

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.03 —

Информационная безопасность
автоматизированных систем

Специализация —

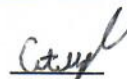
Защищённые автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

УЧЕБНЫЙ РЕСУРС ДЛЯ ИССЛЕДОВАНИЯ МЕХАНИЗМОВ
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕЛЯЦИОННЫХ
БАЗ ДАННЫХ В ЯЗЫКЕ ПРОГРАММИРОВАНИЯ SQL

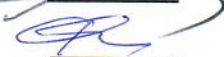
Студент

 Сливин Артем Максимович

Руководитель

 Мали В.А.

Нормоконтролёр

 Фатеев А.Г.

Рецензент начальник отдела
АО «ПНИЭИ»

 Оськин Р.С.

Работа допущена к защите (протокол заседания кафедры от 15.06.20 № 13)

Заведующий кафедрой

 С.Л. Зефирова

Работа защищена с отметкой отлично (протокол заседания ГЭК от 25.06.20 № 7)

Секретарь ГЭК

 А.П. Иванов

Пенза 2020

Оглавление

Введение.....	4
1 Анализ требований, применяемых к учебному ресурсу.....	6
2 Оценка безопасности технологий интеграции дистанционных ресурсов обучения с системами управления обучением.....	10
2.1 Анализ информационных источников, содержащих информацию о современных системах управления обучением и технологиях интеграции с ними внешних ресурсов.....	10
2.2 Анализ реализации технологий интеграции внешних ресурсов с системами управления обучением с точки зрения информационной безопасности.....	20
3 Проектирование учебного ресурса.....	34
3.1 Проектирование архитектуры учебного ресурса.....	34
3.2 Проектирование модуля разграничения доступа.....	35
3.3 Проектирование модуля управления учебным ресурсом.....	37
3.4 Проектирование модуля контроля учебного процесса.....	40
3.5 Проектирование модуля интерфейса обучающегося.....	43
3.6 Проектирование модуля обмена данными с внешними ресурсами.....	43
3.7 Проектирование модуля взаимодействия с базой данных.....	44
3.8 Проектирование модуля регистрации событий.....	46
3.9 Проектирование модуля обеспечения информационной безопасности.....	46
4 Разработка учебного ресурса.....	52
4.1 Разработка модуля разграничения доступа.....	52
4.2 Разработка модуля управления учебным ресурсом.....	59
4.3 Разработка модуля контроля учебного процесса.....	69
4.4 Разработка модуля интерфейса обучающегося.....	70

4.5 Разработка модуля обмена данными с внешними ресурсами.....	70
4.6 Разработка модуля взаимодействия с базой данных.....	71
4.7 Разработка модуля регистрации событий.....	73
4.8 Разработка модуля обеспечения информационной безопасности.....	80
5 Тестирование учебного ресурса.....	86
6 Разработка документации к учебному ресурсу.....	93
7 Вредные психофизиологические факторы, влияющие на органы зрения специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	94
Заключение.....	96
Список используемых источников.....	99
Приложение А. Руководство по инсталляции.....	102
Приложение Б. Руководство по эксплуатации.....	111

Введение

В современном мире реляционные базы данных используются практически в каждой организации, а число и сложность кибератак, производимых на базы данных, с каждым годом неуклонно растут. В соответствии с последними исследованиями, 24% всех кибератак направлены на веб-ресурсы. Основной целью таких атак является получение доступа к базам данных, содержащих защищаемую информацию. Организации и люди, чья информация, представляющая для них ценность, хранится в базах данных, заинтересованы в том, чтобы их ценная информация была в безопасности. Надёжную защиту баз данных могут обеспечить квалифицированные специалисты в области информационной безопасности. Но специалист, умеющий пользоваться самыми современными технологиями в области информационной безопасности, в процессе своего обучения должен пользоваться самыми актуальными и информативными ресурсами. Современные технологии предоставления дистанционного образования позволяют получить доступ к информации из любой точки мира.

В связи с вышеописанным возникает необходимость разработки защищённых с точки зрения информационной безопасности дистанционных ресурсов обучения, дополняющих и улучшающих учебный процесс.

Цель выпускной квалификационной работы - разработать защищённый с точки зрения информационной безопасности дистанционный учебный ресурс для получения навыков обеспечения информационной безопасности реляционных баз данных средствами языка SQL (далее — учебный ресурс). Разработанный учебный ресурс можно будет использовать как основу для создания новых интерактивных учебных ресурсов.

Для достижения цели работы были поставлены следующие задачи:

- провести анализ требований, применяемых к учебному ресурсу;
- провести оценку безопасности технологий интеграции

дистанционных ресурсов обучения с системами управления обучением;

- выполнить проектирование учебного ресурса;
- разработать учебный ресурс;
- провести тестирование учебного ресурса;
- разработать документацию к учебному ресурсу;
- установить вредные психофизиологические факторы, влияющие на

органы зрения специалиста по защите информации, а также определить методы и средства физической культуры, снижающие их воздействие.

1 Анализ требований, применяемых к учебному ресурсу

Согласно техническому заданию на выпускную квалификационную работу разрабатываемый учебный ресурс должен состоять из следующих модулей:

- модуль разграничения доступа, обеспечивающий:
 - аутентификацию пользователей на основе аутентификационной информации (пароля) и логина, принимаемых от внешнего ресурса по стандарту Learning Tools Interoperability (далее — LTI);
 - аутентификацию пользователей на основе аутентификационной информации (пароля) и логина, вводимых пользователем при непосредственном доступе к учебному ресурсу;
 - присвоение пользователям на основе результатов прохождения ими аутентификации одной из следующих ролей: администратор, преподаватель, обучающийся;
 - авторизацию пользователей на выполнение действий на учебном ресурсе в соответствии с присвоенной им ролью;
- модуль управления учебным ресурсом, предоставляющий администратору следующие функции:
 - управление полномочиями доступа пользователей к объектам доступа учебного ресурса: право на чтение (read) и право на запись (write);
 - просмотр журнала событий учебного ресурса;
 - контроль целостности учебного ресурса;
 - блокировка доступа к учебному ресурсу по критериям: IPv4-адрес, IPv6-адрес;
- модуль контроля учебного процесса, предоставляющий преподавателю следующие функции:
 - загрузка учебных материалов на учебный ресурс;

- удаление учебных материалов с учебного ресурса;
- просмотр результата выполнения обучающимися заданий;
- просмотр времени начала и окончания выполнения обучающимися заданий;
- просмотр количества попыток выполнения задания обучающимися;
- модуль интерфейса обучающегося, предоставляющий обучающимся интерфейс для работы с учебными материалами и выполнения заданий на учебном ресурсе;
- модуль обмена данными с внешними ресурсами, обеспечивающий:
 - передачу данных по стандарту LTI внешнему ресурсу, через который пользователи взаимодействуют с учебным ресурсом;
 - приём данных по стандарту LTI от внешнего ресурса, через который пользователи взаимодействуют с учебным ресурсом;
- модуль взаимодействия с базой данных, обеспечивающий:
 - чтение данных из базы данных учебного ресурса посредством выполнения SQL-запросов к базе данных учебного ресурса;
 - изменение данных в базе данных учебного ресурса посредством выполнения SQL-запросов к базе данных учебного ресурса;
 - удаление данных из базы данных учебного ресурса посредством выполнения SQL-запросов к базе данных учебного ресурса;
 - запись новых данных в базу данных учебного ресурса посредством выполнения SQL-запросов к базе данных учебного ресурса;
- модуль регистрации событий, обеспечивающий регистрацию следующих событий информационной безопасности:
 - вход пользователя в систему;
 - выход пользователя из системы;

- начало работы пользователя с объектом учебного ресурса;
- завершение работы пользователя с объектом учебного ресурса;
- модуль обеспечения информационной безопасности, реализующий следующие механизмы защиты:
 - механизма контроля целостности учебного ресурса;
 - механизм блокировки доступа к учебному ресурсу по критериям: IPv4-адрес, IPv6-адрес;
 - механизм анализа загружаемых на учебный ресурс файлов на предмет наличия в них следующих объектов: вредоносное программное обеспечение, деструктивные конструкции;
 - механизм защиты от SQL-инъекций.

Также в соответствии с техническим заданием на выпускную квалификационную работу к разрабатываемому учебному ресурсу применяются следующие технические требования:

- учебный ресурс должен быть размещён на web-сервере под управлением Apache HTTP Server версии не ниже 2.4.38;
- на учебном ресурсе должна использоваться одна из следующих систем управления базами данных (далее — СУБД):
 - MySQL версии не ниже 8.0.18;
 - MariaDB версии не ниже 10.3.22;
- управление СУБД должно осуществляться через приложение phpMyAdmin версии не ниже 4.9.1;
- обмен данными между учебным ресурсом и внешним ресурсом при доступе пользователей к учебному ресурсу через внешние ресурсы должен осуществляться по стандарту LTI;
- учебный ресурс должен быть разработан с использованием

следующих языков программирования и доступных для них библиотек:

- PHP не ниже версии 7.3 для серверной части учебного ресурса;
- SQL, используемый в СУБД MySQL версии не ниже 8.0.18, для работы с базами данных;
- HTML5, CSS3 и JavaScript не ниже версии ES8 (ECMAScript 2017) для клиентской части (интерфейса) учебного ресурса.

Кроме того, разрабатываемый учебный ресурс должен соответствовать требованиям Положения Пензенского государственного университета № 101-06 от 27.09.2018 «Об электронной информационно-образовательной среде университета» [1]. В результате анализа требований, представленных в вышеописанном документе, к разрабатываемому учебному ресурсу применяются следующие требования:

- авторизация пользователей по принципу логин-пароль с использованием веб-интерфейса (требование реализовано в модуле разграничения доступа);
- хранение учётных записей пользователей в базе данных (требование реализовано в модуле взаимодействия с базой данных);
- защита конфиденциальности личной информации пользователей ЭИОС (требование реализовано в модуле обеспечения информационной безопасности);
- разделение прав доступа пользователей системы (требование реализовано в модуле разграничения доступа);
- поддержка проведения занятий и процедур оценки результатов обучения с применением компьютерного тестирования (требование реализовано в модуле контроля учебного процесса).

2 Оценка безопасности технологий интеграции дистанционных ресурсов обучения с системами управления обучением

2.1 Анализ информационных источников, содержащих информацию о современных системах управления обучением и технологиях интеграции с ними внешних ресурсов

2.1.1 Поиск представленных на современном мировом рынке систем управления обучением.

Системы управления обучением на современном мировом рынке подразделяются на два больших класса:

- системы управления обучением с проприетарным программным обеспечением (далее — проприетарное ПО); такие системы управления обучением поставляются в виде облачного сервиса, предоставляя своему клиенту панель управления системой управления обучением для её наполнения контентом; примеры таких систем управления обучением: Adobe Captivate Prime [2], Looor [3], Agylia [4];

- системы управления обучением с открытым программным обеспечением (далее — открытое ПО); такие платформы поставляются в виде файлов с исходными текстами, которые вручную устанавливаются пользователями на их серверы; примеры таких систем управления обучением: Moodle [5], Sakai [6], Canvas [7].

Для того, чтобы полноценно оценить безопасность технологии интеграции дистанционных ресурсов обучения с некоторой системой управления обучением, должна быть возможность исследовать реализацию системы управления обучением путём либо анализа её исходных текстов, либо дизассемблирования/ декомпиляции. Так как современные проприетарные системы управления обучением являются облачным сервисом, соответственно, доступ к реализации таких платформ отсутствует, то значит, не представляется возможности убедиться в безопасности таких ресурсов. Таким образом, в данной работе исследоваться будут только системы управления обучением с

открытым ПО.

В результате анализа систем управления обучением с открытым ПО, представленных в сети Интернет, для исследования были выбраны следующие системы управления обучением:

- Moodle [5];
- Sakai [6];
- Canvas [7];
- Chamilo [8];
- Open edX [9];
- Totara Learn [10].

Вышеописанные системы управления обучением являются наиболее популярными решениями на рынке цифрового обучения из класса систем управления обучением с открытым ПО. Остальные системы управления обучением с открытым ПО являются либо нишевыми и не подходят для нужд университетов и других учебных заведений, либо на данный момент не имеют достаточного функционала для интеграции с ними дистанционных ресурсов обучения.

2.1.2 Описание системы управления обучением Moodle.

Moodle — система управления обучением, распространяемая под лицензией GNU GPL [11]. Используется как платформа для дистанционного обучения в школах, высших учебных заведениях, малых и крупных компаниях и в других организациях.

Согласно исследованиям на рынке систем управления обучением [12], на основе Moodle построено более 50% всех учебных платформ в Европе (включая Российскую Федерацию), Латинской Америке и Океании, а также 25% - в Северной Америке. Большое количество учебных ресурсов российских высших учебных заведений также построено на основе Moodle.

Для интеграции учебных ресурсов Moodle без дополнительных модулей

использует три технологии:

- Aviation Industry Computer-Based Training Committee HTTP-based AICC/CMI Protocol (AICC HACP) [13];
- Sharable Content Object Reference Model версии 1.2 (SCORM 1.2) [14] (при необходимости имеются модули, обновляющие SCORM 1.2 в Moodle до SCORM 2004);
- Learning Tools Interoperability версии 1.3 (LTI 1.3) [15].

Анализ вышеописанных технологий представлен в параграфе 2.2 настоящей работы.

Преимущества Moodle:

- полностью бесплатен;
- регулярные обновления;
- большое активное сообщество, в связи с чем у данной системы управления обучением имеется большое количество модулей (плагинов), существенно расширяющих функционал учебной платформы на основе Moodle;
- устанавливается на Apache HTTP Server и поддерживает такие базы данных, как PostgreSQL, MySQL, MariaDB и другие. Кроме того, имеются программные пакеты с предустановленным веб-сервером и базами данных и предустановленным Moodle;
- имеется приложение для персональных компьютеров и мобильных устройств для удобного доступа к учебной платформе;
- имеется дополнительный модуль, добавляющий Moodle технологию Experience API (xAPI) [16] для интеграции с внешними учебными ресурсами.

Недостатки Moodle:

- отсутствует официальная техническая поддержка; обратиться за помощью можно только к партнёрам проекта Moodle через официальный сайт Moodle;

- несмотря на существующие преднастроенные программные пакеты, Moodle сложен в тонкой настройке под нужды организации, в связи с чем для установки Moodle требуются специалисты;

- при большом количестве пользователей снижается производительность, если система управления обучением использует базы данных, отличные от PostgreSQL и MariaDB.

2.1.3 Описание системы управления обучением Sakai.

Sakai – система управления обучением, распространяемая под лицензией Educational Community License [17]. Используется как платформа для дистанционного обучения преимущественно высшими учебными заведениями.

Согласно исследованиям на рынке систем управления обучением [12], на основе Sakai построено 2% всех учебных платформ в Европе (включая Российскую Федерацию) и Латинской Америке, а также 3% - в Северной Америке.

Для интеграции учебных ресурсов Sakai без дополнительных модулей использует две технологии:

- Sharable Content Object Reference Model версии 2004 (SCORM 2004); данная технология доступна путём установки дополнительного модуля;

- Learning Tools Interoperability версии 1.3 (LTI 1.3).

Анализ вышеописанных технологий представлен в параграфе 2.2 настоящей работы.

Преимущества Sakai:

- бесплатна (но имеются платные дополнительные модули);

- ежегодные обновления;

- ориентация на коллаборативное решение задач студентами: Sakai позволяет для каждой задачи распределить студентов на группы и установить роли студентов в группах;

- возможность масштабирования учебной платформы; в Sakai все

учебные ресурсы создаются в виде поддоменов учебной платформы, из-за чего пользователи учебной платформы распределяются между поддоменами, снижая нагрузку на основной ресурс;

- имеются официальная техническая поддержка и перечень часто задаваемых вопросов;

- имеется приложение для мобильных устройств для удобного доступа к учебной платформе;

- имеется дополнительный модуль, добавляющий Sakai технологию Experience API (xAPI) [16] для интеграции с внешними учебными ресурсами.

Недостаток Sakai — малое общее количество официальных дополнительных модулей, а их функционал в основе своей ориентирован под нужды учебной программы высших учебных заведений Соединённых Штатов Америки; в связи с этим расширение функционала учебной платформы на основе Sakai достигается путём установки сторонних плагинов, что, во-первых, снижает общий уровень информационной безопасности системы, во-вторых, в некоторых случаях может оказаться затруднительным процессом, и в-третьих, может привести к ошибкам в функционировании учебной платформы.

Особенностью Sakai является её архитектура. Система управления обучением Sakai устанавливается на сервер Apache Tomcat под управлением Java и предоставляет пользователям свои ресурсы в виде Java-сервисов; поддерживаемые базы данных — Oracle и MySQL. В связи с этим при принятии решения о построении учебной платформы на основе Sakai следует учитывать, обладают ли необходимыми для этого знаниями специалисты, разрабатывающие учебную платформу.

2.1.4 Описание системы управления обучением Canvas.

Canvas — система управления обучением, распространяемая под лицензией Affero General Public License (AGPLv3) [18]. Ранее была известна под названием Instructure. Используется как платформа для дистанционного

обучения в школах и высших учебных заведениях.

Согласно исследованиям на рынке систем управления обучением [12], на основе Canvas построено около 5% всех учебных платформ в Европе (включая Российскую Федерацию), Латинской Америке и Океании, а также 19% - в Северной Америке. При этом Canvas в 2018 и 2019 годах является самой быстрорастущей по количеству пользователей системой управления обучением. Однако вышеописанная статистика собрана для двух версий Canvas в совокупности — версии с открытым ПО и проприетарной версии. В рамках настоящей работы интересна только версия Canvas с открытым ПО.

Для интеграции учебных ресурсов Canvas версии с открытым ПО использует только Learning Tools Interoperability версии 1.3 (LTI 1.3).

Анализ вышеописанной технологии представлен в параграфе 2.2 настоящей работы.

Преимущества Canvas (версии с открытым ПО):

- бесплатна;
- регулярные обновления;
- быстрорастущее сообщество пользователей, в связи с чем у данной системы управления обучением появляется всё больше дополнительных модулей;
- простая установка и настройка;
- имеется приложение для мобильных устройств для удобного доступа к учебной платформе.

Недостатки Canvas:

- отсутствует официальная техническая поддержка для версии Canvas с открытым ПО;
- часть функционала, доступного в других системах управления обучением бесплатно, в Canvas поставляется в виде проприетарных модулей и только для проприетарной версии Canvas (например, SCORM 2004, сбор

статистики пользователей, проверка ответов студентов на плагиат, голосовые чаты); на момент написания настоящей работы модулей с открытым ПО, разработанных сообществом, недостаточно для достижения системой управления обучением Canvas функционала других систем управления обучением.

2.1.5 Описание системы управления обучением Chamilo.

Chamilo — система управления обучением, распространяемая под лицензией GPLv3 [11]. Chamilo является новой платформой на рынке систем управления обучением и делает акцент на сегмент пользователей развивающихся стран. Chamilo пользуются приблизительно 11 000 000 человек по всему миру.

Для интеграции учебных ресурсов Chamilo без дополнительных модулей использует две технологии:

- Sharable Content Object Reference Model версии 1.2 (SCORM 1.2);
- Learning Tools Interoperability версии 1.1 (LTI 1.1).

Анализ вышеописанных технологий представлен в параграфе 2.2 настоящей работы.

Преимущества Chamilo:

- полностью бесплатна;
- регулярные обновления;
- простая установка и настройка;
- поддержка высоконагруженных учебных платформ: учебная платформа на основе Chamilo, насчитывающая 700 000 уникальных пользователей и построенная на одном физическом сервере, работает без перебоев.

Недостатки Chamilo:

- отсутствует официальная техническая поддержка; обратиться за помощью можно только к партнёрам проекта Chamilo через официальный сайт

Chamilo;

- сообщество пользователей малочисленно;
- значительная часть документации на момент написания настоящей работы представлена только на испанском языке.

2.1.6 Описание системы управления обучением Open edX.

Open edX — система управления обучением, распространяемая под лицензией Affero General Public License (AGPLv3) [18]. Open edX разработана Массачусетским технологическим институтом и набирает большую популярность среди высших учебных заведений Соединённых Штатов Америки, однако на момент написания настоящей работы практически полностью отсутствует на мировом рынке.

Для интеграции учебных ресурсов Open edX без дополнительных модулей использует только Learning Tools Interoperability версии 1.3 (LTI 1.3).

Анализ вышеописанной технологии представлен в параграфе 2.2 настоящей работы.

Open edX распространяется как в виде открытого ПО, так и в виде облачного сервиса. В рамках настоящей работы интересна только версия Open edX с открытым ПО.

Преимущества Open edX (версия с открытым ПО):

- бесплатна;
- регулярные обновления;
- самый обширный функционал среди всех систем управления обучения с открытым ПО;
- быстрорастущее сообщество пользователей, в связи с чем у данной системы управления обучением появляется всё больше дополнительных модулей;
- имеются дополнительные модули, добавляющие в Open edX функционал технологий SCORM версии 1.2 и xAPI;

Недостатки Open edX:

- техническая поддержка представлена только в виде архива ранее заданных вопросов;
- среди всех исследованных в настоящей работе систем управления обучением Open edX является наиболее сложной и трудоёмкой в установке и настройке за счёт большого количества подсистем и нестандартных технологий, с помощью которых Open edX разработан и функционирует (серверная часть Open edX работает на Django – фреймворке языка программирования Python).

2.1.7 Описание системы управления обучением Totara Learn.

Totara Learn — система управления обучением, распространяемая под лицензией General Public License (GPLv3) [11]. Totara Learn разработана на основе Moodle. В то время как Moodle разработан под нужды школ, университетов и других учебных организаций, Totara Learn фокусируется на рынке корпоративного образования. На момент написания настоящей работы у Totara Learn 5 000 000 уникальных пользователей.

