<?=
    $_SESSION['user']['session_token']; ?>">
4.
5.  if ($_SERVER['REQUEST_METHOD'] == 'POST') {
6.  if ($_SESSION['user']['session_token'] == $POST['session_token']) {
```

Листинг 3.3.

Следующий метод, Double Submit Cookie, более легкий, в сравнении в предыдущим и не требует сохранения состояния на сервере. Он базируется на том, что пользователь получает от сервера токен двумя методами, в cookie-файлах и в одном из параметров ответа внутри HTML кода. При дальнейших запросах пользователь предоставляет серверу оба токена, где они сравниваются. Далее процесс идентичен первому методу. В использовании этого метода необходимо учитывать, что имеют доступ к cookie-файлам основного домена, если это явным образом не запрещено [48].

Последний метод, Encrypted Token, в отличие от предыдущих методов не требует сохранения состояния сессии, не требует cookie-файлы, и двух токенов и позволяет обеспечить более надежную защиту от CSRF-атак. Основная идея метода в том, что нельзя подделать данные, которые зашифрованы надежным алгоритмом, не зная ключа. В рамках данного метода токен передается с сервера исключительно в параметрах ответа, а сам токен генерируется с использованием идентификатора пользователя и метки времени. Перечень используемой базы фактов для шифрования может расширяться. Как и в предыдущих методах процесс начинается с генерации токена и его отправке в ответ на запрос пользователя. При дальнейших

запросах пользователя токен отправляется на сервер, где подлежит проверке. Процесс проверки заключается в расшифровке полученного токена и сравнении и с исходными данными. Дальнейшие действия идентичны предыдущим двум методам [56, 69].

Наконец сформируем основные требования к токенам:

1. Токен должен быть уникален при каждой операции;

2. Одноразовость токена;

3. Токен должен иметь достаточную длину, чтобы быть устойчивым к подбору;

4. Для генерации должны использоваться надежные алгоритмы;

5. Действие токена должно быть ограничено во времени.

Таким образом можно сказать что на данный момент существуют достаточное количество подходов к решению проблемы CSRF-атак, основные — это методы с вовлечением пользователя и с использованием генерируемых на сервере токенов. Для обеспечения достаточного уровня безопасности в таких важных операциях как денежные переводы рационально использовать сочетание обеих концепций [42].

Архитектура базы данных в нашем проекте предусматривает простую иерархию пользователей. Все авторизированные пользователи подразделяются на две роли: обычные пользователи и преподаватели. Разделение реализовано значением поля teacher_access, которое предусматривает всего два значение: ИСТИНА и ЛОЖЬ. В случае истины у пользователя появляются дополнительные возможности, что недоступны простым пользователям.

В нашем проекте интегрирована вторая ступень защиты при авторизации – двухфакторная аутентификация. Это метод, в котором используется две различных аутентификационных сущности. Двухфакторная аутентификация призвана обеспечить лучший уровень безопасности аккаунта пользователя. На сегодняшний день существует множество подходов к

реализации двухфакторной аутентификации. Некоторые подходы предполагают использование специальных устройств, которые называют токены. Они содержат уникальные данные, с помощью которых можно однозначно идентифицировать пользователя. Токены могут предусматривать подключения к компьютеру, а могут иметь дисплей, на котором будут отображаться специально сгенерированные коды. В качестве второго фактора аутентификации также могут использоваться биометрические данные пользователя, такие как снимок сетчатки глаза или отпечаток пальца. Двухфакторная аутентификация в нашем проекте работает на платформе Google Authenticator, и предполагает использование смартфона, на который установлено одноименное приложение (рис 3.6.). Для начала работы необходимо осуществить регистрацию аккаунта в нашем хранилище, в процессе этого, пользователю предлагается отсканировать в приложение специально сгенерированный QR-код или ввести символьный аналог вручную в приложении. После регистрации ключа на экране смартфона появится название аккаунта и шестизначный цифровой код, который обновляется каждые 30 секунд. Теперь при авторизации в аккаунт проекта пользователю, помимо логина и пароля будет необходимо ввести шестизначный сгенерированный код из приложения на смартфоне.

Для работы системы двойной аутентификации необходимо интегрировать ее в проект. Для этого были использованы библиотеки GoogleAuthenticator.php и FixedByteNotation.php. Также необходимо встроить определенный код в саму процедуру регистрации (листинг 3.4.).

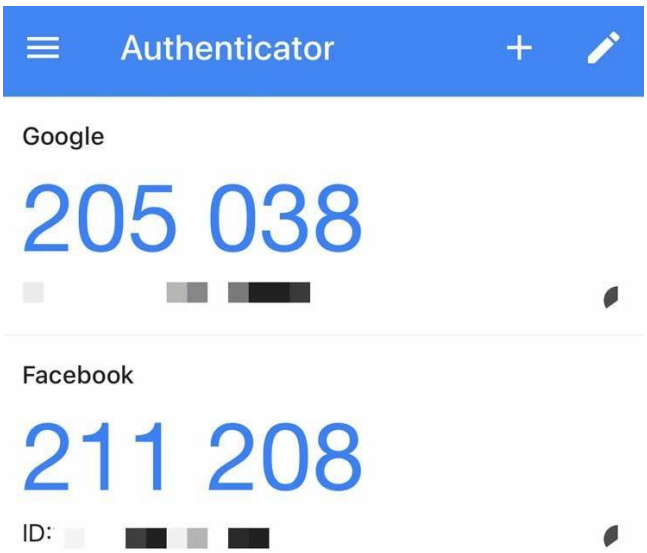

Рис 3.6. Двух факторная аутентификация.

```
1.  require_once 'GoogleAuthenticator.php';
2.  $ga = new PHP_GoogleAuthenticator();
3.  $secret = $ga->createSecret(32);
4.  $login = $signup_fields_data['email'];
5.  $qr_code = $ga->getQRCodeGoogleUrl($login, $secret);
6.  mysqli_query($link, "INSERT INTO `users` VALUES ('$login',
    '$secret')");
```

Листинг 3.4.