Для интеграции учебных ресурсов Totara Learn использует четыре технологии:

- Aviation Industry Computer-Based Training Committee HTTP-based AICC/CMI Protocol (AICC HACP);
- Sharable Content Object Reference Model версии 1.2 (SCORM 1.2);
- Learning Tools Interoperability версии 1.3 (LTI 1.3);
- Experience API (xAPI).

Анализ вышеописанных технологий представлен в параграфе 2.2 настоящей работы.

Преимущества Totara Learn:

- полностью бесплатна;
- регулярные обновления;
- официальная техническая поддержка.

Недостатки Open edX:

- сообщество пользователей по сравнению с другими исследованными в настоящей работе системами управления обучением малочисленно;

- базовый функционал Totara Learn удовлетворяет потребности корпоративного обучения, но не достаточен для построения учебной платформы школ и университетов: отсутствует журнал оценок, нет возможности построить расписание занятий на семестр, студент не имеет возможности связаться с преподавателем и т.д.; на момент написания настоящей работы дополнительные модули для Totara Learn, добавляющие вышеописанный функционал, отсутствуют, в связи с чем такой функционал необходимо будет разрабатывать самостоятельно.

2.1.8 Вывод.

Из информации, полученной об исследуемых системах управления обучением, был сделан вывод, что каждая из шести вышеописанных систем управления обучением может быть использована для построения учебной платформы, поддерживающей интеграцию с дистанционными ресурсами обучения. Однако для безопасной интеграции внешних учебных ресурсов с учебной платформой необходимо сначала исследовать технологии, с помощью которых внешние ресурсы будут интегрироваться с учебной платформой, что и будет проведено в параграфе 2.2 настоящей работы. На основе результата анализа этих технологий будет сделан вывод, какие системы управления обучением могут быть использованы для безопасной интеграции с внешним учебным ресурсом.

В таблице 1 представлена информация о технологиях обмена данными с внешними ресурсами, поддерживаемых исследуемыми системами управления обучением.

Таблица 1 — Информация о технологиях обмена данными с внешними ресурсами, поддерживаемых исследуемыми системами управления обучением

Система управления обучением	Технология интеграции			
	AICC HACP	SCORM	LTI	xAPI
Moodle	Присутствует	Присутствует	Присутствует	Присутствует
Sakai	Отсутствует	Присутствует	Присутствует	Присутствует
Canvas	Отсутствует	Отсутствует	Присутствует	Отсутствует
Chamilo	Отсутствует	Присутствует	Присутствует	Отсутствует
Open edX	Отсутствует	Присутствует	Присутствует	Присутствует
Totara Learn	Присутствует	Присутствует	Присутствует	Присутствует

2.2 Анализ реализации технологий интеграции внешних ресурсов с системами управления обучением с точки зрения информационной безопасности

2.2.1 Анализ технологии AICC HACP.

Aviation Industry Computer-Based Training Committee HTTP-based AICC/CMI Protocol (AICC HACP) – стандарт, разработанный организацией Aviation Industry Computer-Based Training Committee (AICC) для систем обучения специалистов в области авиации, однако данный стандарт быстро набрал популярность за пределами сферы авиации. Является первым стандартом обмена данными систем управления обучением с внешними учебными ресурсами.

AICC HACP использует следующие технологии для своего функционирования:

- HTTP (RFC 7230 [19], 7231 [20], 7232 [21], 7233 [22], 7234 [23], 7235 [24]) или HTTP Over TLS (HTTPS, RFC 2818 [25]);

- JavaScript Application Programming Interface (JS API).

Таким образом, если система управления обучением и внешний учебный ресурс поддерживают HTTPS (порт 443), то обмен данными между ними будет вестись по HTTPS, формирующему криптографически защищённый туннель

для обмена сообщениями, и будет обеспечиваться конфиденциальность передаваемых данных; иначе используется HTTP (в большинстве случаев порт 80) и конфиденциальность передаваемых данных не обеспечивается.

На рисунке 1 представлена схема установления соединения и обмена данными в стандарте AICC HACP.

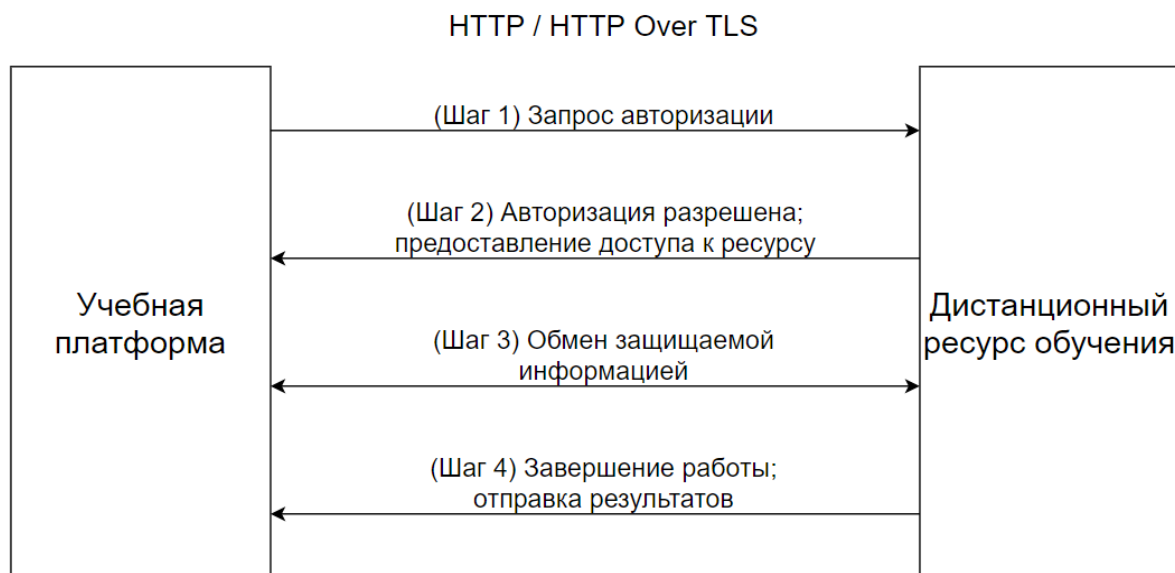


Рисунок 1 — Схема установления соединения и обмена данными в стандарте AICC HACP

На шаге 1 учебная платформа от имени студента отправляет дистанционному ресурсу обучения HTTP-запрос авторизации методом GET для доступа к учебному ресурсу, указывая в параметрах HTTP-запроса уникальный идентификатор сессии (AICC_SID) и URL учебной платформы (AICC_URL).

На шаге 2 дистанционный ресурс обучения завершает идентификацию студента и авторизацию учебной платформы и предоставляет доступ к учебным ресурсам.

На шаге 3 обмен защищаемой информацией между учебной платформой и дистанционным ресурсом обучения выполняется с помощью HTTP-посылок методом POST.

На шаге 4 при завершении работы студента с учебным ресурсом дистанционный ресурс обучения отправляет HTTP-посылку методом POST, содержащий результат прохождения задания студентом, и завершает

соединение с учебной платформой.

Преимущества AICC HACP:

- среди четырёх исследуемых технологий интеграции внешних ресурсов с системами управления обучением AICC HACP использует наименьший объём HTTP-трафика;
- поддерживает HTTP Over TLS;
- поддерживает интеграцию с внешними ресурсами, расположенными на отличном от учебной платформы домене (кроссплатформенное взаимодействие).

Недостатки AICC HACP:

- невозможность наблюдения за процессом выполнения задания студентом; можно узнать только итоговый результат выполненной работы;
- официальная поддержка стандарта завершена в 2014 году;
- не поддерживает современные форматы данных типа JSON и XML;
- защита информации, кроме протокола HTTP Over TLS, отсутствует.

2.2.2 Анализ технологии SCORM.

Sharable Content Object Reference Model (SCORM) – стандарт обмена данными систем управления обучением с внешними учебными ресурсами, разработанный гражданской веткой Министерства обороны Соединённых Штатов Америки в рамках программы по улучшению цифрового образования. Последней версией стандарта является SCORM 2004, однако наиболее популярным является SCORM 1.2, который используется большинством систем управления обучением и который будет рассматриваться в рамках настоящей работы.

SCORM использует следующие технологии для своего функционирования:

- JavaScript Application Programming Interface (JS API);
- Extensible Markup Language (XML, RFC 3470 [26]);

— Adobe Flash Player (RFC 7425 [27]).

Особенностью SCORM является модель взаимодействия студента и учебной платформы с учебным ресурсом. В SCORM система управления обучением и дистанционный ресурс обучения должны находиться на одном домене, что позволяет студенту пройти авторизацию на учебной платформе, а дальше взаимодействовать с внешним учебным ресурсом только в рамках учебной платформы без отправки HTTP-трафика за пределы учебной платформы. Это значительно снижает риск нарушения свойств безопасности защищаемой информации.

На рисунке 2 представлена схема установления соединения и обмена данными в стандарте SCORM.



Рисунок 2 — Схема установления соединения и обмена данными в стандарте SCORM

На шаге 1 учебная платформа от имени студента отправляет дистанционному ресурсу обучения HTTP-запрос авторизации методом GET для доступа к учебному ресурсу.

На шаге 2 дистанционный ресурс обучения запрашивает с помощью HTTP-запроса методом GET у учебной платформы идентификационную информацию о студенте.

На шаге 3 учебная платформа с помощью HTTP-посылки методом POST отправляет дистанционному ресурсу обучения идентификационную информацию студента.

На шаге 4 дистанционный ресурс обучения завершает идентификацию студента и авторизацию учебной платформы и предоставляет доступ к учебным ресурсам.

На шаге 5 обмен защищаемой информацией между учебной платформой и дистанционным ресурсом обучения выполняется с помощью HTTP-посылок методом POST.

На шаге 6 при завершении работы студента с учебным ресурсом дистанционный ресурс обучения отправляет HTTP-посылку методом POST, содержащий результат прохождения задания студентом, и завершает соединение с учебной платформой.

Преимущества SCORM:

- отсутствует HTTP-трафик, выходящий за пределы учебной платформы;
- возможность хранения дистанционных ресурсов обучения в ZIP-архиве с паролем любой сложности.

Недостатки SCORM:

- не поддерживает HTTP Over TLS; даже если учебная платформа поддерживает HTTP Over TLS, обмен данными с дистанционным ресурсом обучения будет вестись через протокол HTTP;
- дистанционный ресурс обучения должен находиться на одном с учебной платформой домене;
- основан на Adobe Flash Player, официальная поддержка которого

заканчивается 31.12.2020 года;

- невозможность наблюдения за процессом выполнения задания студентом; можно узнать только итоговый результат выполненной работы и время, затраченное на выполнение задания;

- последнее обновление стандарта было в 2009 году.

2.2.3 Анализ технологии LTI.

Learning Tools Interoperability (LTI) – стандарт обмена данными между внешними ресурсами и учебной платформой, разработанный IMS Global Learning Consortium. Позволяет интегрировать внешние ресурсы в учебный процесс платформы, создавая для пользователей учебной платформы ощущение работы с внутренним ресурсом платформы.

Стандарт LTI базируется на следующих технологиях:

- HTTP Over TLS (HTTPS, RFC 2818) – стандарт установления HTTP соединения по протоколу TLS;

- OAuth 2.0 – стандарт (фреймворк) авторизации сторонних лиц для доступа к защищаемым ресурсам (RFC 6749) [28];

- OpenID Connect (далее – OIDC) – протокол идентификации, позволяющий Клиенту подтвердить подлинность пользователя с помощью Сервера авторизации [29];

- JavaScript Application Programming Interface (JS API);

- JSON Web Token (далее – JWT) – протокол передачи данных в формате JSON (RFC 7519) [30].

Все сообщения между учебной платформой и внешним ресурсом передаются по протоколу HTTPS, формирующему криптографически защищённый туннель для обмена сообщениями.

Все сообщения между учебной платформой и внешним ресурсом соответствуют стандарту OAuth 2.0, а именно:

- в поле HTTP-заголовка Authorization указывается OAuth 2.0;

— все сообщения от учебной платформы содержат Ключ потребителя – произвольно выбранную последовательность символов, позволяющую внешнему ресурсу идентифицировать учебную платформу;

— все сообщения между учебной платформой и внешним ресурсом дополняются криптографической хеш-функцией, вычисленной на секретном ключе, о котором учебная платформа и внешний ресурс заранее договариваются; вычисление криптографической хеш-функции выполняется по алгоритмам HMAC-SHA1 и HMAC-SHA256.

На рисунке 3 представлена схема установления соединения и обмена данными в стандарте LTI.

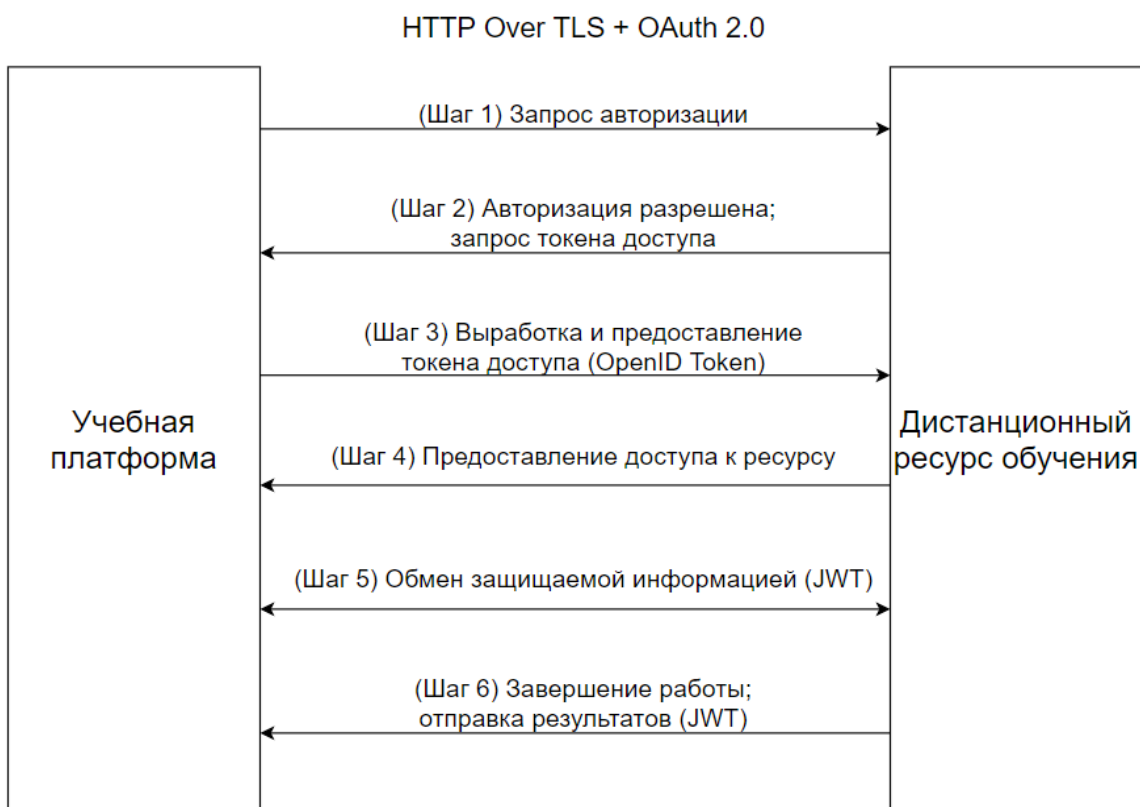


Рисунок 3 — Схема установления соединения и обмена данными в стандарте LTI

На шаге 1 учебная платформа отправляет внешнему ресурсу запрос авторизации для доступа к защищаемым ресурсам.

На шаге 2 внешний ресурс запрашивает у учебной платформы токен доступа. Токен доступа выдаётся Сервером авторизации, роль которого в

стандарте LTI выполняет учебная платформа.

На шаге 3 учебная платформа вырабатывает токен доступа и отправляет его внешнему ресурсу. При этом токен доступа сформирован в формате OpenID Token. Данный токен является аналогичным JWT, но содержит в себе информацию для идентификации студента внешним ресурсом.

На шаге 4 завершается идентификация студента и авторизация учебной платформы и предоставляется доступ к внешним учебным ресурсам.

На шагах 5 и 6 обмен защищаемой информацией выполняется с помощью JWT. Данные токены содержат в себе криптографическую хеш-функцию, вычисляемую по алгоритмам из RFC 7518 [31] (чаще всего используется HMAC-SHA256).

Преимущества LTI:

- поддерживает HTTP Over TLS;
- поддерживает интеграцию с внешними ресурсами, расположенными на отличном от учебной платформы домене (кроссплатформенное взаимодействие);
- передаваемые сообщения содержат имитовставку, в том числе и сообщения с защищаемой информацией;
- присутствуют механизмы идентификации и аутентификации пользователя;
- преподаватель может наблюдать за процессом выполнения задания студентом;
- управление доступом на основе ролей: права доступа к учебному курсу меняются в зависимости от контекста (роли пользователя).

Недостатки LTI:

- в стандарте LTI имеется возможность передачи защищаемой информации о студенте различного рода, в связи с чем внешний учебный ресурс может запрашивать у учебной платформы информацию о студенте,

которую передавать не следует; при настройке LTI на учебной платформе важно чётко указать, какая защищаемая информация будет передаваться внешним учебным ресурсам;

- некорректная обработка внешним ресурсом контекста пользователя может привести к несанкционированному повышению его привилегий; например, если пользователь сначала зашёл на внешний ресурс с одной учебной платформы в роли преподавателя, а с другой учебной платформы — в роли студента, то при некорректной обработке контекста пользователь будет иметь права доступа преподавателя в обеих сессиях.

2.2.4 Анализ технологии xAPI.

Experience API (xAPI, Tin Can API) – стандарт обмена данными между внешними ресурсами и учебной платформой, разработанный Rustici Software. Позволяет интегрировать внешние ресурсы в учебный процесс платформы, а также устанавливать взаимодействие между двумя учебными платформами.

xAPI возник как логическое продолжение SCORM, учитывая его преимущества и недостатки, а также пожелания сообщества. Важным отличием xAPI от SCORM является его архитектура — xAPI вместо Adobe Flash Player использует REST архитектуру с JSON в качестве формата данных и JavaScript – для своего функционирования в браузере. Кроме того, вся информация о процессе обучения собирается в отдельном хранилище учебных записей (Learning Record Store (LRS)), что позволяет собирать значительно больше статистики об обучающихся и учебном курсе, чем в SCORM.

Стандарт xAPI базируется на следующих технологиях:

- HTTP (RFC 7230, 7231, 7232, 7233, 7234, 7235) или HTTP Over TLS (HTTPS, RFC 2818);
- OAuth 2.0 – стандарт (фреймворк) авторизации сторонних лиц для доступа к защищаемым ресурсам (RFC 6749);
- OpenID Connect (далее – OIDC) – протокол идентификации,

позволяющий Клиенту подтвердить подлинность пользователя с помощью Сервера авторизации;

- JavaScript Application Programming Interface (JS API);
- JSON Web Token (далее – JWT) – протокол передачи данных в формате JSON (RFC 7519).

Все сообщения между учебной платформой и внешним ресурсом соответствуют стандарту OAuth 2.0.

На рисунке 4 представлена схема установления соединения и обмена данными в стандарте xAPI.

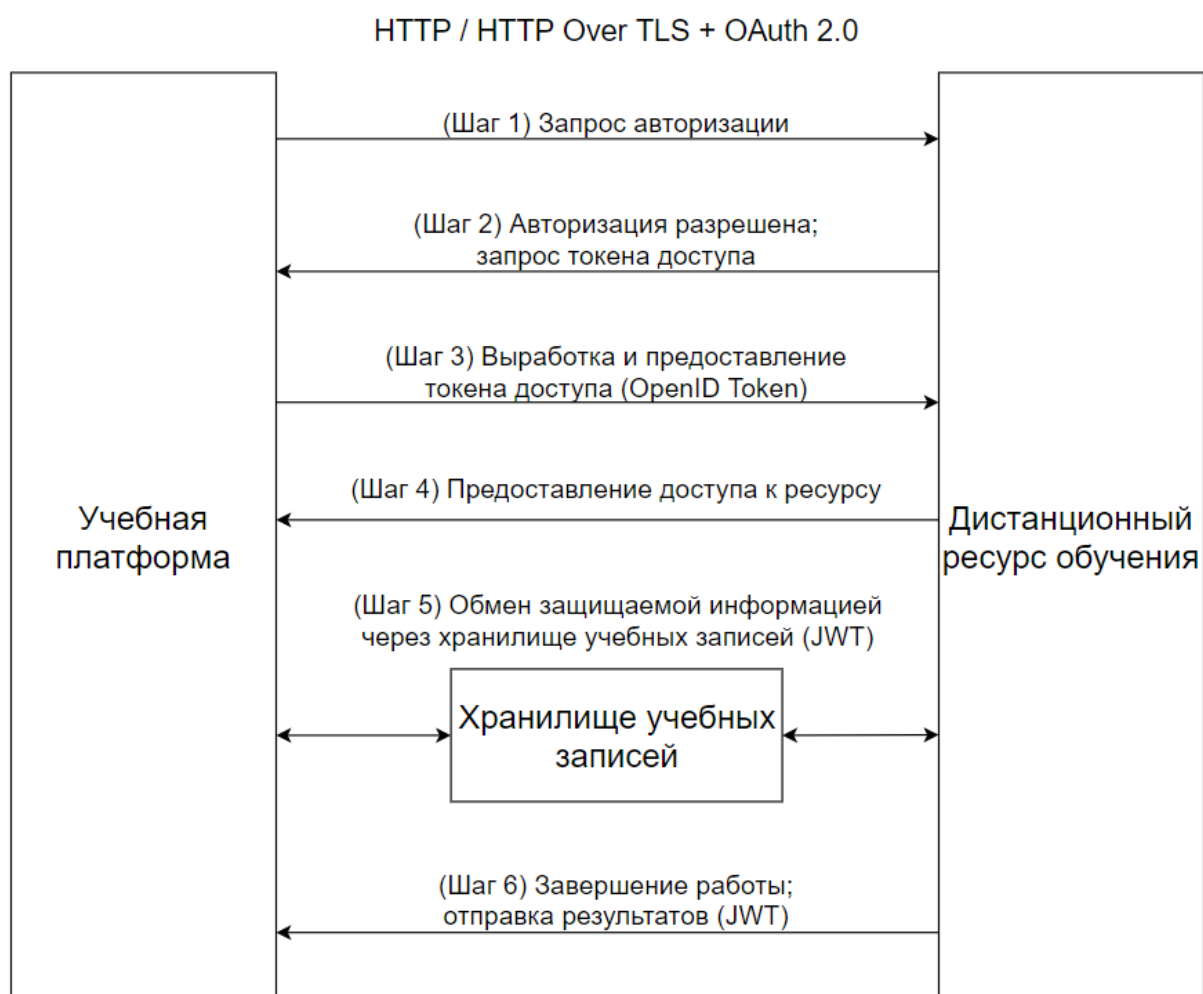


Рисунок 4 — Схема установления соединения и обмена данными в стандарте xAPI

На шаге 1 учебная платформа отправляет внешнему ресурсу запрос авторизации для доступа к защищаемым ресурсам.

На шаге 2 внешний ресурс запрашивает у учебной платформы токен доступа. Токен доступа выдаётся Сервером авторизации, роль которого в стандарте xAPI выполняет учебная платформа.

На шаге 3 учебная платформа вырабатывает токен доступа и отправляет его внешнему ресурсу. При этом токен доступа сформирован в формате OpenID Token. Данный токен является аналогичным JWT, но содержит в себе информацию для идентификации студента внешним ресурсом.

На шаге 4 завершается идентификация студента и авторизация учебной платформы и предоставляется доступ к внешним учебным ресурсам.

На шаге 5 обмен защищаемой информацией выполняется с помощью JWT через хранилище учебных записей. Данные токены содержат в себе криптографическую хеш-функцию, вычисляемую по алгоритмам из RFC 7518 (чаще всего используется HMAC-SHA256).

На шаге 6 обмен защищаемой информацией выполняется с помощью JWT. Данные токены содержат в себе криптографическую хеш-функцию, вычисляемую по алгоритмам из RFC 7518 (чаще всего используется HMAC-SHA256).

Преимущества xAPI:

- поддерживает HTTP Over TLS;
- внешние учебные ресурсы могут быть сформированы не только в виде веб-ресурса, но также и в качестве приложений для персональных компьютеров и мобильных устройств;
- в связи с тем, что данные о прогрессе выполнения заданий хранятся в хранилище учебных записей, то студент может выполнять задания в приложении, установленном на его устройстве, без доступа к сети Интернет; когда доступ к сети Интернет восстановится, то данные о выполненном задании будут загружены в хранилище учебных записей;
- поддерживает интеграцию с внешними ресурсами,

расположенными на отличном от учебной платформы домене (кроссплатформенное взаимодействие);

- передаваемые сообщения содержат имитовставку, в том числе и сообщения с защищаемой информацией;

- присутствуют механизмы идентификации и аутентификации пользователя;

- преподаватель может наблюдать за процессом выполнения задания студентом;

- управление доступом на основе ролей: права доступа к учебному курсу меняются в зависимости от контекста (роли пользователя).

Недостатки xAPI:

- xAPI даёт большую свободу его реализации разработчикам, в связи с чем для подключения внешнего учебного ресурса к учебной платформе необходимо сначала связаться с разработчиком внешнего ресурса и узнать, какие данные его ресурс использует на входе и какие данные возвращает;

- статистика об обучающихся и учебном курсе значительно шире, чем в SCORM, но значительно уступает сбору статистики в LTI;

- некорректная обработка внешним ресурсом контекста пользователя может привести к несанкционированному повышению его привилегий; например, если пользователь сначала зашёл на внешний ресурс с одной учебной платформы в роли преподавателя, а с другой учебной платформы — в роли студента, то при некорректной обработке контекста пользователь будет иметь права доступа преподавателя в обеих сессиях;

- на момент написания настоящей работы не имеет широкого распространения среди учебных ресурсов.

2.2.5 Вывод.

В AICC НАСР обеспечивается только свойство конфиденциальности защищаемой информации при её передаче между учебной платформой и

внешним ресурсом посредством протокола HTTP Over TLS (если таковой используется). Кроме того, обмен защищаемой информацией выполняется с помощью HTTP-посылок методом POST без использования каких-либо мер защиты, а метод POST сам по себе не обеспечивает никакой дополнительной защиты. Также авторизация выполняется с помощью HTTP-запроса методом GET, который уязвим для сетевых атак, особенно для атак типа «человек посередине».

В SCORM отсутствуют любые методы защиты информации; так как обмен данными учебной платформы и студента с дистанционным ресурсом обучения происходит на едином домене, то информационная безопасность защищаемой информации полностью зависит от информационной безопасности учебной платформы. Таким образом, при разработке внешнего ресурса обучения отсутствует возможность внедрения мер защиты информации. Кроме того, для добавления внешнего ресурса в учебную программу преподаватель должен сначала обратиться к администратору учебной платформы, а последний должен затем получить исходные тексты от автора внешнего ресурса и разместить их в учебной платформе, что часто не представляется возможным.

В LTI и xAPI конфиденциальность защищаемой информации при её передаче между учебной платформой и внешним ресурсом обеспечивается протоколом HTTP Over TLS, её целостность – криптографической хеш-функцией в стандарте OAuth 2.0 и протоколе JWT, а её аутентичность – криптографической хеш-функцией в стандарте OAuth 2.0 и протоколе JWT, а также протоколом OIDC.

Таким образом, слабые защитные меры в стандартах AICC HACP и SCORM не позволяют на их основе разрабатывать безопасный обмен данными между учебной платформой и дистанционным ресурсом обучения. Также стандарты AICC HACP и SCORM являются устаревшими, а дальнейшая стабильная работа SCORM при скором окончании поддержки браузерами и компанией Adobe технологии Adobe Flash Player не гарантируется.

Стандарты LTI и xAPI с точки зрения реализации защитных механизмов идентичны и в обоих стандартах реализовано достаточно мер информационной безопасности для безопасной интеграции в учебный процесс дистанционных ресурсов обучения. Однако отсутствие стандартизированной структуры данных при их обмене между учебной платформой и внешним ресурсом, поддержка сторонних приложений, устанавливаемых на устройства студентов, в качестве учебных ресурсов, а также необходимость формирования и обеспечения информационной безопасности отдельного хранилища учебных записей (по сути, базы данных) создают необходимость в разработке дополнительных мер защиты для реализации безопасного обмена данными между учебной платформой и учебным ресурсом через xAPI по сравнению с LTI.

Как итог, был сделан вывод, что стандарты LTI и xAPI могут использоваться как основа для построения безопасного обмена данными между учебной платформой и дистанционным ресурсом обучения, однако в ходе исследований, проведенных в настоящей работе, было определено, что стандарт LTI предоставляет больше функционала под нужды учебных заведений России, является более распространённым и более надёжным стандартом обмена данными между учебной платформой и дистанционным ресурсом обучения, чем xAPI. А так как LTI поддерживается всеми исследованными системами управления обучением, то они все могут быть использованы для безопасной интеграции с внешним учебным ресурсом.

Так как разрабатываемый в рамках выпускной квалификационной работы учебный ресурс должен обеспечивать обмен данными с электронной информационно-образовательной средой Пензенского государственного университета, которая построена на основе Moodle, то было принято решение при разработке учебного ресурса также использовать платформу Moodle. Однако с разрабатываемым учебным ресурсом сможет взаимодействовать любая платформа, поддерживающая стандарт LTI.

3 Проектирование учебного ресурса

3.1 Проектирование архитектуры учебного ресурса

После выбора технологий, подходящих для разработки защищённого учебного ресурса, была разработана архитектура учебного ресурса. Архитектура учебного ресурса представлена на рисунке 5.

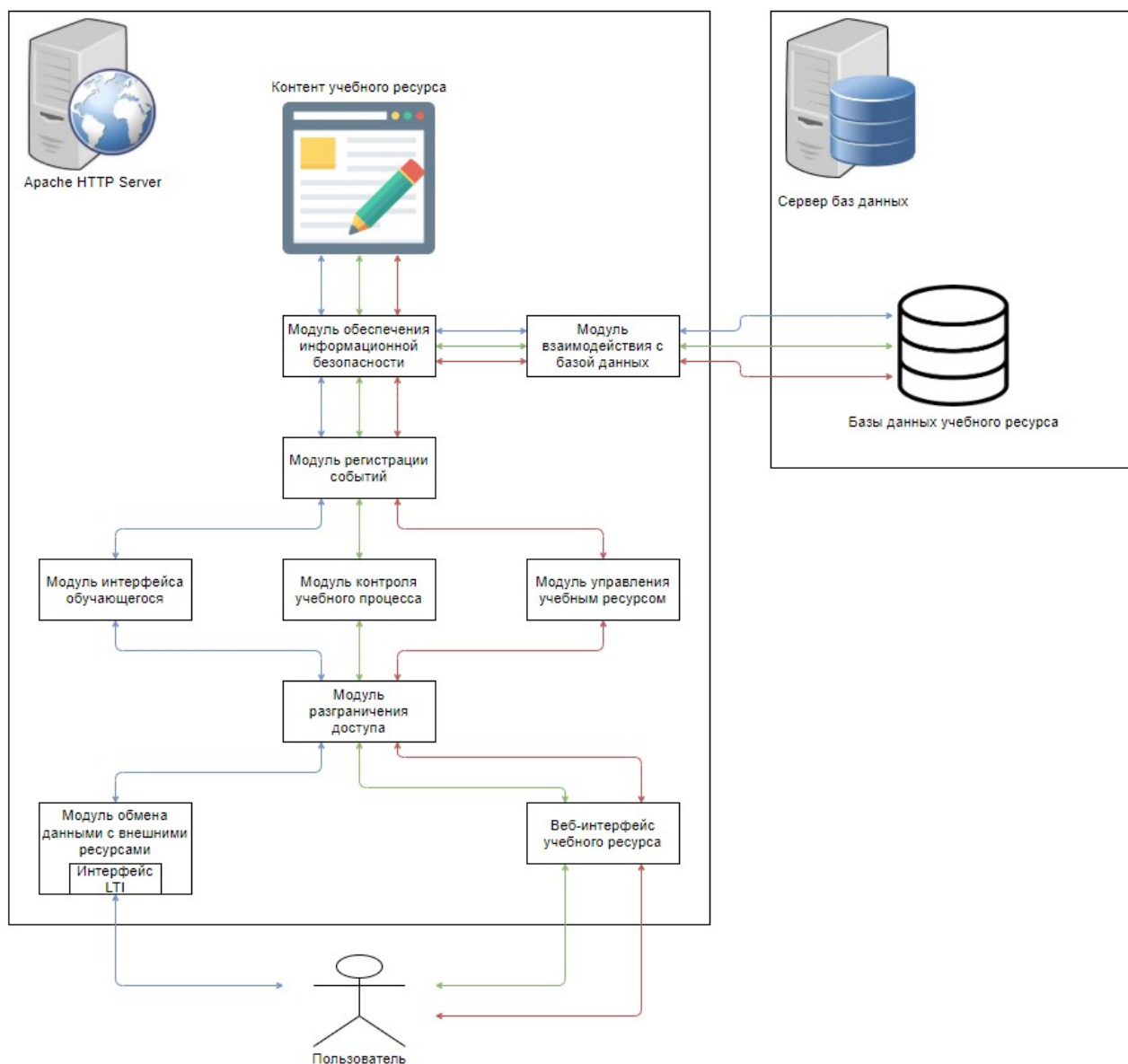


Рисунок 5 — Архитектура учебного ресурса

На рисунке 5 представлены следующие потоки данных:

- красной линией — поток данных между администратором учебного ресурса и учебным ресурсом;
- зелёной линией — поток данных между преподавателем и учебным

ресурсом;

— синей линией — поток данных между студентом и учебным ресурсом.

Исходные тексты учебного ресурса будут располагаться на веб-сервере под управлением Apache HTTP Server, а базы данных учебного ресурса будут располагаться на сервере базы данных (сервер баз данных поддерживает базы данных MySQL и MariaDB).

Разрабатываемый учебный ресурс будет построен на основе платформы Moodle, но будет использоваться её минимальная версия, необходимая для корректной работы ресурса. По мере необходимости в учебный ресурс могут добавляться дополнительные плагины из официального GitHub-репозитория проекта Moodle [32], которые реализуют требования, поставленные в техническом задании к выпускной квалификационной работе.

3.2 Проектирование модуля разграничения доступа

В соответствии с техническим заданием на выпускную квалификационную работу модуль разграничения доступа должен обеспечивать:

— аутентификацию пользователей на основе аутентификационной информации (пароля) и логина, принимаемых от внешнего ресурса по стандарту Learning Tools Interoperability (далее — LTI);

— аутентификацию пользователей на основе аутентификационной информации (пароля) и логина, вводимых пользователем при непосредственном доступе к учебному ресурсу;

— присвоение пользователям на основе результатов прохождения ими аутентификации одной из следующих ролей: администратор, преподаватель, обучающийся;

— авторизацию пользователей на выполнение действий на учебном ресурсе в соответствии с присвоенной им ролью.

Кроме того, в Moodle при работе с LTI имеется уязвимость в виде несанкционированного повышения привилегий пользователей, подключившихся через интерфейс LTI. Подробное описание данной уязвимости представлено в пункте 4.1.2 настоящей работы. Модуль разграничения доступа решает эту проблему.

На рисунке 6 представлен алгоритм работы модуля разграничения доступа.

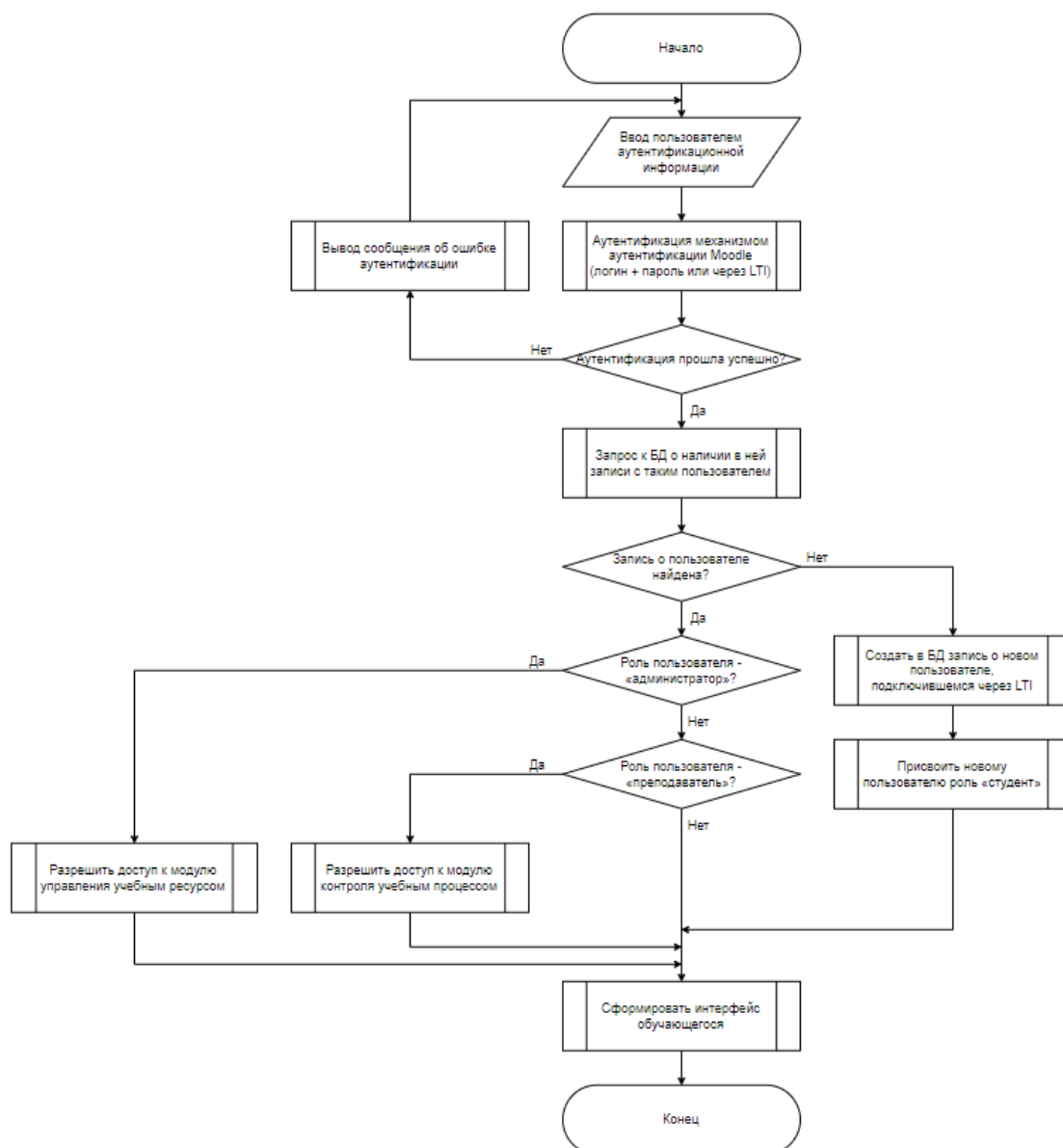


Рисунок 6 — Алгоритм работы модуля разграничения доступа

Так как к учебному ресурсу можно подключаться как через веб-интерфейс, так и через интерфейс LTI, то модуль разграничения доступа

имеет две точки входа для перехвата аутентификационной информации как с формы ввода логина и пароля, так и из интерфейса LTI. Аутентификационную информацию, приходящую в POST-запросах, обрабатывает модуль обмена данными с внешними ресурсами, а обработанные данные передаёт модулю разграничения доступа.

После назначения пользователю его роли модуль разграничения доступа настраивает его рабочую среду в зависимости от роли.

3.3 Проектирование модуля управления учебным ресурсом

В соответствии с техническим заданием на выпускную квалификационную работу модуль управления учебным ресурсом должен обеспечивать:

- управление полномочиями доступа пользователей к объектам доступа учебного ресурса: право на чтение (read) и право на запись (write);
- просмотр журнала событий учебного ресурса;
- контроль целостности учебного ресурса;
- блокировка доступа к учебному ресурсу по критериям: IPv4-адрес, IPv6-адрес.

Так как задачи, выполняемые модулем управления учебным ресурсом, решаются отдельно друг от друга, то ниже представлены блок-схемы для каждой отдельной задачи модуля управления учебным ресурсом.

На рисунке 7 представлен алгоритм работы модуля управления учебным ресурсом для управления полномочиями доступа пользователей.

На рисунке 8 представлен алгоритм работы модуля управления учебным ресурсом для просмотра журнала событий учебного ресурса.

На рисунке 9 представлен алгоритм работы модуля управления учебным ресурсом для контроля целостности учебного ресурса.