В первой строке подключается сама библиотека (класс), внутри которой необходимые для работы системы функции. Далее создается экземпляр класса PHP_GoogleAuthenticator, с помощью которого в третьей строке создается хэш (секрет) размером в 32 символа. Алгоритм выбора хэширующей функции идет в порядке доступности функции: random_bytes, mcrypt_create_iv, openssl_random_pseudo_bytes. После генерации хэша, на его основе создается QR-код с помощью функции getQRCodeGoogleUrl, который позже вставляется на страницу для сканирования в приложении на смартфоне. Функция принимает на вход два парамента: логин пользователя и

сгенерированный хэш (листинг 3.4. строка 5). В конце данные регистрации пользователя и хэш аутентификации записываются в базу данных.

Теперь, при регистрации необходимо сначала ввести имя пользователя, email и пароль, после чего, на следующей странице, предлагается два варианта активации генератора в приложении Google Authenticator: ручной ввод кода, или сканирование кода камерой смартфона. После активации пользователь может пользоваться системой. Если пользователем введен неверный или просроченный сгенерированный код, то система выдаст ошибку и перенаправит на страницу авторизации.

Процедура двухфакторной аутентификации позволяет значительно повысить степень защиты аккаунта пользователя и делает задачу взлома для злоумышленника крайне затруднительной. На сегодняшний день большинство интернет-сервисов предоставляют своим пользователям возможность использовать в процедуре авторизации систему двухфакторной аутентификации. Для простых пользователей этого вполне достаточно.

3.3. Практическая часть

Гипотеза нашего исследования состоит в предположении, что применение методов обеспечения информационной безопасности позволят электронному ресурсу быть устойчивым к большинству попыток злоумышленников изменить внутреннее состояние программы или получить доступ к защищенной информации. Одна из задач нашего исследования - разработать электронный образовательный ресурс в соответствии с предъявляемыми требованиями, описать разработанный продукт и проанализировать степень обеспечения информационной безопасности.

Анализ эффективности защиты электронного образовательного ресурса будет произведен по методу диверсионного анализа, его также называют инверсионным [40].

Диверсионный подход предназначен для выявления и прогнозирования проблем в целях обеспечения безопасности различных систем и процессов от отрицательных последствий. Подход разработан Б.Л. Злотиным и А.В. Зусманом и описан в труде «Методика прогнозирования чрезвычайных ситуаций, вредных и нежелательных явлений» [30]. Он позволяет выявить потенциальные слабые места системы, которые наиболее вероятно станут причиной проблем. Диверсионный подход гибок – может подстраиваться под поставленные задачи и условия. В основе подхода лежит теория решения изобретательских задач [29].

Реализация диверсионного подхода происходит поэтапно. Существует множество вариантов плана диверсионного метода. Авторы подхода предлагают наиболее детальную последовательность, состоящую из 10 комплексных этапов. Диверсионный подход гибок и в плане комбинации этапов – позволяет подстроиться к условиям конкретной задачи. Для реализации задачи нашего исследования достаточно следующих этапов [61]:

1. Инвертирование задачи;
2. Формулирование гипотез;
3. Выявление ресурсов, способствующих реализации задачи;
4. Тестирование выявленных гипотез;
5. Предложение мер по предотвращению проблем.

Этап инвертирования задачи состоит в переосмыслении изначально поставленной задачи так, чтобы из поиска причин потенциальных проблем, задачей стало непосредственное достижение этих проблем. Авторы предлагают следующий пример формулировки инвертированной задачи: «Необходимо СОЗДАТЬ возможность появления чрезвычайных ситуаций, вредных и нежелательных явлений, связанных с данной системой» [30]. Чем более конкретна задача, тем более просто она воспринимается. Инвертированная задача активизирует потребность человека в деятельности. Легче стремиться к осознаваемому результату, чем пытаться предугадать.

Этап формулирования гипотез заключается в выявлении конкретных путей достижения требуемого результата. Авторы подхода подчеркивают, что вариантов диверсий может быть множество и ни один из выявленных вариантов не должен быть упущен или отброшен без проверки, так как такое упущение может стать причиной проблем в будущем. По этой же причине не следует досрочно прекращать исследование или проводить его не в полном объеме. Выявление гипотез – задача, требующая творческой активности исследователя. Творчество должно проявляться не только в простом поиске возможных вариантов, но и в используемых подходах к исследованию объекта. Чем большей информацией владеет исследователь об объекте, тем выше качество конечного анализа [30].

Стадия выявления ресурсов, способствующих реализации задачи предполагает выявление необходимых составляющих успеха осуществления инвертированной задачи. Они являются потенциальными слабыми местами, которые могут стать причиной самопроизвольного или искусственного негативного последствия.

Этап тестирования заключается в экспериментальной проверке выявленных гипотез на основе диверсионных ресурсов.

После основной части анализа и обработки результатов необходимо сделать выводы, куда входят предложение мер по необходимой коррекции состояния системы в целях предупреждения проблемных ситуаций.

Наша исходная задача состоит в проверке эффективности предпринятых мер защиты, которые противодействуют несанкционированному доступу к аккаунту пользователя электронного образовательного ресурса.

Согласно алгоритму проведения диверсионного анализа – сначала необходимо инвертировать задачу: обойти составляющие элементы системы защиты ЭОР от несанкционированного доступа.

Гипотезы диверсионного анализа уязвимостей:

1. При попытке авторизации, сайт предлагает пройти процедуру регистрации. Зарегистрировавшись, можно получить полноценный санкционированный доступ к закрытой части сайта.

2. Форма входа предполагает заполнение трех полей: email, пароль и сгенерированный код. Из формы регистрации можно узнать, что коды генерируются на платформе сервиса Google Authenticator. После поиска информации о нем, узнаем, что в качестве кода выступает шестизначная последовательность цифр, которая меняется раз в 30 секунд. Имея компьютер, на котором осуществляется доступ к ЭОР, можно получить значения всех трех полей из DOM дерева страницы, но значение последнего поля будет уже просрочено.

3. Множество сайтов до сих пор имеют уязвимости к SQL-инъекциям, соответственно есть причины протестировать эту возможность. При наличии этой уязвимости можно расширить возможности при получении несанкционированного доступа.

4. С помощью CSRF атаки возможно совершать различные действия от имени авторизированного пользователя. Предположим, что скрипт обработки запросов на добавление файлов в базу данных имеет имя upload_files.php (точное имя можно узнать, например, перебором возможных вариантов), туда направляются данные формы, обрабатываются, после чего осуществляется запрос к базе данных на добавление записи. Если пользователь приложения, имеющий активную сессию, зайдет на специально написанную страницу со скрытой формой, то можно реализовать отправку формы от его имени.

5. Если система двухфакторной аутентификации не защищена от создания дубликатов генератора, то при регистрации нового пользователя на контролируемом компьютере возможно узнать хэш-код, по которому можно зарегистрировать генератор в приложении Google Authenticator.

6. Система двухфакторной аутентификации требует ввода шестизначного кода, состоящего из цифр от 0 до 9. Если система не

ограничивает нас в количестве попыток, то при наличии остальных авторизационных данных – есть возможность подобрать пароль.

Этап выявления диверсионных ресурсов. На нем необходимо определить факторы, которые способствуют успешному осуществлению атаки. В нашем случае, к диверсионным ресурсам относятся:

1. Осуществление запросов по протоколу HTTP;

2. Веб-приложение не имеет механизма подтверждения регистрации новых пользователей;

3. Механизм авторизации не огранивает пользователей в попытках ввода данных авторизации;

4. Отсутствие на компьютере запрета на установку дополнительного программного обеспечения;

5. Данные, которые поступают на сервер со стороны пользователя не проходят процедуру обработки на наличие небезопасных подстрок;

6. Запросы к базе данных осуществляются без применения приемов подготовленных запросов;

7. Форма, отправляющая запрос на сервер от лица авторизированного пользователя доступна для неавторизированных пользователей;

8. Обработчики форм на сервере не имеют возможностей для проверки подлинности источника запроса;

9. Система двухфакторной аутентификации не ограничивает количество носителей генератора;

10. В распоряжении имеется компьютер, на котором пользователи авторизуются в системе ЭОР.

Этап тестирования. Проверка истинности выявленных гипотез экспериментальным путем.

Проверка гипотезы 1: При переходе на страницу авторизации, проследуем по ссылке на страницу регистрации. Вводим вымышленные регистрационные данные: имя пользователя, email, пароль и направление обучения. Подтверждаем регистрацию отправкой формы на сервер.

Регистрируем генератор кодов в системе Google Authenticator и переходим на страницу авторизации в системе. Вводим те же данные, что и при регистрации, подтверждаем отправкой формы для авторизации, после чего сервер перенаправляет нас на страницу с единственной надписью: «Ваш аккаунт не подтвержден, пожалуйста, свяжитесь с администратором». Следовательно, после регистрации пользователя, система проверяет email-адрес на наличие в списке допустимых адресов. При наличии адреса в списке допустимых, алгоритм помечает аккаунт как подтвержденный и разрешает доступ к закрытой части сайта. Из этого следует вывод, что гипотеза неверна.

Проверка гипотезы 2: Большинство пользователей для перехода на нужный сайт используют поисковик, если сайт посещается часто, то высока вероятность, что нужный сайт поместят в закладки в браузере. В данном случае мы изменили адрес закладки на подставной. Если перейти по этой ссылке, то пользователь попадает на такую же страницу авторизации, как и оригинальная, за двумя исключениями: URL-адрес страницы незначительно отличается, а форма авторизации имеет измененный атрибут action. Форма на поддельной странице отправляет данные на наш сервер. При отправке формы срабатывает браузерное событие, которое перенаправляет пользователя на оригинальную страницу авторизации. Таким образом мы получаем два из трех действующих параметров авторизации. Последний параметр – генерируемый код, в нашем случае уже не действителен. Как вывод, можно считать данную гипотезу отчасти подтвержденной. Это действительно хороший инструмент для более крупного алгоритма получения несанкционированного доступа.

Проверка гипотезы 3: Для тестирования уязвимости сайта к SQL инъекциям будем использовать стандартный словарь с командами для обхода аутентификации средствами инъекций. Отметим, что тестирование этой гипотезы подразумевает наличие кода двухфакторной аутентификации.

Тестирование не показало положительных результатов, после каждой команды на экран выводилось сообщение о неверно введенном пароле, из

чего можем сделать предположение, что пользовательский ввод обрабатывается на стороне сервера или для формирования запросов к базе данных, используются приемы подготовленных запросов.

Проверка гипотезы 4: Для испытания гипотезы создадим страницу, которая содержит две скрытые формы, первая автоматически отправляется, как только пользователь заходит на страницу. Данные из первой формы отправляются на тот же адрес, куда посылаются запросы на добавление файлов в базу данных. Вторая форма отправляется на наш сервер, после того как сервер ответит на первую форму. Она содержит код ответа сервера «жертвы», эти данные помещаются во вторую форму. Заставим пользователя перейти на нашу страницу методом фишинга.

После того как пользователь зашел на нашу страницу и формы отправились, мы получаем ответ от второй форму, которая содержит код ответа сервера на первую форму. В результате тестов мы собрали 17 ответов. 11 из них содержали код ответа 403, остальные вернули код 401. Согласно списку кодов состояния HTTP, код 403 соответствует значению «запрещено (не уполномочен)». Этот код означает, что сервер принял запрос, но отказался выполнять его из-за ограничений в доступе для клиента к указанному ресурсу [79]. Так как сервер принял запрос, значит адрес верен, но он отказался его исполнять вернув код 403, что значит что сервер отличил запрос от неавторизированного (401 - для доступа к запрашиваемому ресурсу требуется аутентификация), соответственно можно утверждать что система защиты располагает защитой от CSRF атак, и, как следствие, данная гипотеза неверна.