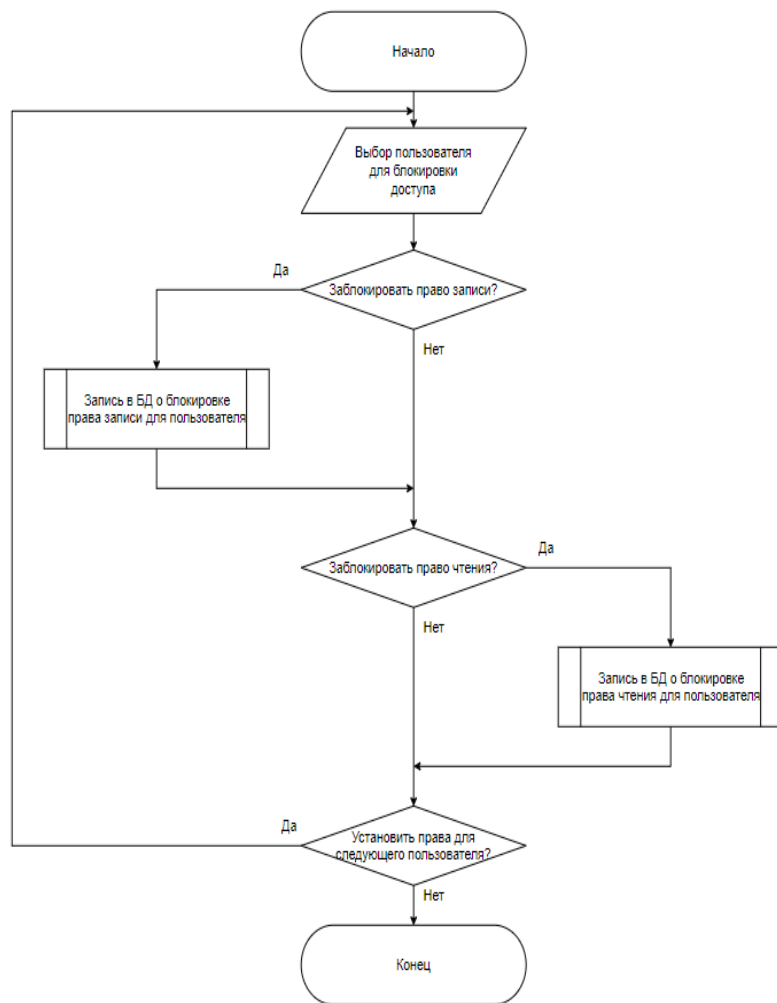


Рисунок 7 — Алгоритм работы модуля управления учебным ресурсом для управления полномочиями доступа пользователей

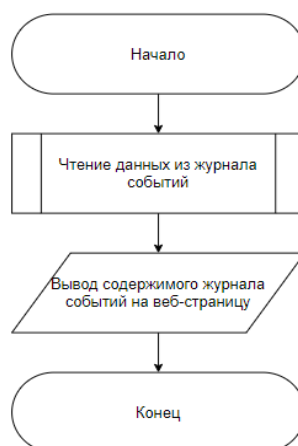


Рисунок 8 — Алгоритм работы модуля управления учебным ресурсом для просмотра журнала событий учебного ресурса

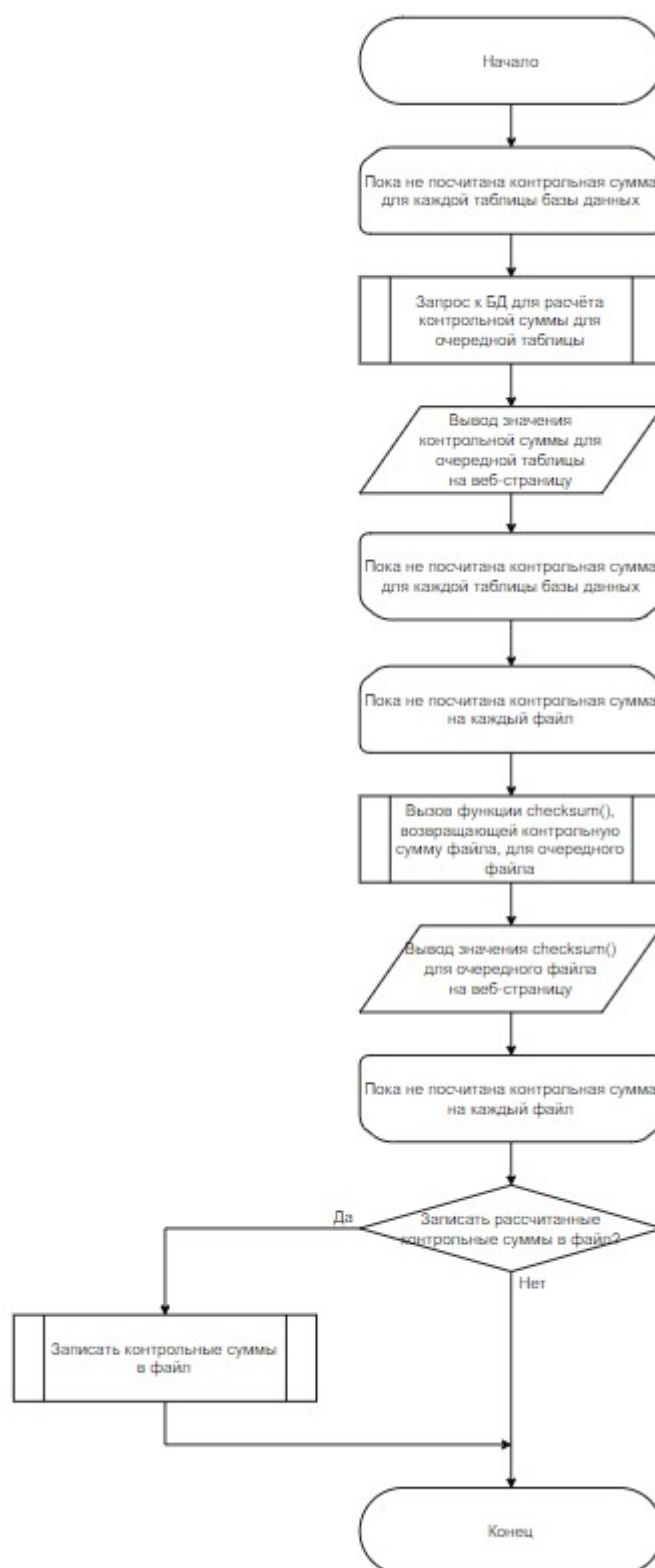


Рисунок 9 — Алгоритм работы модуля управления учебным ресурсом для контроля целостности учебного ресурса

На рисунке 10 представлен алгоритм работы модуля управления учебным ресурсом для блокировки доступа к учебному ресурсу.

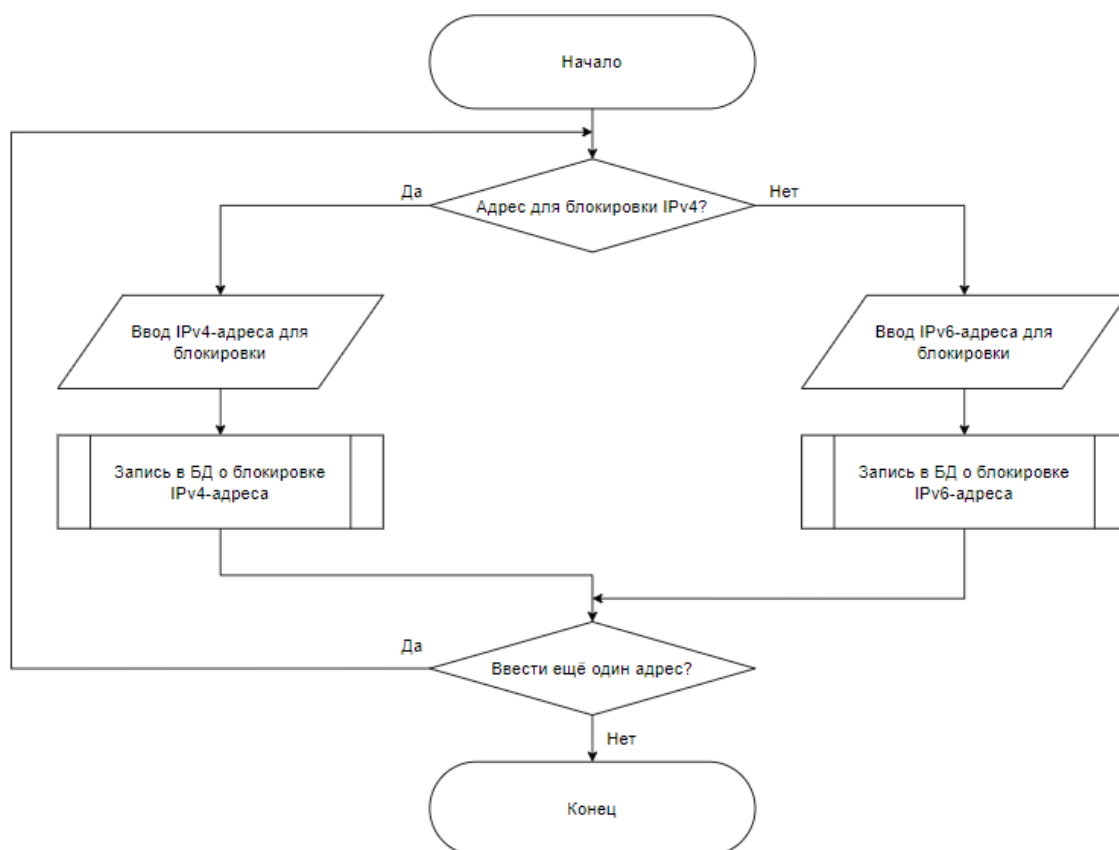


Рисунок 10 — Алгоритм работы модуля управления учебным ресурсом для блокировки доступа к учебному ресурсу

Проверка прав пользователя на чтение и запись реализована в модуле обеспечения информационной безопасности.

3.4 Проектирование модуля контроля учебного процесса

В соответствии с техническим заданием на выпускную квалификационную работу модуль контроля учебного процесса должен обеспечивать:

- загрузку учебных материалов на учебный ресурс;
- удаление учебных материалов с учебного ресурса;
- просмотр результата выполнения обучающимися заданий;
- просмотр времени начала и окончания выполнения обучающимися заданий;
- просмотр количества попыток выполнения задания обучающимися.

Так как задачи, выполняемые модулем контроля учебного процесса,

решаются отдельно друг от друга, то ниже представлены блок-схемы для каждой отдельной задачи модуля контроля учебного процесса.

На рисунке 11 представлен алгоритм работы модуля контроля учебного процесса для загрузки учебных материалов на учебный ресурс.

На рисунке 12 представлен алгоритм работы модуля контроля учебного процесса для удаления учебных материалов с учебного ресурса.

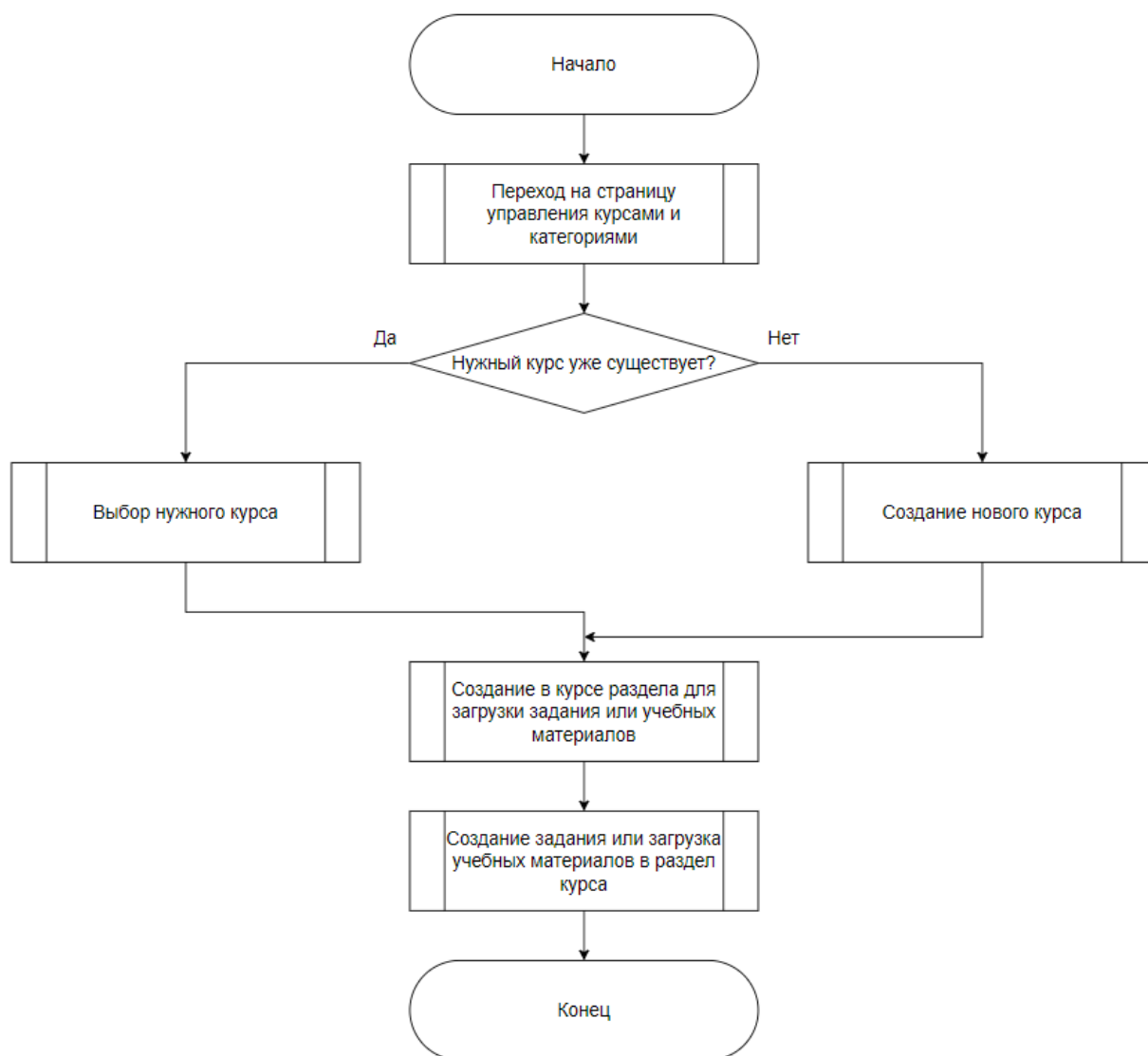


Рисунок 11 — Алгоритм работы модуля контроля учебного процесса для загрузки учебных материалов на учебный ресурс

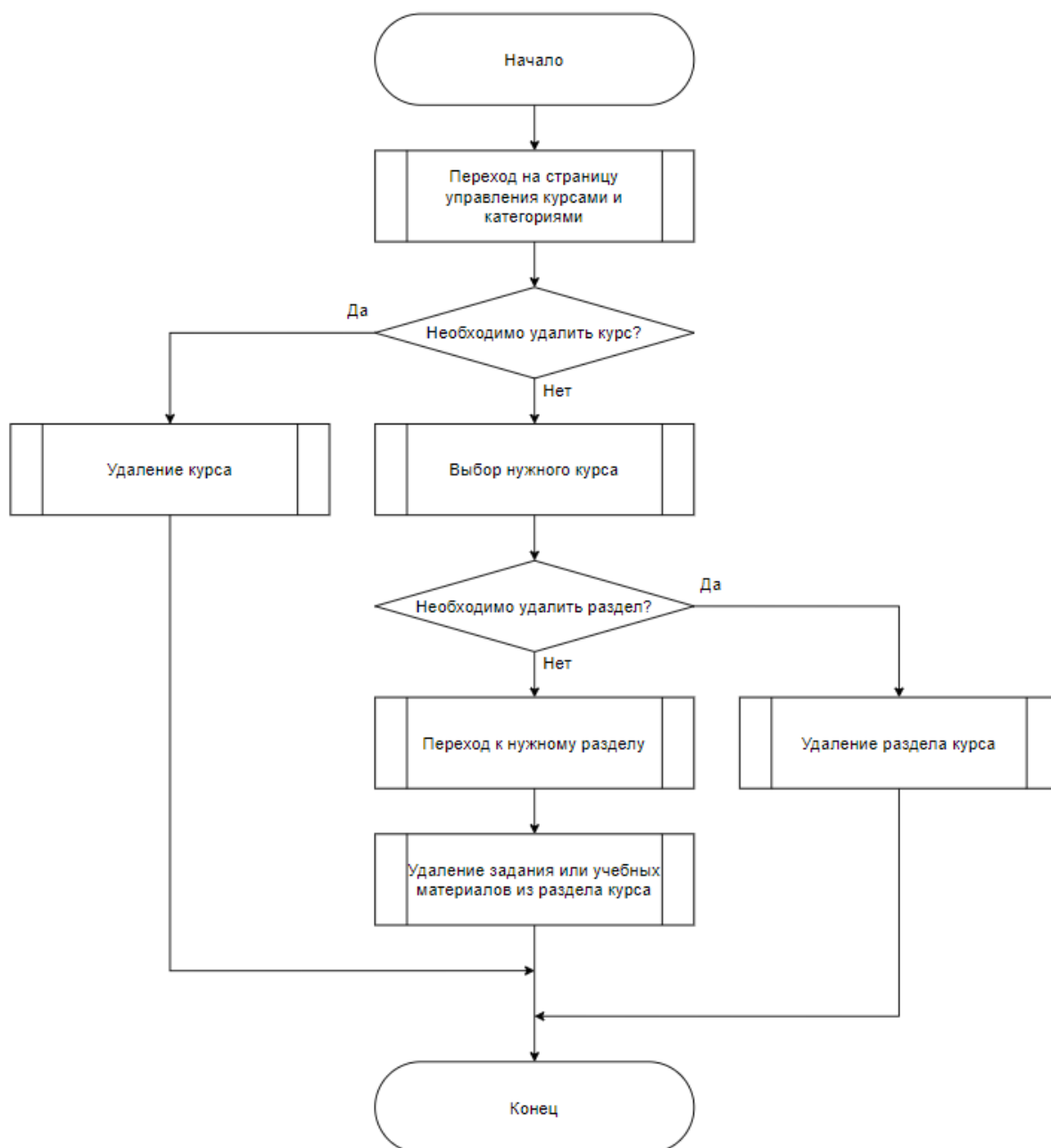


Рисунок 12 — Алгоритм работы модуля контроля учебного процесса для удаления учебных материалов с учебного ресурса

На рисунке 13 представлен алгоритм работы модуля контроля учебного процесса для просмотра результата выполнения обучающимися заданий, времени начала и окончания выполнения обучающимися заданий и количества попыток выполнения задания обучающимися.

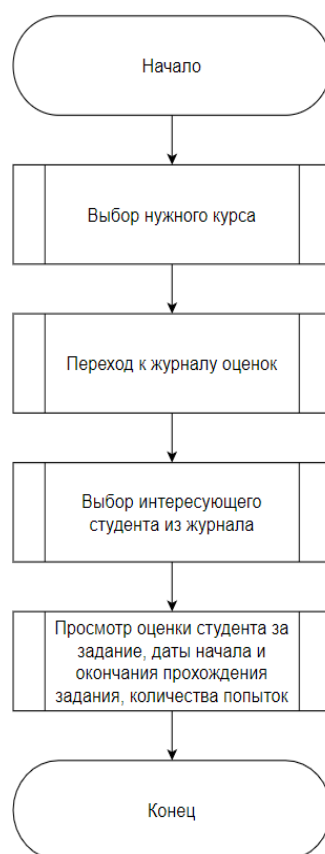


Рисунок 13 — Алгоритм работы модуля контроля учебного процесса для просмотра результата выполнения обучающимися заданий, времени начала и окончания выполнения обучающимися заданий и количества попыток выполнения задания обучающимися

3.5 Проектирование модуля интерфейса обучающегося

В соответствии с техническим заданием на выпускную квалификационную работу модуль интерфейса обучающегося должен предоставлять обучающимся интерфейс для работы с учебными материалами и выполнения заданий на учебном ресурсе. Таким образом, модуль интерфейса обучающегося включает в себя настроенный графический интерфейс учебного ресурса, задания и учебные материалы, выложенные преподавателями.

В рамках модуля интерфейса обучающегося было разработано задание «Исследование механизмов обеспечения информационной безопасности реляционных баз данных в языке программирования SQL».

3.6 Проектирование модуля обмена данными с внешними ресурсами

В соответствии с техническим заданием на выпускную

квалификационную работу модуль обмена данными с внешними ресурсами должен обеспечивать:

На рисунке 14 представлен алгоритм работы модуля обмена данными с внешними ресурсами.

Рисунок 14 — Алгоритм работы модуля обмена данными с внешними ресурсами

В соответствии с техническим заданием на выпускную квалификационную работу модуль взаимодействия с базой данных должен обеспечивать:

- изменение данных в базе данных учебного ресурса посредством выполнения SQL-запросов к базе данных учебного ресурса;
- удаление данных из базы данных учебного ресурса посредством выполнения SQL-запросов к базе данных учебного ресурса;
- запись данных в базу данных учебного ресурса посредством выполнения SQL-запросов к базе данных учебного ресурса.

На рисунке 15 представлен алгоритм работы модуля взаимодействия с базой данных.

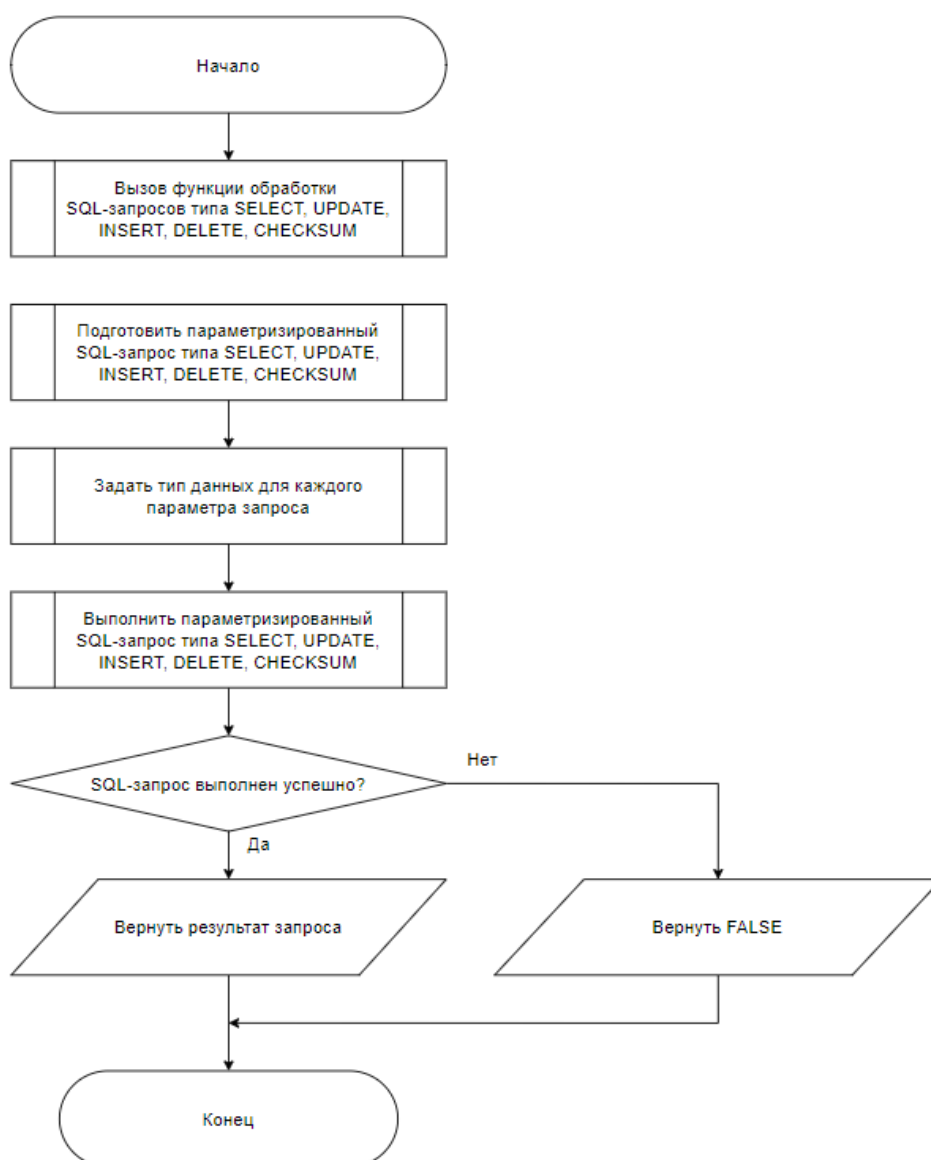


Рисунок 15 — Алгоритм работы модуля взаимодействия с базой данных

3.8 Проектирование модуля регистрации событий

В соответствии с техническим заданием на выпускную квалификационную работу модуль регистрации событий должен обеспечивать регистрацию следующих событий:

- вход пользователя в систему;
- выход пользователя из системы;
- начало работы пользователя с объектом учебного ресурса;
- завершение работы пользователя с объектом учебного ресурса.

Модуль регистрации событий собирает данные из модуля управления учебным ресурсом, модуля контроля учебного процесса и модуля интерфейса обучающегося.

На рисунке 16 представлен алгоритм работы модуля регистрации событий.

3.9 Проектирование модуля обеспечения информационной безопасности

В соответствии с техническим заданием на выпускную квалификационную работу модуль обеспечения информационной безопасности должен реализовывать:

- механизм контроля целостности учебного ресурса;
- механизм блокировки доступа к учебному ресурсу по критериям: IPv4-адрес, IPv6-адрес;
- механизм анализа загружаемых на учебный ресурс файлов на предмет наличия в них следующих объектов: вредоносное программное обеспечение, деструктивные конструкции;
- механизм защиты от SQL-инъекций.

Дополнительно к вышеописанным механизмам модуль обеспечения информационной безопасности реализует механизм проверки полномочий доступа пользователей.

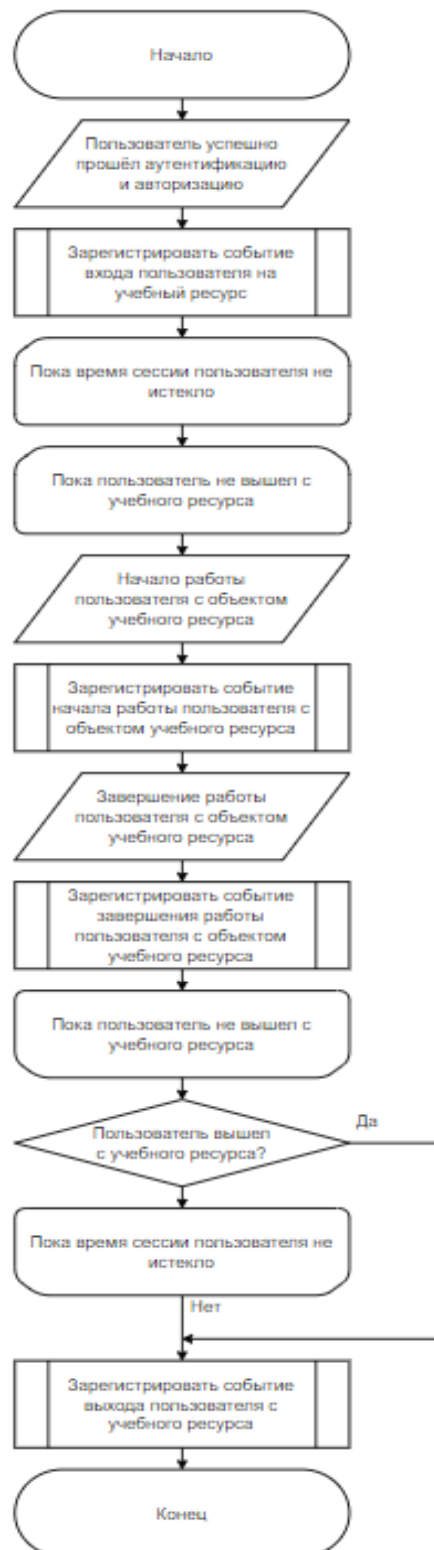


Рисунок 16 — Алгоритм работы модуля регистрации событий

Алгоритм работы механизма контроля целостности учебного ресурса представлен на рисунке 9.

На рисунке 17 представлен алгоритм работы механизма проверки полномочий доступа пользователей.

На рисунке 18 представлен алгоритм работы механизма блокировки доступа к учебному ресурсу по IP-адресу.

На рисунке 19 представлен алгоритм работы механизма анализа загружаемых на учебный ресурс файлов.

На рисунке 20 представлен алгоритм работы механизма защиты от SQL-инъекций.

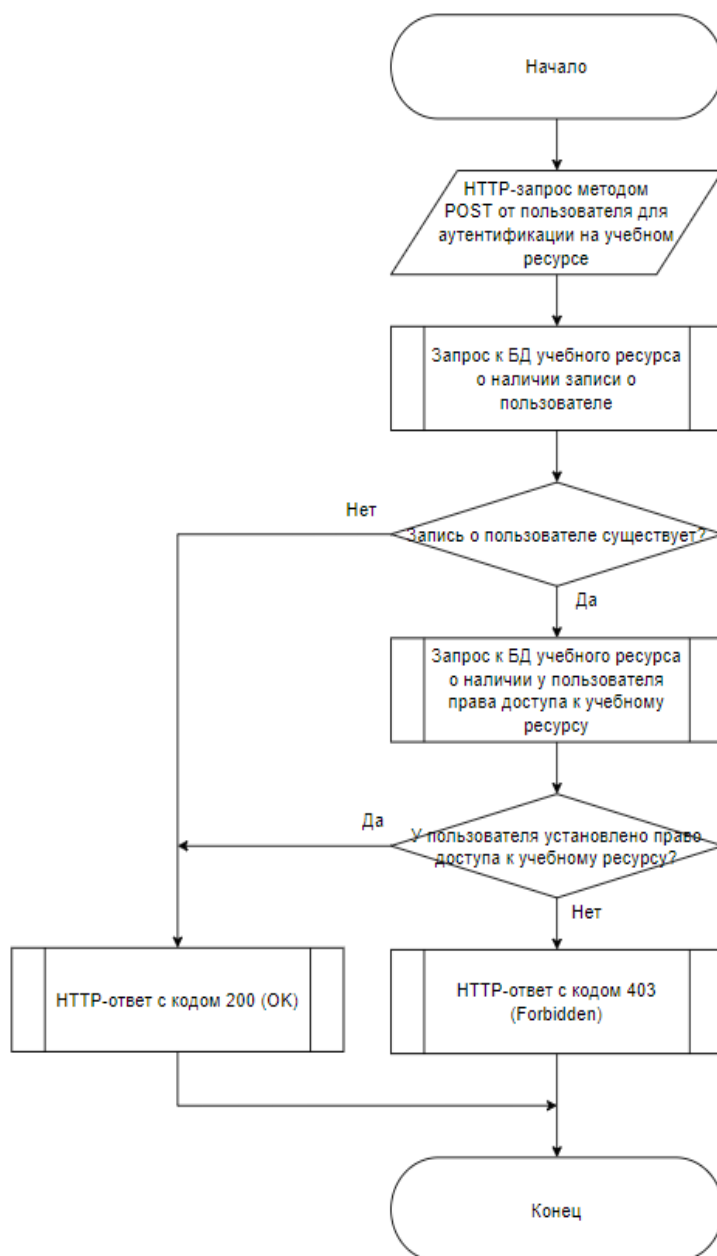


Рисунок 17 — Алгоритм работы механизма проверки полномочий доступа пользователей

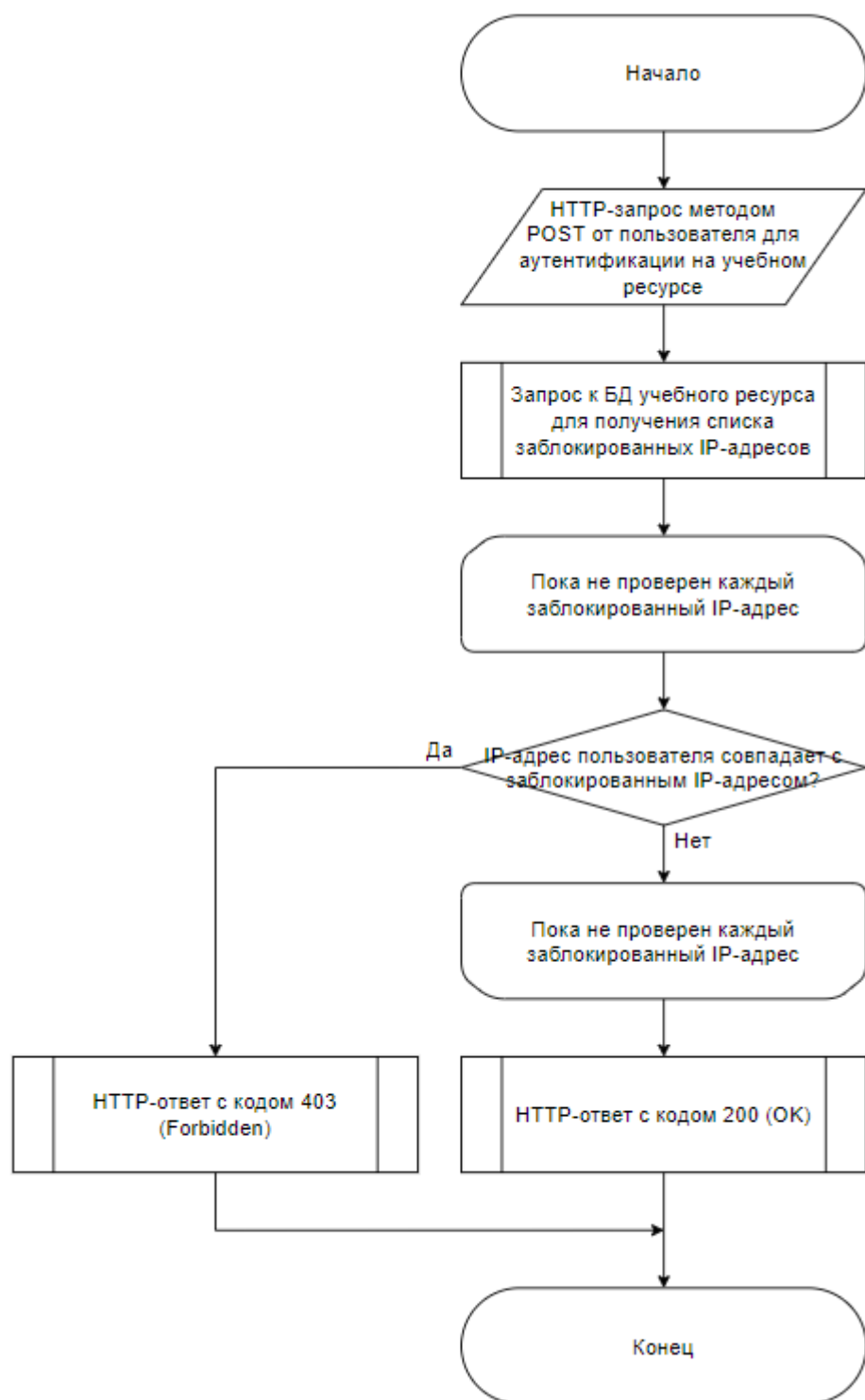


Рисунок 18 — Алгоритм работы механизма блокировки доступа к учебному ресурсу по IP-адресу

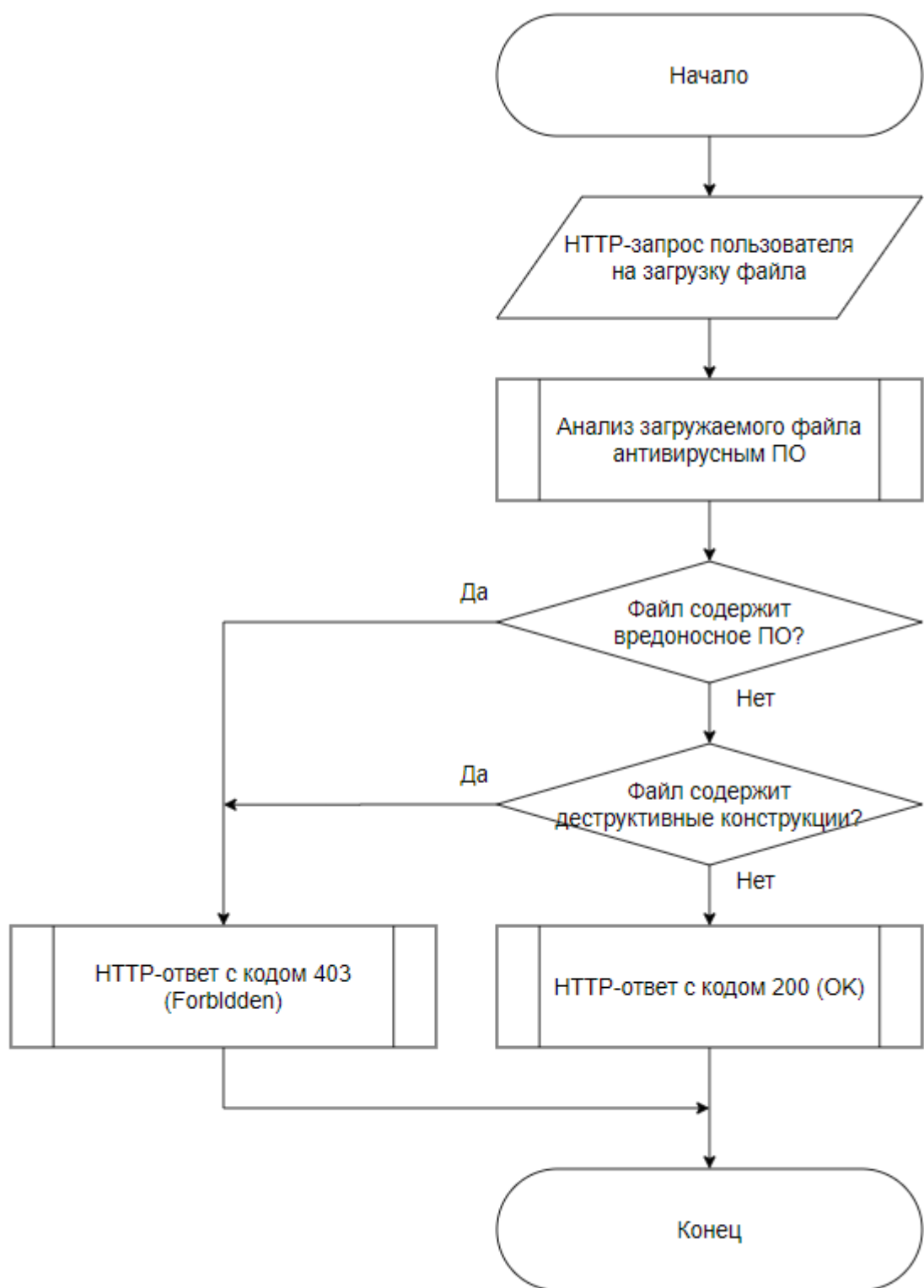


Рисунок 19 — Алгоритм работы механизма анализа загружаемых на учебный ресурс файлов

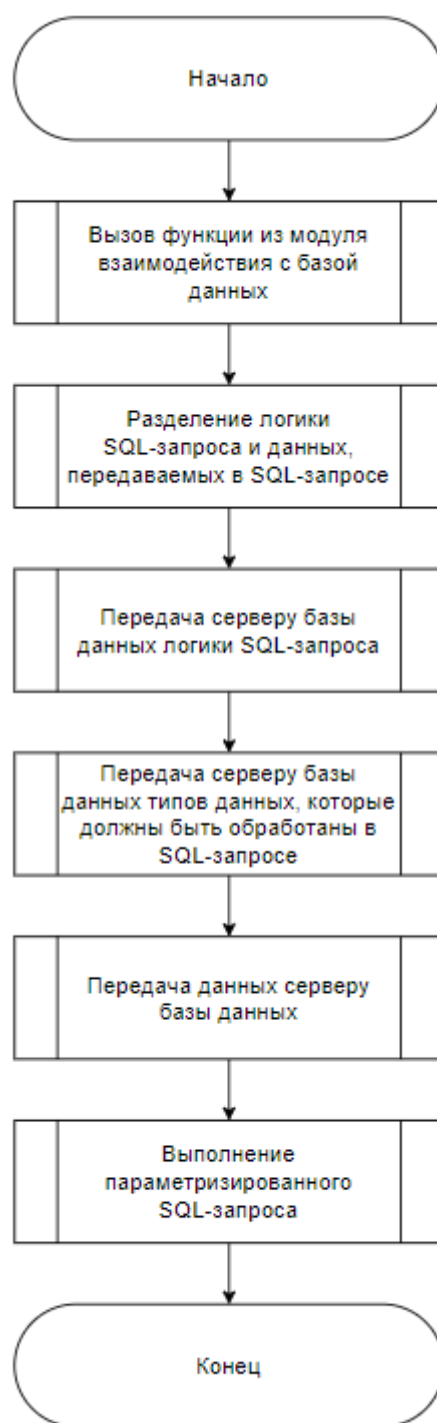


Рисунок 20 — Алгоритм работы механизма защиты от SQL-инъекций

4 Разработка учебного ресурса

4.1 Разработка модуля разграничения доступа

4.1.1 Описание функций модуля разграничения доступа.

В соответствии с задачами, которые должен выполнять модуль разграничения доступа, были разработаны его функции, представленные в таблице 2. Функции модуля разграничения доступа определены в файле *./services/access_module.php*. Также для ведения контроля доступа пользователей к учебному ресурсу была создана таблица «known_users» в базе данных учебного ресурса.

Таблица 2 — Функции модуля разграничения доступа

Название функции	Описание функции
auth_lti_user	С помощью вызовы функции lti_user_exists проверяет существование в БД записи о подключающемся по LTI пользователе. Если запись уже есть, то функция завершает свою работу; иначе выполняется вызов функции create_lti_user.
create_lti_user	С помощью вызова функции insert_query (<i>./services/database_module.php</i>) создаёт в таблице «known_users» запись о новом пользователе (роль «студент»), подключившемся через LTI, после чего вызывает функцию user_allow_access.
get_lti_user	Точка входа для начала обработки данных пользователей, принятых по интерфейсу LTI. Извлекаются данные из POST-запроса платформы-потребителя и передаются на вход функции auth_lti_user, после чего выполняется вызов функций update_lastip_and_moodle_id, check_read_access (<i>./services/security_module.php</i>) и set_user_login_time (<i>./services/registration_module.php</i>).

Продолжение таблицы 2

Название функции	Описание функции
get_web_user	Точка входа для обработки аутентификационной информации администратора и преподавателей через веб-интерфейс. Определяет, существует ли в БД запись о данном пользователе посредством вызова функции web_user_exists. Если запись существует, то аутентификация, произведённая ранее системными функциями Moodle, считается пройденной успешно и выполняется вызов функций update_lastip_and_moodle_id, check_read_access (./services/security_module.php) и set_user_login_time (./services/registration_module.php); иначе аутентификация не была пройдена и пользователю предлагается заново ввести логин и пароль.
lti_user_exists	С помощью вызова функции select_query (./services/database_module.php) проверяет существование записи о пользователе в БД учебного ресурса. Возвращает TRUE, если запись имеется и FALSE в противном случае.
update_lastip_and_moodle_id	С помощью вызова функции update_query (./services/database_module.php) обновляет IP-адрес пользователя и синхронизирует параметр moodle_id в БД с идентификатором, присвоенным пользователю платформой Moodle.
user_allow_access	С помощью вызова функции update_query (./services/database_module.php) модифицирует запись о пользователе, разрешая ему доступ к интерфейсу обучающегося.
web_user_exists	С помощью вызова функции select_query (./services/database_module.php) проверяет существование записи об администраторе или преподавателе в БД учебного ресурса. Возвращает TRUE, если запись имеется и FALSE в противном случае.

Кроме того, в рамках модуля разграничения доступа был создан .htaccess файл, который запрещает любой внешний доступ к разрабатываемым модулям учебного ресурса, разрешая использование их функций только серверу, на

котором находится учебный ресурс.

4.1.2 Разработка механизма аутентификации пользователей через интерфейс LTI.

В состав Moodle входит плагин, обеспечивающий возможность подключения к контенту учебного ресурса с другой платформы через интерфейс LTI. Данный плагин был настроен и активирован на разрабатываемом учебном ресурсе.

Недостатком Moodle является отсутствие возможности управления доступом к учебному ресурсу для каждого отдельного пользователя, подключившегося через LTI (ресурс либо доступен для всех, кто имеет доступ к ссылке на внешний учебный ресурс, либо недоступен для всех). Для управления доступом каждого отдельного пользователя, подключившегося к учебному ресурсу через LTI, необходимо проводить аутентификацию пользователей перед их переходом к учебному ресурсу. Эту задачу решает модуль разграничения доступа.

В рамках настоящей выпускной квалификационной работы платформа, через которую студент получает доступ к внешнему учебному ресурсу по интерфейсу LTI, называется «платформа-потребитель».