Проверка гипотезы 5: Так как мы располагаем доступом к компьютеру, на котором часто пользуются хранилищем учебных материалов – скопируем на компьютер файлы уже установленной программы Neospy. Также можно использовать SpyGo или ZD Screen Recorder. Эти программы предназначены для скрытой записи видео с экрана компьютера. Мы используем Neospy по причине скрытности программы от глаз пользователя. Она также может

записывать нажатия клавиш клавиатуры. Политика безопасности на компьютерах настроена таким образом, что пользователи не могут ничего установить, но можно запускать уже установленные программы, по этой причине достаточно скопировать файлы уже установленной версии Neospy.

Мы запустили программу в скрытом режиме и настроили на запись снимков с экрана при любых событиях на экране и на запись нажатий клавиш клавиатуры.

В результате испытания мы получили изображение QR-кода, который используется для регистрации генератора кодов, а также логин и пароль пользователя. Далее мы совершили попытку регистрации дубликата генератора на другом смартфоне с установленным приложением Google Authenticator. При попытке входа появилось сообщение о неверности введенного кода. После этого было совершено еще две попытки регистрации дубликата. Каждый из дубликатов показывал различные коды, из чего следует вывод, что действительны ключи только из первого генератора. В итоге мы получили логин и пароль, но не получили генератор действительных кодов. Таким образом, можно сделать вывод о неверности гипотезы, даже при частичных успехах.

Проверка гипотезы 6: Две из предыдущих гипотез показал возможность получения логина и пароля пользователя. Также, в одной из предыдущих гипотез мы выяснили, что система не ограничивает нас в попытках авторизации. Следовательно, мы можем осуществить подбор пароля. Система Google Authenticator требует ввод шестизначного пароля, состоящего из цифр от 0 до 9. Чтобы вычислить количество возможных комбинаций необходимо количество возможных вариантов одной позиции возвести в степень общего числа таких позиций - 10^6 (1 млн) комбинаций. Для подбора пароля воспользуемся расширением для браузера www_brute. После настройки перебора на нужные диапазоны – активировали процесс подбора. В результате выяснилось, что скорость тестирования одного пароля составляет примерно 1,5 секунды. За срок действительности одного кода

успевает протестироваться 20 вариантов, что крайне мало, в сравнении с общим числом комбинаций. Было произведено десять сессий по 30 секунд, за это время не была найдена нужная комбинация. Вероятность найти действительный код составляет 0,02%, из чего делаем вывод, что гипотеза с подбором кода неверна.

Предложение мер по предотвращению проблем:

1. Внести правку в правила использования компьютерной техники о том, что пользователям необходимо проверять адреса посещаемых сайтов, либо переходить на них из поисковиков;
2. Все данные поступающие от пользователя, включая Cookie-файлы, данные форм, GET и POST запросы должны проходить обязательную обработку на предмет небезопасных подстрок;
3. Все запросы к базе данных, в которых участвуют данные, полученные от пользователя - необходимо осуществлять с помощью подготовленных запросов;
4. Необходимо генерировать уникальные токены для сессий авторизированных пользователей, после чего после чего помещать их как скрытые поля во все формы и файлы сессии. При осуществлении запроса со стороны пользователя необходимо сравнивать полученный токен и тот, что хранится в сессии;
5. Для лучшей безопасности такие же меры можно предпринять и для неавторизированных пользователей, а после авторизации просто заменять старый токен на новый;
6. Провести инструктаж с персоналом и обучающимися на тему методов мошенничества в интернете;
7. Проводить мониторинг программ, которые запускаются с запуском операционной системы;
8. Внести изменения в политику безопасности компьютеров, согласно которым невозможно будет запускать неодобренные исполняемые файлы.

9. Использование HTTPS протокола, так данные, передаваемые по этому протоколу зашифрованы, их нельзя перехватить или несанкционированно прочитать.

ВЫВОДЫ ПО ТРЕТЬЕЙ ГЛАВЕ

Разработанное нами продукт называется хранилище учебных материалов ЧИПС УРГУПС. Он представляет собой веб-приложение (сайт) и запускается в браузере при переходе по соответствующему URL-адресу. Приложение предназначено для хранения электронных материалов, которые могут понадобится для обеспечения учебного процесса. Наш электронный образовательный ресурс поддерживает опциональный режим доступности для слабовидящих. Сайт также поддерживает доступность интерфейса программ, которые читают текст с экрана. Приложение построено при помощи следующих основных технологий: HTML, БЭМ, CSS, SCSS, Gulp, NPM, PHP, Google Authenticator, MySQL. Основные меры защиты, использующиеся в приложении: пользовательские данные подлежат обработке на сервере, используется защита от SQL-инъекций и межсайтовой подделки запросов, а также в проект интегрирована система двухфакторной аутентификации.

Для проверки эффективности защиты информационной безопасности нашего приложения использовался диверсионный анализ, в рамках которого задачей стало обойти защиту элементов защиты, с конечной целью получения несанкционированного доступа к закрытой части сайта. В рамках анализа было выявлено 6 основных гипотез по обходу защиты. Каждая из них была практически протестирована на проекте. В результате тестов были отвергнуты все гипотезы. При этом, в ходе тестирования двух из гипотез были получены логины и пароли аккаунтов пользователей, а также генерируемые коды. Из-за ограниченного срока действия кодов, ими уже нельзя было воспользоваться. На основе полученных данных в процессе

анализа приложения был сформирован перечень мер по ликвидации выявленных уязвимостей, среди них: использование HTTPS протокола передачи данных, обязательная обработка данных поступающих со стороны пользователя, а также все запросы к базе данных, которые зависят от данных пользователя, необходимо производить методами подготовленных запросов.