В ходе анализа сетевых пакетов, передаваемых между платформой-потребителем и учебным ресурсом, было установлено, что платформа-потребитель передаёт POST-запрос, содержащий аутентификационную информацию пользователя, учебному ресурсу по адресу *./enrol/lti/tool.php?id=n* (где *n* – идентификатор ресурса, к которому пользователь хочет получить доступ). Среди прочих параметров передаются:

- `oauth_consumer_key` – ключ платформы-потребителя, по которому учебный ресурс идентифицирует платформу-потребителя;
- `lis_person_name_given` – имя пользователя;
- `lis_person_name_family` – фамилия пользователя;

- `ext_user_username` – логин пользователя;
- `lis_person_contact_email_primary` – электронная почта пользователя;
- `oauth_signature_method` – тип используемой криптографической хеш-функции;

- `oauth_signature` – хеш, вычисленный криптографической хеш-функцией (параметр `oauth_signature_method`) на основе секретного ключа.

Если вычисленный на учебном ресурсе хеш идентичен принятому в параметре `oauth_signature`, то платформа-потребитель знает секретный ключ учебного ресурса, соответственно, студенты платформы-потребителя должны быть допущены модулем разграничения доступа к учебному ресурсу.

Если же вычисленный на учебном ресурсе хеш отличается от принятого в параметре `oauth_signature`, то соединение между платформой-потребителем и учебным ресурсом сбрасывается.

Для проверки данных, принятых по интерфейсу LTI, в файле *./enrol/lti/tool.php* вызывается функция `handleRequest` из файла *./lib/ltiprovider/src/ToolProvider/ToolProvider.php*. В данной функции для проверки аутентификационной информации, переданной платформой-потребителем в POST-запросе, вызывается функция `authenticate` из этого же файла, возвращающая `TRUE`, если аутентификация прошла успешно, и `FALSE`, если предоставленная аутентификационная информация некорректна.

В случае, если аутентификация не была пройдена, то соединение с пользователем разрывается. Если же аутентификация была пройдена успешно, то выполняется вызов служебной функции `set_user` из файла *./lib/classes/session/manager.php*, в которой создаётся сессия пользователя и настраиваются переменные окружения. До создания сессии пользователя и переменных окружения в функцию `set_user` была добавлена проверка типа подключения пользователя к учебному ресурсу — через LTI или через веб-интерфейс. Если пользователь подключается через интерфейс LTI, то

выполняется вызов функции `get_lti_user`, реализующей авторизацию пользователя через LTI (на основе аутентификационной информации) и настройку интерфейса обучающегося, из `./services/access_module.php`; в противном случае выполняется вызов функции `get_web_user` из `./services/access_module.php` для авторизации пользователей (на основе аутентификационной информации), подключающихся через веб-интерфейс учебного ресурса (аутентификация через веб-интерфейс описана в пункте 4.1.3 настоящей работы).

Также при работе с интерфейсом LTI платформа Moodle имеет уязвимость несанкционированного повышения привилегий. Связана эта уязвимость с механизмом идентификации в Moodle, который однозначно идентифицирует пользователей по комбинации их электронной почты и логина, после чего авторизует их на выполнение определённых действий в соответствии с настройками платформы. В рамках одной платформы такая комбинация будет действительно уникальной, однако в случае, когда через интерфейс LTI к учебному ресурсу могут подключаться пользователи с двух или более платформ-потребителей, то возможна ситуация, при которой пользователи могут иметь одинаковые логин и электронную почту. Например:

- на первой платформе-потребителе есть пользователь с некоторыми логином и электронной почтой, которому при подключении через LTI к курсу «А» учебного ресурса должна быть присвоена роль преподавателя на курсе «А»;

- на второй платформе-потребителе есть пользователь с логином и электронной почтой, идентичными пользователю с первой платформы-потребителя; этому пользователю при подключении через LTI к курсу «Б» учебного ресурса должна быть установлена роль студента на курсе «Б».

В рассматриваемой ситуации в случае, если пользователь сначала зайдёт

через LTI на учебный ресурс с первой платформы-потребителя, то в его сессии ему будет присвоена роль преподавателя и он будет иметь доступ к курсу «А». Если же он после этого зайдёт через LTI на учебный ресурс со второй платформы-потребителя, то учебный ресурс идентифицирует его как того же пользователя, что и с первой платформы-потребителя, в связи с чем вместо создания новой сессии в роли студента он зайдёт в сессию преподавателя, но с доступом к курсу «Б». Возникает несанкционированное повышение привилегий.

Модуль разграничения доступа решает вышеописанную уязвимость путём следующих изменений в процессах идентификации и авторизации пользователей:

- при идентификации пользователей в учебном ресурсе проверяется не только электронная почта и логин, но и роль пользователя; если обнаружен новый пользователь, то ему присваивается роль «студент»;

- все пользователи разделяются на «локальных», получающих доступ к учебному ресурсу через его веб-интерфейс, и «внешних», получающих доступ к учебному ресурсу через интерфейс LTI;

- «локальные» пользователи создаются администратором сайта; таким пользователям может быть установлена любая роль (администратор, преподаватель, студент);

- всем «внешним» пользователям при первом входе на учебный ресурс устанавливается роль «студента».

Таким образом, вышеописанными мерами исключается возможность несанкционированного повышения привилегий пользователей, подключающихся через интерфейс LTI.

4.1.3 Разработка механизма аутентификации пользователей через веб-интерфейс.

Являясь защищённым веб-ресурсом, разрабатываемый учебный ресурс

допускает аутентификацию через веб-интерфейс (посредством ввода логина и пароля) только для администратора и преподавателей (записи об этих пользователях изначально хранятся в базе данных учебного ресурса). Для реализации такого механизма аутентификации необходимо изменить стандартный процесс аутентификации Moodle, добавив в него необходимый функционал.

Аутентификация в Moodle производится посредством ввода логина и пароля на странице *./login/index.php* и последующего вызова функции `authenticate_user_login`; успешная аутентификация пользователя завершается вызовом функции `set_user` из файла *./lib/classes/session/manager.php*, в которой создаётся сессия пользователя и настраиваются переменные окружения. Так как в техническом задании к выпускной квалификационной работе для веб-интерфейса необходимо реализовать аутентификацию через логин и пароль, то не имеет смысла изменять непосредственно механизм аутентификации Moodle. Таким образом, чтобы разрешить доступ к учебному ресурсу только для администратора и преподавателей, записи о которых имеются в таблице «known_users», в функцию `set_user` была добавлена проверка типа подключения пользователя к учебному ресурсу — через LTI или через веб-интерфейс. Если пользователь подключается через интерфейс LTI, то выполняется вызов функции `get_lti_user`, реализующей авторизацию пользователя через LTI (на основе аутентификационной информации) и настройку интерфейса обучающегося (аутентификация через интерфейс LTI описана в пункте 4.1.2 настоящей работы), из *./services/access_module.php*; в противном случае выполняется вызов функции `get_web_user` из *./services/access_module.php* для авторизации пользователей (на основе аутентификационной информации), подключающихся через веб-интерфейс учебного ресурса. В результате таких изменений процедура аутентификации через веб-интерфейс будет заканчиваться успешно

только для пользователей, имеющих запись в таблице «known_users». В случае непрохождения процедуры аутентификации пользователи будут перенаправляться на страницу *./login/index.php* для повторной аутентификации.

4.1.4 Разработка механизма присвоения пользователям ролей.

Привилегированные пользователи (администратор и преподаватели) заносятся в базу данных учебного ресурса перед его запуском, в связи с чем таким пользователям роль установлена изначально.

Всем пользователям, подключающимся к учебному ресурсу через интерфейс LTI, устанавливается роль «студент». Роль «студента» устанавливается в функции `create_lti_user` при создании записи о новом пользователе.

4.1.5 Разработка механизма авторизации пользователей.

Авторизация пользователей в учебном ресурсе реализована посредством анализа роли пользователя, указанной в БД учебного ресурса, следующим образом:

- вне зависимости от роли пользователя, если о нём есть запись в БД учебного ресурса, то ему предоставляется доступ к интерфейсу обучающегося;
- если роль пользователя - «администратор», то для такого пользователя доступен дополнительный функционал — модуль управления учебным ресурсом (*./services/admin_module.php*);
- если роль пользователя - «преподаватель», то для такого пользователя доступен дополнительный функционал — модуль контроля учебного процесса.

4.2 Разработка модуля управления учебным ресурсом

4.2.1 Описание функций модуля управления учебным ресурсом.

В соответствии с задачами, которые должен выполнять модуль управления учебным ресурсом, были разработаны его функции, представленные в таблице 3. Функции модуля управления учебным ресурсом

определены в следующих файлах:

— *./services/admin_module.php* – основной файл модуля управления учебным ресурсом, представляющий собой меню выбора задачи; в зависимости от выбранной задачи подгружает функционал из других файлов;

— *./services/admin/read_access.php*, *./services/admin/js/read_access.js* – файлы модуля управления учебным ресурсом для настройки прав доступа пользователей к учебному ресурсу;

— *./services/admin/view_events.php*, *./services/admin/js/view_events.js* – файлы модуля управления учебным ресурсом для просмотра журнала событий;

— *./services/admin/checksum.php*, *./services/admin/js/checksum.js*, *./services/admin/checksum.txt* – файлы модуля управления учебным ресурсом для проведения контроля целостности учебного ресурса;

— *./services/admin/ban_ip.php*, *./services/admin/js/ban_ip.js* – файлы модуля управления учебным ресурсом для блокировки доступа к учебному ресурсу по IPv4- и IPv6-адресам.

Для ведения записей о заблокированных IP-адресах в базе данных учебного ресурса была создана таблица «banned_ip».

Таблица 3 — Функции модуля управления учебным ресурсом

Название функции	Описание функции
<i>./services/admin_module.php</i>	
check_admin	С помощью вызова функции <i>select_query</i> (<i>./services/database_module.php</i>) проверяет, является ли пользователь, отправляющий HTTP-запросы к серверу учебного ресурса на доступ к веб-странице <i>./services/admin_module.php</i> , администратором данного учебного ресурса. Если пользователь является администратором, то доступ к данной веб-странице разрешается; в противном случае сервер отправляет в ответ ошибку с кодом 403, запрещая пользователю доступ к веб-странице.

Продолжение таблицы 3

Название функции	Описание функции
./services/admin/read_access.php	
block_user	Выполняет блокировку доступа пользователя к учебному ресурсу. С помощью вызова функции select_query (./services/database_module.php) проверяет, существует ли в БД учебного ресурса запись о пользователе, которого администратор хочет заблокировать. Если запись существует, то с помощью вызова функции update_query (./services/database_module.php) обновляет запись о пользователе, запрещая ему доступ; в противном случае с помощью вызова функции insert_query (./services/database_module.php) создаёт новую запись в БД учебного ресурса о заблокированном пользователе.
execute_action	Проверяет код команды, переданной администратором, в зависимости от чего вызывает либо функцию block_user, либо функцию unblock_user.
is_action_required	Точка входа модуля управления учебным ресурсом, принимающая команды администратора. Обработывает данные, переданные администратором в POST-запросе. После обработки данных вызывает функцию execute_action.
print_users	С помощью вызова функции select_query (./services/database_module.php) в зависимости от переданного функции параметра выводит на веб-страницу список заблокированных или активных пользователей учебного ресурса.

Продолжение таблицы 3

Название функции	Описание функции
unblock_user	Выполняет снятие блокировки доступа пользователя к учебному ресурсу. С помощью вызова функции <code>select_query</code> (<code>./services/database_module.php</code>) проверяет, существует ли в БД учебного ресурса запись о пользователе, которого администратор хочет разблокировать. Если запись существует, то с помощью вызова функции <code>select_query</code> (<code>./services/database_module.php</code>) проверяется, посещал ли данный пользователь в прошлом учебный ресурс. Если посещал, то с помощью вызова функции <code>update_query</code> (<code>./services/database_module.php</code>) обновляет запись о пользователе, разрешая ему доступ к учебному ресурсу; в противном случае с помощью вызова функции <code>delete_query</code> (<code>./services/database_module.php</code>) удаляет запись о пользователе из БД учебного ресурса.
	<code>./services/admin/js/read_access.js</code>
setPOSTAction	Устанавливает на кнопки, отвечающие за отправку администратором команды блокировки пользователя или снятия блокировки с пользователя, соответствующее действие.
	<code>./services/admin/view_events.php</code>
build_view	Выводит на веб-страницу содержимое журнала событий в виде таблицы.
get_eventlog_content	С помощью вызова функции <code>is_update_required</code> проверяет, необходимо ли выполнить запись в журнал событий, после чего выводит на веб-страницу содержимое файла журнала событий (<code>./services/admin/eventlog.txt</code>).
is_update_required	Обрабатывает команды, передаваемые администратором в POST-запросах, обновляя содержимое журнала событий.
update_eventlog	Выполняет запись данных в журнал событий.

Продолжение таблицы 3

Название функции	Описание функции
./services/admin/js/view_points.js	
setPOSTData	В зависимости от нажатой администратором кнопки устанавливает данные, которые надо передать в POST-запросе («пустую» строку, если нажата кнопка «Очистить журнал», или данные, которые ввёл администратор в интерактивном режиме для записи в журнал событий).
./services/admin/checksum.php	
get_file_names	Выполняет рекурсивный поиск всех файлов в указанной директории. Возвращает массив с абсолютными путями ко всем файлам в директории.
is_write_required	Обрабатывает команду администратора о записи контрольных сумм в файл. Вызывает функцию write_checksums.
show_database_checksums	С помощью вызова функции checksum_query (./services/database_module.php) получает из базы данных контрольные суммы на таблицы «known_users» и «banned_ip», после чего выводит их на веб-страницу.
show_file_checksums	Получает от функции get_file_names абсолютные пути ко всем файлам в директории, после чего рассчитывает контрольную сумму по ГОСТ Р 34.11-94 для каждого из файлов и выводит их на веб-страницу.
write_checksums	Записывает в файл checksum.txt рассчитанные контрольные суммы и служебную информацию, генерируемую в функции setPOSTData (./services/admin/js/checksum.js).
./services/admin/js/checksum.js	
setPOSTData	Формирует данные по команде администратора для передачи в POST-запросе для записи в файл checksum.txt. К наименованиям объектов и их контрольным суммам также добавляет дату и время создания записи.

Продолжение таблицы 3

Название функции	Описание функции
./services/admin/ban_ip.php	
block_ip	Выполняет блокировку доступа к учебному ресурсу с переданного функции в параметре IP-адреса. С помощью вызова функции <code>select_query</code> (<code>./services/database_module.php</code>) проверяет, существует ли в БД учебного ресурса запись о блокировке IP-адреса, который администратор хочет заблокировать. Если запись существует, то на веб-страницу выводится сообщение «IP-адрес уже заблокирован» и функция завершает свою работу; в противном случае с помощью вызова функции <code>insert_query</code> (<code>./services/database_module.php</code>) создаёт новую запись в БД учебного ресурса о заблокированном IP-адресе, после чего выводит на веб-страницу сообщение «IP-адрес заблокирован».
execute_action	Проверяет код команды, переданной администратором, в зависимости от чего вызывает либо функцию <code>block_ip</code> , либо функцию <code>unblock_ip</code> .
is_action_required	Точка входа модуля управления учебным ресурсом, принимающая команды администратора. Обрабатывает данные, переданные администратором в POST-запросе. После обработки данных вызывает функцию <code>execute_action</code> .
print_banned_ip	Выводит на веб-страницу в виде таблицы заблокированные IP-адреса.
print_known_ip	Выводит на веб-страницу в виде таблицы IP-адреса всех известных пользователей учебного ресурса.
unblock_ip	С помощью вызова функции <code>select_query</code> (<code>./services/database_module.php</code>) выполняет удаление из БД учебного ресурса записи о блокировке переданного функции в параметре IP-адреса, после чего выводит на веб-страницу сообщение «IP-адрес разблокирован».
./services/admin/js/ban_ip.js	
setPOSTAction	Устанавливает на кнопки, отвечающие за отправку администратором команды блокировки IP-адреса или снятия блокировки с IP-адреса, соответствующее действие.

4.2.2 Разработка механизма управления полномочиями доступа пользователей.

В соответствии с настройками безопасности учебного ресурса право на запись в файлы учебного ресурса и создание новых файлов имеют только пользователи, которым присвоены роли «администратор» и «преподаватель». Так как право администратора на чтение и/или запись отключать нельзя (иначе он потеряет возможность администрирования сайта), то остаётся только регулирование права на запись преподавателей на учебном ресурсе.

Право на запись у преподавателя регулируется установкой права на модификацию контента учебного ресурса в настройках администратора, встроенных в платформу Moodle. В связи с этим разработка собственного аналога контроля права на запись не требуется. Установка прав на модификацию контента учебного ресурса описана в «Руководстве по эксплуатации» учебного ресурса.

Управление правами на чтение (т. е. правами доступа к контенту учебного ресурса) реализовано в файлах `./services/admin/read_access.php` и `./services/admin/js/read_access.js`; при этом файл `./services/admin/js/read_access.js` подгружается файлом `./services/admin/read_access.php`. Файл `./services/admin/read_access.php` подгружается на основную страницу модуля управления учебным ресурсом при нажатии раздела «Управление полномочиями доступа пользователей».

Управление правом пользователей на доступ к учебному ресурсу администратор может производить двумя способами:

- самостоятельным вводом данных о пользователе, которого необходимо заблокировать или разблокировать; при таком способе обязательными параметрами являются «Логин», «email» и «Роль»;
- нажатием кнопок «Разблокировать» или «Заблокировать» напротив пользователей в таблицах «Заблокированные пользователи» и «Активные пользователи», представленных на веб-странице.

При самостоятельном вводе данных обязательными параметрами являются «Логин», «email» и «Роль»; дополнительно для блокировки пользователя можно указать параметры «Имя» и «Фамилия» (если параметры оставлены пустыми, то они будут заменены на «%DEFAULT%»). «Имя» и «Фамилия» будут использоваться программой только при создании новой записи о заблокированном пользователе (т. к. для однозначной идентификации пользователя достаточно комбинации электронной почты, логина и его роли).

Контроль за доступом пользователей к учебному ресурсу реализован в модуле обеспечения информационной безопасности.

4.2.3 Разработка механизма просмотра журнала событий.

В рамках данного механизма был создан журнал событий `eventlog.txt`, расположенный в `./services/admin/`. Запись в журнал событий реализована в модуле регистрации событий.

Механизм просмотра журнала событий реализован в файлах `./services/admin/view_events.php` и `./services/admin/js/view_events.js`; при этом файл `./services/admin/js/view_events.js` подгружается файлом `./services/admin/view_events.php`. Файл `./services/admin/view_events.php` подгружается на основную страницу модуля управления учебным ресурсом при нажатии раздела «Просмотр журнала событий».

Журнал событий представлен администратору в двух видах:

- непосредственно содержимое файла журнала событий; администратор может либо изменить содержимое файла, после чего нажать кнопку «Сохранить журнал» для применения изменений, либо очистить журнал событий, нажав кнопку «Очистить журнал»;

- таблица событий, в которой содержимое журнала событий представлено в удобном для чтения виде.

4.2.4 Разработка механизма контроля целостности.

Механизм контроля целостности учебного ресурса может использоваться администратором для достижения следующих целей:

— при инсталляции учебного ресурса — убедиться, что файлы не были заранее подменены, а также не были повреждены во время их передачи или установки;

— при эксплуатации учебного ресурса — убедиться в том, что файлы не были несанкционированно изменены.

При этом было решено проводить контроль целостности только файлов и таблиц базы данных, реализующих модули, описанные в ТЗ, по следующим причинам:

— модули, разработанные в рамках настоящей выпускной квалификационной работы, могут работать независимо от системных таблиц базы данных Moodle, полагаясь только на данные из таблиц, созданных специально для этих модулей; в связи с этим при повреждении или несанкционированной модификации системных файлов Moodle несанкционированный доступ к ресурсу будет по-прежнему невозможен;

— платформа Moodle проводит внутренний контроль целостности своих плагинов; если некоторые файлы повреждены, то Moodle входит в «аварийный режим» (maintenance mode), при котором получить доступ к ресурсу может только администратор; Moodle будет находиться в этом режиме, пока администратор не исправит ошибки.

Платформа Moodle в своём минимальном варианте имеет более 19000 файлов. Расчёт контрольной суммы на сервере (с помощью PHP-скрипта) для такого количества файлов требует использования значительного сетевого трафика и временных затрат, в связи с чем сервер в соответствии со своими настройками, запрещающими исполнение скриптов дольше определённого времени, разорвёт соединение с администратором значительно раньше окончания выполнения скрипта. Расчёт же контрольной суммы на устройстве администратора (с помощью JS-скрипта) невозможен, т. к. большинство файлов учебного ресурса специально защищены от внешних HTTP-запросов и

доступны только серверу, который подгружает их по мере необходимости для пользователя.

В связи с вышеописанным модули, разработанные в рамках настоящей выпускной квалификационной работы, будут обеспечивать свойство конфиденциальности учебного ресурса в ситуации, когда целостность системных файлов Moodle была нарушена.

В рамках механизма контроля целостности был создан файл `checksum.txt`, расположенный в `./services/admin/`. Администратор может сохранить в этот файл рассчитанные контрольные суммы.

Механизм контроля целостности реализован в файлах `./services/admin/checksum.php` и `./services/admin/js/checksum.js`; при этом файл `./services/admin/js/checksum.js` подгружается файлом `./services/admin/checksum.php`. Файл `./services/admin/checksum.php` подгружается на основную страницу модуля управления учебным ресурсом при нажатии раздела «Контроль целостности».

По умолчанию MySQL версии 8.0.18 и выше и MariaDB версии не ниже 10.3.22 для расчёта контрольных сумм таблиц баз данных используют алгоритм CRC32. Однако доступные алгоритмы расчёта контрольных сумм в разных версиях вышеописанных СУБД отличаются и могут быть заданы хостингом самостоятельно.

Контрольные суммы для файлов модулей учебного ресурса рассчитываются в виде криптографической хеш-функции ГОСТ Р 34.11-94 с параметрами из RFC 4357 (раздел 11.2) [33].

Администратор может сохранить рассчитанные контрольные суммы в файл `checksum.txt`, нажав на веб-странице кнопку «Сохранить в файл».

4.2.5 Разработка механизма блокировки IP-адресов.

Механизм блокировки IP-адресов функционирует аналогично механизму управления полномочиями доступа пользователей.

Управление блокировкой IP-адресов реализовано в файлах

./services/admin/ban_ip.php и *./services/admin/js/ban_ip.js*; при этом файл *./services/admin/js/ban_ip.js* подгружается файлом *./services/admin/ban_ip.php*. Файл *./services/admin/ban_ip.php* подгружается на основную страницу модуля управления учебным ресурсом при нажатии раздела «Управление блокировкой IP-адресов».

Управление блокировкой IP-адресов администратор может производить двумя способами:

- самостоятельным вводом IP-адреса, который необходимо заблокировать или разблокировать;
- нажатием кнопок «Разблокировать» или «Заблокировать» напротив IP-адресов в таблицах «Заблокированные IP-адреса» и «Известные IP-адреса», представленных на веб-странице.

Контроль за доступом пользователей к учебному ресурсу на основании их IP-адреса реализован в модуле обеспечения информационной безопасности.

4.3 Разработка модуля контроля учебного процесса

Модуль контроля учебного процесса обеспечивает преподавателей учебного ресурса функционалом для настройки и наблюдения за учебным процессом. Являясь учебной платформой, Moodle изначально имеет все механизмы для управления учебными курсами, в связи с чем эти механизмы были настроены под задачи, которые должен решать модуль контроля учебного процесса.

Все пользователи учебного ресурса, которым присвоена роль «преподаватель», могут создавать и модифицировать курсы учебного ресурса. Перейдя на страницу курса и выбрав раздел «Редактировать настройки», преподаватели могут в интерактивном режиме создавать, изменять и удалять задания и учебные материалы, доступные студентам.

Перейдя на страницу курса и выбрав раздел «Оценки», преподаватели получают доступ к журналу оценок. Журнал оценок предоставляет широкие возможности фильтрации, сортировки, поиска, просмотра статистики

определённых студентов или определённых заданий.

В «Руководстве по эксплуатации» учебного ресурса в части функционала, доступного преподавателям, подробно описаны функции, доступные преподавателям.

4.4 Разработка модуля интерфейса обучающегося

В рамках модуля интерфейса обучающегося был настроен интерфейс учебного ресурса: цветовая схема, размещение интерфейсных блоков, визуальное представление заданий и учебных материалов и другое.

Кроме того, было разработано задание «Исследование механизмов обеспечения информационной безопасности реляционных баз данных в языке программирования SQL», к которому студенты могут подключиться через интерфейс LTI.

4.5 Разработка модуля обмена данными с внешними ресурсами

Модуль обмена данными с внешними ресурсами реализован на основе плагинов, реализующих интерфейс LTI на платформе Moodle. Плагины взяты из официального GitHub-репозитория проекта Moodle.

Интерфейс LTI в Moodle реализуется двумя плагинами:

- плагин аутентификации (*./auth/lti/*), в котором в файле *auth.php* реализовано переопределение системной функции аутентификации пользователей для проведения аутентификации по данным, передающимся через интерфейс LTI; аутентификация выполняется в соответствии с алгоритмом, описанным в пункте 2.2.3 настоящей выпускной квалификационной работы;
- плагин предоставления доступа к ресурсам (*./enrol/lti/*), в котором:
 - в файле *cartridge.php* создаётся специальная ссылка, по которой студенты внешнего ресурса могут получить доступ к объекту настоящего учебного ресурса;
 - в файле *index.php* реализовано визуальное отображение

LTI-объекта в учебном курсе;

- в файле `lib.php` реализована библиотека функций для непосредственного создания LTI-объекта;
- в файле `proxy.php` реализован функционал для сокрытия (при необходимости) LTI-объекта от внешнего доступа;
- в файле `settings.php` реализованы функции для управления LTI-объектом; доступны преподавателю и администратору;
- в файле `tool.php` реализована обработка HTTP-запросов пользователей на доступ к LTI-объекту.

После окончания работы плагина аутентификации (при успешном прохождении аутентификации пользователем) выполняется вызов функций модуля обеспечения информационной безопасности для фильтрации входящих соединений в соответствии с настройками безопасности учебного ресурса. Если модуль обеспечения информационной безопасности не разорвал соединение с пользователем (в соответствии с настройками безопасности), то выполняется вызов функции `get_lti_user` из модуля разграничения доступа для прохождения аутентификации и авторизации пользователей в соответствии с настройками модуля разграничения доступа.

4.6 Разработка модуля взаимодействия с базой данных

4.6.1 Описание функций модуля взаимодействия с базой данных.

В соответствии с задачами, которые должен выполнять модуль взаимодействия с базой данных, были разработаны его функции, представленные в таблице 4. Функции модуля взаимодействия с базой данных определены в файле `.\services\database_module.php`.

Таблица 4 — Функции модуля взаимодействия с базой данных

Название функции	Описание функции
checksum_query	Выполняет запрос к БД для подсчёта контрольных сумм таблиц known_users и banned_ip. В случае успешного запроса возвращает ассоциативный массив с контрольными суммами таблиц. В случае некорректного запроса возвращает сообщение об ошибке и прекращает своё выполнение.
delete_query	Реализует функционал оператора DELETE (т. е. удаление данных из базы данных). В случае успешного запроса возвращает TRUE. В случае некорректного запроса к БД возвращает сообщение об ошибке и прекращает своё выполнение.
insert_query	Реализует функционал оператора INSERT (т. е. запись данных в базу данных). В случае успешного запроса возвращает TRUE. В случае некорректного запроса к БД возвращает сообщение об ошибке и прекращает своё выполнение.
select_query	Реализует функционал оператора SELECT (т. е. чтение данных из базы данных). В случае успешного запроса возвращает результат запроса к БД в виде двухмерного ассоциативного массива (пустой массив в случае, если сервер базы данных на запрос вернул пустое множество). В случае некорректного запроса к БД возвращает сообщение об ошибке и прекращает своё выполнение.
update_query	Реализует функционал оператора UPDATE (т. е. изменение данных в базе данных). В случае успешного запроса возвращает TRUE. В случае некорректного запроса к БД возвращает сообщение об ошибке и прекращает своё выполнение.

4.6.2 Разработка функций модуля взаимодействия с базой данных.

Архитектура учебного ресурса разработана таким образом, что все остальные модули учебного ресурса взаимодействуют с БД только с помощью функций модуля взаимодействия с базой данных. Для совершения запроса к БД вызывается функция с соответствующим типом запроса (CHECKSUM,

DELETE, INSERT, SELECT, UPDATE). Все функции модуля взаимодействия с базой данных, кроме `checksum_query`, принимают в качестве параметров данные, которые будут подставляться в параметризованный запрос к БД учебного ресурса. Общий алгоритм работы функций модуля взаимодействия с базой данных следующий:

- проанализировать входные параметры;
- на основе входных параметров построить параметризованный запрос к БД учебного ресурса;
- на основе входных параметров установить тип данных для каждого параметра запроса;
- выполнить параметризованный запрос к БД учебного ресурса;
- вернуть результат запроса.

Выбор использования в функциях модуля взаимодействия с базой данных параметризованных SQL-запросов вместо стандартных основан на следующих их преимуществах:

- последовательные однотипные SQL-запросы (какими и являются большинство SQL-запросов на учебном ресурсе) выполняются значительно быстрее, чем при стандартных SQL-запросах;
- параметризованные SQL-запросы противодействуют возможным SQL-инъекциям.

Подробное описание использования в модуле взаимодействия с базой данных параметризованных SQL-запросов для противодействия SQL-инъекциям представлено в пункте 4.8.6 настоящей выпускной квалификационной работы.

4.7 Разработка модуля регистрации событий

4.7.1 Описание функций модуля регистрации событий.

В соответствии с задачами, которые должен выполнять модуль регистрации событий, были разработаны его функции, представленные в

таблице 5. Функции модуля регистрации событий определены в файле *./services\registration_module.php*.

В модуле регистрации событий все события регистрируются в часовой зоне Москвы (UTC+3).

Таблица 5 — Функции модуля регистрации событий

Название функции	Описание функции
eventlog_format	Обрабатывает данные о пользователе из базы данных учебного ресурса и приводит их к стандартному для журнала событий виду, после чего вызывает функцию <i>write_event</i> для записи события входа пользователя в систему.
set_user_access_time	С помощью вызова функции <i>select_query</i> (<i>./services/database_module.php</i>) получает данные о пользователе и, вместе с названием объекта учебного ресурса и типом события, передает их функции <i>eventlog_format</i> для записи в журнал событий.
set_user_login_time	Формирует часовой пояс, дату и время входа пользователя в систему и с помощью вызова функции <i>update_query</i> (<i>./services/database_module.php</i>) записывает их в базу данных учебного ресурса. После этого с помощью вызова функции <i>select_query</i> (<i>./services/database_module.php</i>) получает данные о пользователе и передает их функции <i>eventlog_format</i> для записи в журнал событий.
set_user_logout_time	Формирует часовой пояс, дату и время выхода пользователя из системы и с помощью вызова функции <i>update_query</i> (<i>./services/database_module.php</i>) записывает их в базу данных учебного ресурса. После этого с помощью вызова функции <i>select_query</i> (<i>./services/database_module.php</i>) получает данные о пользователе и передает их функции <i>eventlog_format</i> для записи в журнал событий.
write_debug	Служебная функция для отладки. В действующем учебном ресурсе не вызывается.
write_event	Записывает данные в журнал событий <i>eventlog.txt</i> .

4.7.2 Разработка механизма регистрации входа пользователя в систему.

Если пользователь, подключившийся через интерфейс LTI, в базе данных учебного ресурса отсутствует, то учебный ресурс сохраняет о пользователе следующую информацию:

- имя;
- фамилия;
- электронная почта;
- роль «студента»;
- логин;
- уникальный идентификатор.

Для локальных пользователей все вышеописанные данные уже установлены.

При каждой успешной аутентификации и авторизации пользователя (локально или через LTI) в БД учебного ресурса обновляется его IP-адрес.

Механизм регистрации входа пользователя в систему дополнительно к вышеописанной информации сохраняет в базу данных время входа пользователя в систему. Реализован данный механизм в функции `set_user_login_time`. Функция `set_user_login_time` вызывается в функциях `get_lti_user` и `get_web_user` модуля разграничения доступа после успешной аутентификации и авторизации пользователя.

Также модуль регистрации событий помещает событие входа пользователя в систему в файл `eventlog.txt` с помощью вызова функции `eventlog_format` из вышеописанной функции `set_user_login_time`. В функции `eventlog_format` обрабатываются данные о пользователе, полученные из базы данных учебного ресурса, приводятся к стандартному для журнала событий формату и с помощью вызова функции `write_event` записываются в журнал событий.

4.7.3 Разработка механизма регистрации выхода пользователя из системы.

Выход пользователя из системы происходит после окончания сессии пользователя на учебном ресурсе. Пользовательская сессия может закончиться двумя способами:

- пользователь нажал на кнопку выхода из системы;
- истекло время ожидания действий от пользователя (т. е. пользователь бездействовал некоторый промежуток времени); время бездействия, через которое пользовательская сессия заканчивается, устанавливает администратор учебного ресурса, и это правило распространяется на всех пользователей без исключения.

При самостоятельном выходе пользователя из системы путём нажатия кнопки выхода платформа Moodle вызывает функцию `require_logout` (`./lib/moodlelib.php`). В данной функции уничтожается сессия пользователя и удаляются его переменные окружения. Для определения времени выхода пользователя из системы в функцию `require_logout` перед удалением пользовательской сессии был вставлен вызов функции `set_user_logout_time`, которая записывает в БД учебного ресурса время выхода пользователя из системы. Также модуль регистрации событий помещает событие выхода пользователя из системы в файл `eventlog.txt` с помощью вызова функции `eventlog_format` из вышеописанной функции `set_user_logout_time`. В функции `eventlog_format` обрабатываются данные о пользователе, полученные из базы данных учебного ресурса, приводятся к стандартному для журнала событий формату и с помощью вызова функции `write_event` записываются в журнал событий.

В большинстве же случаев пользователь завершает работу с веб-ресурсом простым закрытием его вкладки в веб-браузере. Принципиально механизм завершения пользовательской сессии по причине бездействия работает следующим образом: HTTP-запрос пользователя к веб-страницам вызывает

запрос к БД учебного ресурса о наличии записи о пользователе, отправившем HTTP-запрос; если пользователь в БД не найден, то пользователь перенаправляется на страницу аутентификации (после успешного прохождения аутентификации устанавливается временная метка активности пользователя); в противном случае вычисляется разность между временной меткой на данный момент и временной меткой, когда пользователь последний раз посещал учебный ресурс; если эта разность меньше времени бездействия, то сессия пользователя восстанавливается и временная метка последнего посещения учебного ресурса обновляется; в противном случае пользователь перенаправляется на страницу аутентификации. При этом временная метка активности пользователя обновляется не чаще определённого периода (по умолчанию — 20 секунд) для повышения производительности учебного ресурса.

Таким образом из вышеописанного следуют две особенности механизма регистрации выхода пользователя из системы по причине окончания его сессии:

- установить факт выхода пользователя из системы можно только в моменты, когда этот пользователь отправляет HTTP-запросы к веб-страницам учебного ресурса;

- зафиксированное время выхода пользователя из системы — это время его последнего HTTP-запроса к веб-странице учебного ресурса перед истечением его пользовательской сессии.

Механизм вычисления времени бездействия пользователя реализован в функции `initialise_user_session` (`./lib/classes/session/manager.php`). при поступлении HTTP-запроса к учебному ресурсу выполняется запрос к БД учебного ресурса о существовании записи о пользователе, отправившем HTTP-запрос. Если запись о пользователе найдена, то вычисляется разность между временной меткой на данный момент и временной меткой активности пользователя. Если эта разность больше допустимого времени бездействия, то

пользовательская сессия завершается и пользователь перенаправляется на веб-страницу аутентификации. Для регистрации времени выхода пользователя из системы при выполнении вышеописанного условия был добавлен вызов функции `set_user_logout_time`, которая записывает в БД учебного ресурса время выхода пользователя из системы. Также модуль регистрации событий помещает событие выхода пользователя из системы в файл `eventlog.txt` с помощью вызова функции `eventlog_format` из вышеописанной функции `set_user_logout_time`. В функции `eventlog_format` обрабатываются данные о пользователе, полученные из базы данных учебного ресурса, приводятся к стандартному для журнала событий формату и с помощью вызова функции `write_event` записываются в журнал событий.

4.7.4 Разработка механизма регистрации начала работы пользователя с объектом учебного ресурса.

Для администратора и преподавателя учебного ресурса регистрация начала работы пользователей с объектами учебного ресурса актуальна только для объектов типа «тест» (остальные типы учебных объектов не оцениваются и/или не ограничиваются по времени выполнения). Соответственно, механизм регистрации начала работы пользователя с объектом учебного ресурса был разработан непосредственно для «тестов».

Пользователь может начать работу с объектами типа «тест» двумя способами:

- начать новую учебную сессию, в рамках которой он будет взаимодействовать с тестом;
- продолжить ранее созданную учебную сессию.

Для администратора и преподавателя важно знать, когда пользователь начал именно новую учебную сессию, т. к. продолжение ранее созданной учебной сессии никак не изменяет учебный процесс.

Приступая к выполнению теста, пользователь перенаправляется на

веб-страницу `./mod/quiz/startattempt.php`, где сервер либо устанавливает ему новую учебную сессию, либо продолжает уже созданную пользователем ранее. В файл `./mod/quiz/startattempt.php` был добавлен вызов функции `set_user_access_time` в случае, если создаётся новая учебная сессия. Функция `set_user_access_time` осуществляет запрос к БД учебного ресурса для получения данных о пользователе, который начинает проходить тест, после чего передаёт эти данные функции `eventlog_format` вместе с командой записи события типа «Начало работы с объектом». В функции `eventlog_format` обрабатываются данные о пользователе, полученные из базы данных учебного ресурса, приводятся к стандартному для журнала событий формату и с помощью вызова функции `write_event` записываются в журнал событий.

4.7.5 Разработка механизма регистрации завершения работы пользователя с объектом учебного ресурса.

Пользователь может завершить работу с объектами типа «тест» двумя способами:

- непосредственно прохождением теста и нажатием кнопки «Завершить тест»;
- автоматическим завершением учебной сессии пользователя по причине истечения времени, установленного преподавателем на попытку прохождения теста;
- автоматическим завершением учебной сессии пользователя по причине истечения времени, в течение которого данный тест доступен пользователям.

При возникновении любого из трёх вышеописанных событий пользователь перенаправляется на веб-страницу `./mod/quiz/processattempt.php`. Скрипт на этой веб-странице в результате своей работы выставляет пользователю оценку за пройденный тест, после чего перенаправляет его на

страницу просмотра результатов теста. В файл *./mod/quiz/processattempt.php* перед перенаправлением пользователя был добавлен вызов функции *set_user_access_time* для регистрации факта завершения работы пользователя с объектом учебного ресурса. Функция *set_user_access_time* осуществляет запрос к БД учебного ресурса для получения данных о пользователе, который начинает проходить тест, после чего передаёт эти данные функции *eventlog_format* вместе с командой записи события типа «Завершение работы с объектом». В функции *eventlog_format* обрабатываются данные о пользователе, полученные из базы данных учебного ресурса, приводятся к стандартному для журнала событий формату и с помощью вызова функции *write_event* записываются в журнал событий.

4.8 Разработка модуля обеспечения информационной безопасности

4.8.1 Описание функций модуля обеспечения информационной безопасности.

В соответствии с задачами, которые должен выполнять модуль обеспечения информационной безопасности, были разработаны его функции, представленные в таблице 6. Функции модуля обеспечения информационной безопасности определены в файле *./services/security_module.php*.

Таблица 6 — Функции модуля обеспечения информационной безопасности

Название функции	Описание функции
<i>check_read_access</i>	С помощью вызова функции <i>select_query</i> (<i>./services/database_module.php</i>) получает из БД учебного ресурса информацию о наличии у пользователя права доступа к учебному ресурсу. Если пользователь имеет право доступа, то функция завершает свою работу; в противном случае сервер отправляет HTTP-ответ с кодом 403 (Forbidden), запрещая доступ к учебному ресурсу.

Продолжение таблицы 6

Название функции	Описание функции
check_ip_address	С помощью вызова функции <code>select_query</code> (<code>./services/database_module.php</code>) получает из БД учебного ресурса список заблокированных IP-адресов. Если IP-адрес пользователя, отправившего HTTP-запрос на доступ к учебному ресурсу, входит в список заблокированных IP-адресов, то сервер отправляет HTTP-ответ с кодом 403 (Forbidden), запрещая доступ к учебному ресурсу; в противном случае пользователь допускается до прохождения аутентификации.

4.8.2 Разработка механизма проверки полномочий доступа пользователей.

С помощью модуля управления учебным ресурсом администратор может блокировать и снимать блокировку на доступ к учебному ресурсу с пользователей. Все пользователи (и те, кто имеют право доступа к учебному ресурсу, и те, кого администратор заблокировал) имеют в базе данных учебного ресурса запись, содержащую как минимум электронную почту, логин и роль пользователя, чего достаточно для однозначной идентификации пользователя.

Для механизма блокировки доступа к учебному ресурсу по IP-адресу важно знать актуальные IP-адреса идентифицированных пользователей. В связи с этим проверка полномочий доступа пользователей проводится после успешной аутентификации пользователя и получения его актуального IP-адреса, но перед его авторизацией на учебном ресурсе. В функции `get_lti_user` (`./services/access_module.php`) и `get_web_user` (`./services/access_module.php`), являющиеся точками входа для аутентификации и последующей авторизации пользователей через LTI и веб-интерфейс соответственно, был добавлен вызов функции `check_read_access`, проверяющей право доступа пользователя к учебному ресурсу. Если пользователь был заблокирован администратором, то пользователю будет отправлен HTTP-ответ с кодом 403 (Forbidden), а соединение с ним будет разорвано, в результате чего пользователь не будет допущен к сайту. Если же пользователь имеет право доступа к учебному

ресурсу, то он будет авторизован на доступ к объектам учебного ресурса.

4.8.3 Разработка механизма контроля целостности учебного ресурса.

Механизм контроля целостности учебного ресурса разрабатывался для проведения администратором контроля целостности из его модуля управления учебным ресурсом. Для уменьшения количества перекрёстных зависимостей между файлами и повышения производительности учебного ресурса механизм контроля целостности был реализован в рамках модуля управления учебным ресурсом. Описание работы механизма контроля целостности учебного ресурса представлено в пункте 5.2.4 настоящей выпускной квалификационной работы.

4.8.4 Разработка механизма блокировки доступа к учебному ресурсу по IP-адресу.

По умолчанию учебный ресурс разрешает подключение к нему со всех IP-адресов. Блокировка IP-адресов проводится администратором через модуль управления учебным ресурсом.

В отличие от механизма проверки полномочий доступа пользователей механизм блокировки доступа к учебному ресурсу по IP-адресу срабатывает до начала процедуры аутентификации для предотвращения атак типа «отказ в обслуживании», исходящих от неидентифицированных пользователей.