Таким образом, в главе проработаны две задачи исследования:

1. Изучение этапов разработки электронных образовательных ресурсов;

2. Разработка, описание и анализ защищенности электронного образовательного ресурса.

ЗАКЛЮЧЕНИЕ

Электронные образовательные ресурсы – это фундаментальный компонент информационной образовательной среды, а также основа для применения в процессе обучения новых форм и методов обучения, таких как электронное обучение, сетевое обучение, мобильное обучение, автономное обучение, смешанное и совместное обучение. На данный момент ведутся активные исследования и разработки, основными задачами который является достижение большей эффективности процесса образования. Интерактивность позволяет добиться лучшей активности обучающихся, их вовлеченности в занятие и, соответственно, воспринимаемости материала. Социальная составляющая несет в себе стимулирующую роль, наличие других участников обучения стимулируют конкуренцию среди участников, что также повышает эффективность деятельности. Активно развивается геймификация учебного процесса.

Требования к ЭОР затрагивают множество сторон разработки, проектирования и поддержки проекта. При проектировании необходимо учитывать цели и сценарии взаимодействия пользователей с ЭОР. Необходимо обеспечивать доступность ресурса к использованию пользователей с ограниченными возможностями здоровья. Важна и внешняя

сторона ЭОР, необходимо обеспечить хорошую читаемость, достаточную плотность материалов на экране, удобство интерфейса и навигации, так как этого напрямую зависит эффективность применения ЭОР. Для лучшего восприятия материала, необходимо подбирать такую форму представления, которая обеспечит наиболее простое восприятие.

Процесс разработки электронных образовательных ресурсов разделяется на два комплексных этапа. На первом этапе формируется концепция ресурса, собирается и обрабатывается учебный материал, продумываются сценарии взаимодействия обучающихся с ресурсом, а также подготавливаются инструменты, необходимые для разработки ЭОР. На втором этапе происходит непосредственная разработка ресурса с учетом требований, тестирование промежуточных результатов и последующая доработка.

Базой нашего исследования является образовательная организация среднего профессионального образования «Челябинский институт путей сообщения». Систему информационной безопасности базы исследования можно разделить на три основных категории, а именно информационная безопасность технических средств, безопасность персональных данных и защита обучающихся от доступа к информации, которая может отрицательно сказаться на психическом и физическом здоровье. В институте используется перечень рекомендаций по работе с персональными данными.

Разработанное нами продукт называется хранилище учебных материалов ЧИПС УРГУПС. Как отражено в названии, продукт разрабатывался для использования в рамках образовательной организации ЧИПС УРГУПС. Оно представляет собой веб-приложение. Приложение предназначено для использования как обучающимися, так и преподавателями, и может использоваться в любое время, независимо от местоположения пользователя и текущего времени.

Анализ эффективности защиты электронного образовательного ресурса был произведен по методу инверсионного анализа. Он проходил в пять

этапов, в ходе которых была сформулирована задача анализа, после чего инвертирована в целях проведения анализа. Далее были сформированы шесть гипотез, предполагавших обход предпринятых мер защиты приложения с целью получения несанкционированного доступа к закрытой части хранилища. Были выявлены диверсионные ресурсы, наличие которых способствует успешному произведению обхода мер защиты. На основном этапе были протестированы гипотезы, ни одна из которых полностью не подтвердилась. Две из них показали частично успешные результаты, позволив получить две из трех сущности, необходимых для авторизации. На основании выявленных уязвимостей был сформирован перечень мер и рекомендаций, исполнение которых позволит устранить выявленные уязвимости, а соответственно и повысить общий уровень защищенности ресурса.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Постановление Правительства РФ "Об утверждении государственной программы Российской Федерации "Развитие образования" [Текст] : [Утверждена постановлением Правительства РФ от 26 декабря 2017 года N 1642] : офиц. текст. – Москва. 2017. – 356 с.

2. Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных " [Текст] : [Утверждены постановлением Правительства РФ 1 ноября 2012 года N 1119] : офиц. текст. – Москва. 2012. – 5 с.

3. Постановление Правительства РФ от 21 марта 2012 г. N 211 " Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" [Текст] : [Утверждены постановлением Правительства РФ 21 марта 2012 года N 211] : офиц. текст. – Москва. 2012. – 3 с.

4. Постановление Правительства РФ от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных" [Текст] : [Утверждены постановлением Правительства РФ 6 июля 2008 года N 512] : офиц. текст. – Москва. 2008. – 4 с.

5. Постановление Правительства РФ от 6 июля 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" [Текст] : [Утверждены постановлением Правительства РФ 15 сентября 2008 года N 687] : офиц. текст. – Москва. 2008. – 4 с.

6. Приказ Министерства образования и науки РФ "Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ" [Текст] : [Утвержден приказом Министерства образования и науки Российской Федерации от 23 августа 2017 г. N 816] : офиц. текст. – Москва. 2017. – 4 с.

7. Распоряжение Правительства РФ "Об утверждении Концепции информационной безопасности детей" [Текст] : [Утверждено распоряжением Правительства РФ 2 декабря 2015 года N 2471-р] : офиц. текст. – Москва. 2015. – 10 с.

8. Российская Федерация. Конституция (1993). Конституция Российской Федерации [Текст] : принята всенар. голосованием 12.12.1993 г. / Российская Федерация. Конституция (1993). — М. : АСТ : Астрель, 2007. — 63 с.

9. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 27.12.2018) // Собрание законодательства РФ. - 17.06.1996. - № 25. - ст. 2954.

10. Указ Президента РФ “Доктрина информационной безопасности Российской Федерации” [Текст] : [Утверждена указом президента РФ N 646 от 5 декабря 2016] : офиц. текст. – Москва. 2016. – 10 с.

11. Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" [Текст] : [Принят Государственной Думой 21 декабря 2010 года. Одобрен Советом Федерации 29 декабря 2010 года] : офиц. текст. – Москва. 2010. – 18 с.

12. Федеральный закон "О персональных данных" [Текст] : [Принят Государственной Думой 8 июля 2006 года. Одобрен Советом Федерации 14 июля 2006 года.] : офиц. текст. – Москва. 2006. – 30 с.

13. Федеральный закон "Об информации, информационных технологиях и о защите информации" [Текст] : [Принят Государственной Думой 8 июля 2006 года. Одобрен Советом Федерации 14 июля 2006 года] : офиц. текст. – Москва. 2006. – 180 с.

14. Федеральный закон "Об образовании в Российской Федерации" [Текст] : [Принят Государственной Думой 21 декабря 2012 года. Одобрен Советом Федерации 26 декабря 2012 года.] : офиц. текст. – Москва. 2012. – 169 с.

15. ФСТЭК России “Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных” [Текст] : [Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 года] : офиц. текст. – Москва. 2008. – 72 с.

16. ФСТЭК России “Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных” [Текст] : [Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 года] : офиц. текст. – Москва. 2008. – 10 с.

17. ISO/IEC 27001. Системы обеспечения информационной безопасности: дата введения 2013 (дата обращения 24.12.2019) . –Текст: электронный.

18. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.: дата введения 01.01.1996. – URL: http://docs.cntd.ru/document/gost-r-50739-95 (дата обращения 24.12.2019). – Текст: электронный.

19. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения : Дата введения 2008.02.01. – URL: http://docs.cntd.ru/document/1200058320 (дата обращения 24.12.2019). –Текст: электронный.

20. ГОСТ Р 52292-2004 Информационная технология (ИТ). Электронный обмен информацией. Термины и определения: дата введения 07.01.2005. - URL: http://docs.cntd.ru/document/1200038309 (дата обращения 24.12.2019) . –Текст: электронный.

21. ГОСТ Р 52653-2006. Информационно-коммуникационные технологии в образовании. Термины и определения.: дата введения 01.07.2008. – URL: http://docs.cntd.ru/document/1200053103 (дата обращения 24.12.2019). – Текст: электронный.

22. ГОСТ Р 52657-2006. Информационно-коммуникационные технологии в образовании. Образовательные интернет-порталы федерального уровня. Рубрикация информационных ресурсов: дата введения 01.07.2008.- URL: http://docs.cntd.ru/document/1200053104 (дата обращения 24.12.2019). – Текст: электронный.

23. ГОСТ Р 53620-2009 Информационно-коммуникационные технологии в образовании. Электронные образовательные ресурсы. Общие положения: дата введения 01.01.2011.- URL: http://docs.cntd.ru/document/1200082196 (дата обращения 24.12.2019). –Текст: электронный.

24. ГОСТ Р 55751-2013 Информационно-коммуникационные технологии в образовании. Электронные учебно-методические комплексы. Требования и характеристики : дата введения 01.01.2015.- URL: http://docs.cntd.ru/document/1200108264 (дата обращения 24.12.2019). –Текст: электронный.

25. ГОСТ Р ИСО 14915-1-2010 Эргономика мультимедийных пользовательских интерфейсов. Часть 1. Принципы проектирования и структура : Дата введения 2008.06.01. – URL: http://docs.cntd.ru/document/1200066538 (дата обращения 24.12.2019). –Текст: электронный.

26. ГОСТ Р ИСО 9241-110-2009. Эргономика взаимодействия человек-система. Часть 110. Принципы организации диалога : Дата введения 2010.12.01. – URL: http://docs.cntd.ru/document/gost-r-iso-9241-110-2009 (дата обращения 24.12.2019). –Текст: электронный.

27. ГОСТ Р ИСО 9241-1-2007 Эргономические требования к проведению офисных работ с использованием видеодисплейных терминалов (VDTs). Часть 1. Общее введение : Дата введения 2008.06.01. – URL: http://docs.cntd.ru/document/1200082724 (дата обращения 01.12.2011). –Текст: электронный.

28. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования: дата введения 02.01.2008. - URL: http://docs.cntd.ru/document/gost-r-iso-mek-27001-2006 (дата обращения 24.12.2019) . –Текст: электронный.

29. Альтшуллер Г.С. Творчество как точная наука [Текст] / Г.С. Альтшеллер. 2-е изд. Петрозаводск: Скандинавия, 2004.

30. Б.Л. Злотин, А.В. Зусман. Методика прогнозирования чрезвычайных ситуаций, вредных и нежелательных явлений [Текст] / Злотин Б.Л., Зусман А.В., Кишинев. - 1991 - 22 с.

31. Башмаков А.И. Принципы и технологические основы создания открытых информационно-образовательных сред [Текст] / А. И. Башмаков, В. А. Старых; под ред. А.Н. Тихонова. - М. : Бином. Лаборатория знаний, 2010. - 719 с.

32. Гура В.В. Теоретические основы педагогического проектирования личностно-ориентированных электронных образовательных ресурсов и сред [Текст] : Ростов н/Д: Изд-во ЮФУ, 2007. 320 с.

33. Единые требования к электронным образовательным ресурсам [Текст] : : офиц. текст. – Москва. 2011. – 48 с.

34. Задорожнюк И.Е. Психологические аспекты обучения эргономике [Текст] / И.Е. Задорожнюк // Вопросы психологии. - 2009. - № 5. - С. 163-166.

35. Использование инновационных технологий в образовательном процессе [Текст] : монография / Е. Н. Рогановская, Л.Н. Порядина, П. В. Никитин [и др.] ; Сиб. федер. ун-т ; Краснояр. гос. пед. ун-т им. В. П. Астафьева [и др.]. –Красноярск : ООО «Центр информации», ЦНИ «Монография», 2014 – 236 с.

36. Мандель Б.Р. Инновационные технологии педагогической деятельности [Текст] : учебное пособие для магистрантов . Б.Р. Мандель. – Изд. 2-е, стер. – Москва ; Берлин: Директ-Медиа, 2019. – 260 с.

37. Рекомендация ЮНЕСКО “О развитии и использовании многоязычия и всеобщем доступе к киберпространству” [Текст] : [Утвержден на Генеральной конференции 2003] 2003. – 7 с.

38. Кононов Д.Д., Исаев С.В. Модель безопасности кросс-платформенных веб-сервисов поддержки муниципальных закупок [Текст] / Д.Д. Кононов, С.В. Исаев. // ПДМ, 2011, приложение № 4, 48–50.

39. Маркарова Т.С., Моисеев К.В., Агафонов Ю.В. Создание электронных образовательных ресурсов в условиях традиционной отраслевой библиотеки [Текст] / Т.С. Маркарова, К.В. Моисеев, Ю.В. Агафонов // Информационные ресурсы России. – 2008. - № 2. – С. 12-14.

40. Падалец А.М. Применение диверсионного подхода для выявления угроз информационной безопасности электронного образовательного ресурса [Текст] // Актуальные проблемы образования: позиция молодых. – 2020.

41. Падалец А.М., Зайцев В.С. Когнитивные карты как форма визуального мышления [Текст] // Инновационные научные исследования: теория, методология, практика. – 2018. – С. 226-228.

42. Падалец А.М., Куликова А.С. Методы защиты от сетевых атак типа подделки межсайтовых запросов [Текст] // Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы. – 2020. – С. 91-95.

43. Падалец А.М., Шахматов Н.С., Куликова А.С. Особенности разработки электронных образовательных ресурсов в соответствии с требованиями нормативных документов [Текст] // Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы. – 2020. – С. 95-100.

44. Роберт И.В. Перспективные научные исследования, определяющие развитие информатизации образования [Текст] / И.В. Роберт // Педагогическое образование в России. 2014.№4. С. 199-204.

45. Смольникова И.А. Электронная поддержка учебно-методической деятельности [Текст] / И.А. Смольникова // Информационные технологии в обеспечении нового качества высшего образования. — МИСиС Москва, 2015.

46. Соколова И.В., Смольникова И.А. Концепция электронного учебно-методического комплекса для обеспечения самостоятельной работы студентов информационного профиля [Текст] / И.В. Соколова, И.А. Смольникова // Современное социальное образование: опыт и проблемы модернизации. VII Всероссийский соц.-пед. конгресс. – РГСУ, 2016.

47. Толмачев В.В. Проблемы обеспечения информационной безопасности в общеобразовательных организациях [Текст] / В.В. Толмачев // Конференциум АСОУ. 2015. №1. С. 2198-2210.

48. Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet [Электронный ресурс]. URL.: https://www.owasp.org/index.php/Cross-Site_Request_Forgery_%28CSRF%29_Prevention_Cheat_Sheet (дата обращения: 13.12.18).

49. Cryptography API: Next Generation [Электронный ресурс]. URL.: https://docs.microsoft.com/en-us/windows/win32/seccng/cng-portal (дата обращения: 13.12.18).

50. DDoS-атаки: нападение и защита [Электронный ресурс]. URL: https://habr.com/ru/company/ruvds/blog/321992/ (дата обращения: 01.03.20).

51. HTML Standard. The input element [Электронный ресурс]. URL.: https://html.spec.whatwg.org/multipage/input.html#range-state (дата обращения: 13.12.18).

52. Hypertext Transfer Protocol Version 2 (HTTP/2) [Электронный ресурс]. URL.: https://tools.ietf.org/html/rfc7540 (дата обращения: 22.01.20).

53. ISO 9241-110 — Принципы организации диалога [Электронный ресурс]. URL: https://habr.com/ru/post/257729 (дата обращения: 22.01.20).

54. Moodle Documentation [Электронный ресурс]. URL.: https://docs.moodle.org/38/en/Main_page (дата обращения: 01.03.20).

55. SQL-инъекции [Электронный ресурс]. URL: https://www.php.net/manual/ru/security.database.sql-injection.php (дата обращения: 01.03.20).

56. The Cross-Site Request Forgery (CSRF/XSRF) [Электронный ресурс]. URL.: https://www.cgisecurity.com/csrf-faq.html (дата обращения: 13.12.18).

57. Top 10 Web Application Security Risks [Электронный ресурс]. URL: https://owasp.org/www-project-top-ten/ (дата обращения: 01.03.20).

58. Беляев М.И., Гриншкун В.В., Краснова Г.А. Технология создания электронных средств обучения [Электронный ресурс]: доклад, опубликованный 30.08.2007. URL: http://www.ido.rudn.ru/nfpk/tech/t2.html (дата обращения: 17.10.19).

59. Внедрение SQL-кода [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Внедрение_SQL-кода (дата обращения: 01.03.20).

60. Геймификация в e-learning [Электронный ресурс]. URL: http://e-learningcenter.ru/wp-content/uploads/2014/02/012014-1.pdf (дата обращения: 11.04.19).

61.Д.И. Буслов, И.Н. Холкин. Как, используя диверсионный анализ ТРИЗ, найти критическую уязвимость, грозящую безопасности SAP Hana [Текст] // Математика и информационные технологии в нефтегазовом комплексе. 2015. №2. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/kak-ispolzuya-diversionnyy-analiz-triz-nayti-kriticheskuyu-uyazvimost-grozyaschuyu-bezopasnosti-sap-hana (дата обращения: 01.04.2020).

62. Единый реестр Роскомнадзор [Электронный ресурс]. URL: https://eais.rkn.gov.ru/ (дата обращения: 17.10.19).

63. Защита от SQL-инъекций [Электронный ресурс]. URL: http://phpfaq.ru/mysql/slashes (дата обращения: 01.03.20).

64. Информационно-коммуникационная инфраструктура учреждения сферы образования [Электронный ресурс]. URL: https://www.intuit.ru/studies/courses/12103/1165/print_lecture/19313 (дата обращения: 01.03.20).

65. Как сделать сайт, доступный всем [Электронный ресурс]. URL: https://geekbrains.ru/posts/colorblindness_design_howto (дата обращения: 12.02.20).

66. Клиент — сервер [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Клиент_—_сервер (дата обращения: 17.10.19).

67. Клиент-серверные сети [Электронный ресурс]. URL: https://www.sites.google.com/site/websitecomputernetworks/home/lection/2/2-2/2-2-2 (дата обращения: 17.10.19).

68. Конфиденциальность, целостность, доступность [Электронный ресурс]. URL: https://www.intuit.ru/studies/curriculums/4088/courses/1286/print_lecture/24236 (дата обращения: 17.10.19).

69. Межсайтовая подделка запроса // Википедия. [2018—2018]. Дата обновления: 04.06.2018. URL: https://ru.wikipedia.org/?oldid=93087656 (дата обращения: 23.12.2018).

70. Межсайтовый скриптинг [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Межсайтовый_скриптинг (дата обращения: 01.03.20).

71. Методы борьбы с DoS/DDoS-атаками [Электронный ресурс]. URL: https://xakep.ru/2009/10/14/49752/ (дата обращения: 01.03.20).

72. Основные требования, предъявляемые к разработке электронных средств обучения [Электронный ресурс]. URL: https://zinref.ru/000_uchebniki/02800_logika/011_lekcii_raznie_34/1289.htm (дата обращения: 11.04.19).

73. Подготовленные запросы и хранимые процедуры [Электронный ресурс]. URL: https://www.php.net/manual/ru/pdo.prepared-statements.php (дата обращения: 01.03.20).

74. Политика в области защиты персональных данных ЧИПС УрГУПС [Электронный ресурс]. URL: https://chirt.usurt.ru/about/dokumentatsiya/politika-v-oblasti-zaschity-personalnykh-dannykh (дата обращения: 17.10.19).

75. Порядок разработки электронных образовательных ресурсов [Электронный ресурс]. URL: https://www.intuit.ru/studies/courses/12103/1165/print_lecture/19311 (дата обращения: 13.03.20).

76. Пост-эксплуатация XSS: продвинутые методы и способы защиты [Электронный ресурс]. URL: https://www.securitylab.ru/analytics/440187.php (дата обращения: 01.03.20).

77. Разработка электронных образовательных ресурсов [Электронный ресурс] / Белорусский государственный педагогический университет имени М. Танка. – Минск, 2015 – URL: http://crit.bspu.by/wpcontent/uploads/2015.pdf (дата обращения: 17.10.19).

78. Генеральная прокуратура Российской Федерации. Статистические данные. [Электронный ресурс]. URL.: https://genproc.gov.ru/stat/ (дата обращения: 13.12.18).

79. Список кодов состояния HTTP [Электронный ресурс]. URL.: https://ru.wikipedia.org/wiki/Список_кодов_состояния_HTTP#403 (дата обращения: 13.12.18).

80. Устраняем уязвимости: как защитить сайт от SQL-инъекции [Электронный ресурс]. URL: https://skillbox.ru/media/code/kak_zashchitit_sayt_ot_sql_inektsii/ (дата обращения: 01.03.20).

81. Функции хэширования поролей. Password_hash [Электронный ресурс]. URL.: https://www.php.net/manual/ru/function.password-hash.php (дата обращения: 13.12.18).

82. Функции хэширования поролей. Password_verify [Электронный ресурс]. URL.: https://www.php.net/manual/ru/function.password-verify.php (дата обращения: 13.12.18).

83. Функция mysqli_prepare [Электронный ресурс]. URL: https://www.php.net/manual/ru/mysqli.prepare.php (дата обращения: 01.03.20).

84. Челябинский институт путей сообщения [Электронный ресурс]. URL: https://chirt.usurt.ru/ (дата обращения: 17.10.19).

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1

Перечень обязательных документов, необходимых для системы управления информационной безопасностью персональных данных в образовательной организации.

1. Приказ о назначении ответственных за безопасность ПДн (персональные данные).

2. Приказ о назначении ответственных лиц за ПДн и список ответственных лиц.

3. Приказ о введении режима обработки ПДн.

4. Приказ о создании комиссии для классификации ИСПДн.

5. Перечень подразделений и сотрудников, допущенных к работе с ПДн.

6. Перечень ИСПДн.

7. Перечень ПДн.

8. Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах.

9. Частная модель угроз.

10. Инструкция пользователя ИСПДн.

11. Акт Классификации ИСПДн.

12. СОГЛАСИЕ на обработку ПДн.

13. Обязательство о неразглашении ПДн.

14. Журнал учета носителей ПДн.

15. Журнал учёта обращений субъектов ПДн о выполнении их законных прав.

ПРИЛОЖЕНИЕ 2

Стандартный словарь для обхода аутентификации средствами SQL-инъекций

1. ' or 1=1;

2. ' or 1=1--;

3. ' or 1=1#;

4. ' or 1=1/*;

5. admin' --;

6. admin' #;

7. admin'/*;

8. admin' or '1'='1;

9. admin' or '1'='1'--;

10. admin' or '1'='1'#;

11. admin' or '1'='1'/*;

12. admin'or 1=1 or ''=';

13. admin' or 1=1;

14. admin' or 1=1--;

15. admin' or 1=1#;

16. admin' or 1=1/*;

17. admin') or ('1'='1;

18. admin') or ('1'='1'--;

19. admin') or ('1'='1'#;

20. admin') or ('1'='1'/*;

21. admin') or '1'='1;

22. admin') or '1'='1'--;

23. admin') or '1'='1'#;

24. admin') or '1'='1'/*;

25. 1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055.