Аутентификация через веб-интерфейс выполняется в файле *./login/index.php*. В начало файла *./login/index.php*, на который перенаправляют неаутентифицированного пользователя все веб-страницы учебного ресурса для аутентификации, был добавлен вызов функции `check_ip_address`. Функция `check_ip_address` выполняет запрос к БД учебного ресурса для получения списка заблокированных IP-адресов. Если IP-адрес пользователя совпадает с одним из заблокированных IP-адресов, то сервер отправляет HTTP-ответ с кодом 403 (Forbidden), запрещая пользователю доступ к учебному ресурсу; в противном случае пользователь допускается к процедуре аутентификации.

Для проверки данных, принятых по интерфейсу LTI, в файле *./enrol/lti/tool.php* вызывается функция `handleRequest` из файла

./lib/ltiprotider/src/ToolProvider/ToolProvider.php. В данной функции для проверки аутентификационной информации, переданной платформой-потребителем в POST-запросе, вызывается функция `authenticate` из этого же файла. В функцию `handleRequest` перед вызовом функции `authenticate` был добавлен вызов функции `check_ip_address`, в результате чего аутентификация через LTI будет выполняться только для пользователей с разрешёнными IP-адресами.

4.8.5 Разработка механизма анализа загружаемых на учебный ресурс файлов.

Механизм анализа загружаемых на учебный ресурс файлов реализован в виде двух компонентов:

- серверный антивирус ClamAV;
- плагин антивируса ClamAV для Moodle.

Плагин антивируса ClamAV для Moodle создан разработчиками проекта Moodle совместно с разработчиками ClamAV. Данный плагин позволяет:

- проводить периодическое сканирование ресурса, разработанного на основе Moodle, на предмет наличия в нём вредоносного ПО и деструктивных конструкций.
- анализировать загружаемые на ресурс пользователями файлы на предмет наличия в них вредоносного ПО и деструктивных конструкций.

Антивирус ClamAV при своей работе использует как сигнатурные, так и эвристические методы анализа файлов.

Серверный антивирус ClamAV является необязательным компонентом учебного ресурса. Если он не установлен, то механизм анализа загружаемых на учебный ресурс файлов будет отключен.

Плагин антивируса ClamAV для Moodle не требует никакой дополнительной настройки.

Процесс установки серверного антивируса описан в «Руководстве по

инсталляции» учебного ресурса.

4.8.6 Разработка механизма защиты от SQL-инъекций.

Все запросы к БД учебного ресурса выполняются через функции модуля взаимодействия с базой данных. При этом функции `select_query`, `update_query`, `insert_query`, `delete_query` модуля взаимодействия с базой данных в качестве параметров принимают пользовательский ввод, который потенциально может содержать SQL-инъекции. Функция `checksum_query` не принимает никаких параметров и выполняет заранее установленный SQL-запрос, в связи с чем для неё угроза внедрения SQL-инъекции не актуальна.

Для защиты от SQL-инъекций в функциях `select_query`, `update_query`, `insert_query`, `delete_query` SQL-запросы выполняются в параметризованном виде. Вышеописанные функции принимают в качестве параметров:

- название таблицы, к которой будет выполнен SQL-запрос;
- названия столбцов таблицы, к которым будет выполнен SQL-запрос;
- параметры, которые будут использованы в SQL-запросе;
- логические операторы (если они требуются для конструкции WHERE);
- типы данных параметров и количество параметров, которые будут использованы в SQL-запросе.

При этом пользовательский ввод представлен только в виде параметров, которые будут использованы в SQL-запросе. Название таблицы, названия столбцов таблицы, логические операторы, количество параметров, а также непосредственно тип запроса (SELECT, UPDATE, INSERT, DELETE) формируют логику запроса. Параметризованные SQL-запросы отделяют логику SQL-запроса от его параметров в функциях модуля взаимодействия с базой данных следующим образом.

На первом шаге на сервер базы данных передаётся только логика SQL-запроса без параметров; пример такого запроса:

```
INSERT INTO `known_users` (`email_address`, `user_login`,  
`user_role`) VALUES (?, ?, ?)
```

Символами «?» отмечены параметры, которые позже будут переданы в это SQL-запрос. Сервер базы данных по принятой логике SQL-запроса выбирает таблицу и её столбцы, которые будут участвовать в SQL-запросе; кроме того, сервер базы данных теперь знает количество параметров, которые будут в SQL-запросе, и их позиции в структуре SQL-запроса. Таким образом исключается угроза внедрения дополнительной логики в SQL-запрос (например, с помощью логического оператора ИЛИ: « ' OR 1=1; --»), а также «зацепления» SQL-запросов (например, « '; DROP TABLE known_users; -- »).

На втором шаге на сервер базы данных передаются типы данных для каждого конкретного параметра («integer», «double», «string», «blob»). Из-за этого сервер базы данных не будет производить неявного преобразования типов при несоответствии ожидаемого типа данных и принятого, а будет возвращать ошибку SQL-запроса. Кроме того, сервер базы данных будет обрабатывать специальные символы в данных типа «string». Это исключает угрозу модификации параметров SQL-запроса (например, внедрение символа «'», как в « ' OR 1=1; --»).

На третьем шаге на сервер базы данных отправляются параметры SQL-запроса, выполняется реальный SQL-запрос и возвращается результат SQL-запроса. При этом первый и второй шаг исключают возможность внедрения пользователями SQL-инъекций.

5 Тестирование учебного ресурса

После разработки учебного ресурса было проведено функциональное тестирование всех модулей учебного ресурса. В рамках функционального тестирования проводились тесты для определения корректного выполнения каждого отдельного требования технического задания, предъявляемого к модулям учебного ресурса.

В таблице 7 представлены результаты функционального тестирования модулей учебного ресурса. В рамках каждого тестового случая проводились однотипные тесты с различными входными данными.

Таблица 7 — Результаты функционального тестирования модулей учебного ресурса

Тестовый случай	Результат тестового случая	Тестовый случай пройден успешно?
Модуль разграничения доступа		
Попытка доступа к учебному ресурсу через интерфейс LTI с некорректным секретным ключом	Аутентификация не пройдена. Доступ к учебному ресурсу запрещён.	Да
Попытка доступа к учебному ресурсу через интерфейс LTI с корректным секретным ключом	Пользователь успешно аутентифицирован и авторизован. Доступ к учебному ресурсу предоставлен.	Да
Попытка доступа к учебному ресурсу через веб-интерфейс с вводом несуществующей в БД учебного ресурса комбинации логина и пароля	Аутентификация не пройдена. Доступ к учебному ресурсу запрещён.	Да
Попытка доступа к учебному ресурсу через веб-интерфейс с вводом существующей в БД учебного ресурса комбинации логина и пароля	Пользователь успешно аутентифицирован и авторизован. Доступ к учебному ресурсу предоставлен.	Да

Продолжение таблицы 7

Тестовый случай	Результат тестового случая	Тестовый случай пройден успешно?
Попытка доступа к учебному ресурсу без прохождения аутентификации	Доступ к учебному ресурсу запрещён. Переадресация пользователя на страницу аутентификации.	Да
Попытка доступа к модулю управления учебным ресурсом от имени пользователей с ролью «студент» или «преподаватель»	Доступ к модулю запрещён.	Да
Попытка доступа к модулю управления учебным ресурсом от имени пользователя с ролью «администратор»	Доступ к модулю предоставлен.	Да
Попытка доступа к модулю контроля учебного процесса от имени пользователя с ролью «студент»	Доступ к модулю запрещён.	Да
Попытка доступа к модулю контроля учебного процесса от имени пользователей с ролью «администратор» или «преподаватель»	Доступ к модулю предоставлен.	Да
Попытка доступа к модулю интерфейса обучающегося от имени пользователей с ролью «администратор», «преподаватель» или «студент»	Доступ к модулю предоставлен.	Да
Попытка доступа к модулям учебного ресурса (исключая модуль управления учебным ресурсом, модуль контроля учебного процесса и модуль интерфейса обучающегося) от имени пользователей с ролью «администратор», «преподаватель» или «студент»	Доступ к модулю запрещён.	Да

Продолжение таблицы 7

Тестовый случай	Результат тестового случая	Тестовый случай пройден успешно?
Модуль управления учебным ресурсом		
Отключение права записи у пользователя с ролью «преподаватель»	Пользователь не может создавать, изменять и удалять объекты учебного ресурса	Да
Отключение права записи у пользователя с ролью «администратор»	Пользователь может создавать, изменять и удалять объекты учебного ресурса	Да
Отключение права чтения учебного ресурса (доступа к учебному ресурсу) у пользователя с ролью «преподаватель» или «студент»	Пользователю доступ к учебному ресурсу запрещён.	Да
Отключение права чтения учебного ресурса (доступа к учебному ресурсу) у пользователя с ролью «администратор»	Пользователю доступ к учебному ресурсу предоставлен.	Да
Изменение журнала событий без сохранения изменений	Журнал событий не изменился	Да
Изменение журнала событий с сохранением изменений	Журнал событий изменился	Да
Очистка журнала событий	Журнал событий пуст	Да
Сохранение контрольных сумм в файл	В файл checksum.txt записаны актуальные контрольные суммы	Да
Блокировка IPv4-адреса	IPv4-адрес помещён в таблицу заблокированных IP-адресов	Да
Снятие блокировки с IPv4-адреса	IPv4-адрес удалён из таблицы заблокированных IP-адресов	Да

Продолжение таблицы 7

Тестовый случай	Результат тестового случая	Тестовый случай пройден успешно?
Блокировка IPv6-адреса	IPv6-адрес помещён в таблицу заблокированных IP-адресов	Да
Снятие блокировки с IPv6-адреса	IPv6-адрес удалён из таблицы заблокированных IP-адресов	Да
Модуль контроля учебного процесса		
Загрузка файла в раздел курса	Файл загружен и появился на странице курса	Да
Удаление файла из раздела курса	Файл удалён и отсутствует на странице курса	Да
Просмотр журнала преподавателя	Журнал преподавателя содержит оценки, количество попыток, даты начала и окончания выполнения заданий студентами	Да
Модуль интерфейса обучающегося		
Прохождение доступных учебных заданий	Задания корректно начинаются, отображаются и завершаются; по окончании выполнения задания выставляется оценка	Да
Просмотр учебных материалов	Файлы корректно открываются и отображаются	Да
Модуль обмена данными с внешними ресурсами		
Попытка доступа к учебному ресурсу через «Внешний инструмент» платформы-потребителя	Учебный ресурс получил от платформы-потребителя XML-файл, содержащий информацию о студенте	Да

Продолжение таблицы 7

Тестовый случай	Результат тестового случая	Тестовый случай пройден успешно?
Завершение работы студента с заданием, за которое выставляется оценка	Учебный ресурс отправляет платформе-потребителю XML-файл с результатами выполнения студентом задания и его оценкой	Да
Модуль взаимодействия с базой данных		
Вызов функций модуля взаимодействия с базой данных с некорректными параметрами	SQL-запрос не выполнен; сервер базы данных вернул ошибку	Да
Вызов функций модуля взаимодействия с базой данных с нулевыми параметрами	SQL-запрос не выполнен; сервер базы данных вернул ошибку	Да
Вызов функций модуля взаимодействия с базой данных с корректными параметрами	SQL-запрос выполнен; сервер базы данных вернул результат SQL-запроса	Да
Модуль регистрации событий		
Вход пользователя на учебный ресурс через LTI	В журнал событий добавлена запись о входе пользователя на учебный ресурс	Да
Вход пользователя на учебный ресурс через веб-интерфейс	В журнал событий добавлена запись о входе пользователя на учебный ресурс	Да
Выход пользователя с учебного ресурса путём нажатия кнопки выхода	В журнал событий добавлена запись о самостоятельном выходе пользователя с учебного ресурса	Да
Пользователь не посылает HTTP-запросы к учебному ресурсу в течение предельно допустимого времени бездействия	В журнал событий добавлена запись о выходе пользователя с учебного ресурса по причине тайм-аута	Да

Продолжение таблицы 7

Тестовый случай	Результат тестового случая	Тестовый случай пройден успешно?
Пользователь начал прохождение теста на учебном ресурсе	В журнал событий добавлена запись о начале работы пользователя с объектом учебного ресурса	Да
Пользователь завершил прохождение теста на учебном ресурсе	В журнал событий добавлена запись о завершении работы пользователя с объектом учебного ресурса	Да
Истекло время работы пользователя с тестом	В журнал событий добавлена запись о завершении работы пользователя с объектом учебного ресурса	Да
Модуль обеспечения информационной безопасности		
Удаление записи из таблицы базы данных учебного ресурса	Контрольная сумма таблицы изменилась	Да
Изменение файла учебного ресурса	Контрольная сумма файла изменилась	Да
Попытка доступа к учебному ресурсу через LPI с заблокированного IPv4-адреса	Доступ к учебному ресурсу запрещён.	Да
Попытка доступа к учебному ресурсу через LPI с заблокированного IPv6-адреса	Доступ к учебному ресурсу запрещён.	Да
Попытка доступа к учебному ресурсу через LPI с разрешённого IPv4-адреса	Доступ к учебному ресурсу предоставлен.	Да
Попытка доступа к учебному ресурсу через LPI с разрешённого IPv6-адреса	Доступ к учебному ресурсу предоставлен.	Да
Попытка доступа к учебному ресурсу через веб-интерфейс с заблокированного IPv4-адреса	Доступ к учебному ресурсу запрещён.	Да

Продолжение таблицы 7

Тестовый случай	Результат тестового случая	Тестовый случай пройден успешно?
Попытка доступа к учебному ресурсу через веб-интерфейс с заблокированного IPv6-адреса	Доступ к учебному ресурсу запрещён.	Да
Попытка доступа к учебному ресурсу через веб-интерфейс с разрешённого IPv4-адреса	Доступ к учебному ресурсу предоставлен.	Да
Попытка доступа к учебному ресурсу через веб-интерфейс с разрешённого IPv6-адреса	Доступ к учебному ресурсу предоставлен.	Да
Попытка загрузки на учебный ресурс файла без вредоносного ПО и деструктивных конструкций	Файл успешно загружен	Да
Попытка загрузки на учебный ресурс файла-трояна	Загрузка файла заблокирована	Да
Попытка загрузки на учебный ресурс вирусного файла	Загрузка файла заблокирована	Да
Попытка загрузки на учебный ресурс заархивированного вирусного файла	Загрузка файла заблокирована	Да
Попытка загрузки на учебный ресурс «ZIP-бомбы»	Загрузка файла заблокирована	Да

По результатам функционального тестирования был сделан вывод, что учебный ресурс удовлетворяет всем требованиям, поставленным в техническом задании на выпускную квалификационную работу.

6 Разработка документации к учебному ресурсу

Для работы с учебным ресурсом были разработаны «Руководство по инсталляции» и «Руководство по эксплуатации».

«Руководство по инсталляции» представлено в Приложении А «Руководство по инсталляции» и предназначено только для администратора учебного ресурса.

«Руководство по эксплуатации» представлено в Приложении Б «Руководство по эксплуатации» и предназначено для администратора учебного ресурса и преподавателей учебного ресурса.

7 Вредные психофизиологические факторы, влияющие на органы зрения специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

Согласно ГОСТ 12.0.003-2015 [34], опасные и вредные производственные факторы, обладающие свойствами психофизиологического воздействия на организм человека, подразделяют на:

- физические перегрузки, связанные с тяжестью трудового процесса;
- нервно-психические перегрузки, связанные с напряжённостью трудового процесса.

Большую часть рабочего времени специалист по защите информации проводит за экраном компьютера. Долгая непрерывная работа за компьютером напрягает глаза работника, а излучение монитора может привести к утомлению глаз и ухудшению его зрения. Компьютерный зрительный синдром (синдром сухого глаза), развивающийся из-за долгого сидения за экраном компьютера, провоцирует боль и усталость глаз, сухость в глазах, нечёткость зрения и двоение в глазах, боль в голове, плечах, шее.

Для того, чтобы избежать негативного воздействия на органы зрения, необходимо периодически, примерно каждые 2 часа, проводить профилактическую гимнастику для глаз. Гимнастика для глаз включает в себя следующий комплекс упражнений:

- закрыть и расслабить глаза на 2-3 минуты;
- круговые перемещения взгляда сначала по часовой стрелке, затем — против неё;
- горизонтальные и вертикальные перемещения взгляда;
- перемещения взгляда по диагоналям;
- сведение глаз к переносице и разведение глаз в разные стороны;
- попеременное переключение взгляда с близкого к вам предмета на дальний;

— если чувствуется сухость в глазах, то рекомендуется быстрое моргание глазами;

— приложить к глазам холодную салфетку или сходить умыться холодной водой.

Заключение

Сегодня образование невозможно представить без использования современных технологий обучения. Учитывая современные реалии и потребности мирового рынка в высококвалифицированных специалистах различных направлений деятельности, спрос на технологии дистанционного обучения как никогда ранее высок и будет продолжать расти. Но новые технологии несут с собой и новые угрозы информационной безопасности для компьютерных систем и пользователей. В связи с этим технологии дистанционного обучения в своей работе должны использовать современные методы обеспечения информационной безопасности.

В ходе выпускной квалификационной работы были решены следующие задачи:

- проведён анализ требований, применяемых к учебному ресурсу;
- проведена оценка безопасности технологий интеграции дистанционных ресурсов обучения с системами управления обучением;
- спроектирована архитектура и логика функционирования учебного ресурса;
- разработаны модули, из которых состоит учебный ресурс;
- проведено тестирование учебного ресурса;
- разработаны «Руководство по установке» и «Руководство по эксплуатации» учебного ресурса;
- установлены вредные психофизиологические факторы, влияющие на органы зрения специалиста по защите информации, а также определены методы и средства физической культуры, снижающие их воздействие.

При разработке дистанционного учебного ресурса использовались современные технологии веб-разработки и применялись методики разработки безопасного ПО.

По результатам функционального тестирования был сделан вывод, что

учебный ресурс удовлетворяет всем требованиям, поставленным в техническом задании на выпускную квалификационную работу.

Разработанный в рамках выпускной квалификационной работы дистанционный учебный ресурс обеспечивает информационную безопасность как персональных данных пользователей, посещающих учебный ресурс, так и непосредственно содержимого ресурса, то есть учебных курсов. Данный дистанционный учебный ресурс разработан на основе платформы Moodle, добавляя в неё такие механизмы обеспечения информационной безопасности, как:

- управление доступом на основе ролей;
- управление полномочиями доступа пользователей к учебному ресурсу;
- регистрация событий и ведение журнала событий;
- контроль целостности учебного ресурса;
- блокировка доступа к учебному ресурсу по IPv4- и/или IPv6-адресам;
- проверка загружаемых на учебный ресурс файлов на предмет наличия в них вредоносного ПО или деструктивных конструкций;
- защита от SQL-инъекций.

Разработанный дистанционный учебный ресурс может использоваться преподавателями учебных заведений и другими лицами, желающими расширить и углубить учебный процесс обучающихся.

По результатам анализа технологии LTI с точки зрения информационной безопасности была написана статья «Оценка безопасности технологии интеграции дистанционных ресурсов обучения с системой управления обучения Moodle», с которой было принято участие в седьмой Всероссийской межвузовской научно-практической конференции (ВМНПК — 2020). Вышеописанная статья затем была опубликована в «Сборнике статей по

материалам седьмой Всероссийской межвузовской научно-практической конференции» [35].

Все задачи из технического задания на выпускную квалификационную работу были успешно выполнены.

Список используемых источников

1. Положение Пензенского государственного университета от 27.09.2018 № 101-06 «Об электронной информационно-образовательной среде университета». — URL: https://www.pnzgu.ru/files/pnzgu.ru/doki/localnormact/polozhenie_ob_eios.pdf (дата обращения: 05.04.2020).
2. Adobe Captivate Prime LMS. — URL: <https://www.adobe.com/ru/products/captivateprime.html> (дата обращения: 06.04.2020).
3. Looop – The LMS that drives performance. — URL: [https:// www.looop.co/](https://www.looop.co/) (дата обращения: 06.04.2020).
4. Agylia Learning Management System. — URL: [https:// www.agylia.com/](https://www.agylia.com/) (дата обращения: 06.04.2020).
5. Moodle – Open-source learning platform. — URL: <https://moodle.org/> (дата обращения: 06.04.2020).
6. Sakai Learning Management System. — URL: <https://www.sakailms.org/> (дата обращения: 06.04.2020).
7. Canvas the Learning Management Platform. — URL: <https://www.instructure.com/canvas/> (дата обращения: 06.04.2020).
8. Chamilo LMS. — URL: <https://chamilo.org/en/> (дата обращения: 06.04.2020).
9. Open edX: Home. — URL: <https://open.edx.org/> (дата обращения: 06.04.2020).
10. Totara Learning – Freedom to Learn. — URL: <https://www.totaralearning.com/> (дата обращения: 06.04.2020).
11. The GNU General Public License v3.0. — URL: <https://www.gnu.org/licenses/gpl-3.0.en.html> (дата обращения: 06.04.2020).
12. Academic LMS Market Share: A view across four global regions. — URL: <https://eliterate.us/academic-lms-market-share-view-across-four-global-regions/> (дата обращения: 06.04.2020).
13. AICC Document Archive. — URL: <https://github.com/ADL-AICC/>

AICC-Documents-Archive (дата обращения: 06.04.2020).

14. SCORM solved and explained. — URL: <https://scorm.com/> (дата обращения: 06.04.2020).

15. Learning Tools Interoperability Core Specification. — URL: <http://www.imsglobal.org/spec/lti/v1p3/> (дата обращения 06.04.2020).

16. xAPI solved and explained. — URL: <https://xapi.com/> (дата обращения 06.04.2020).

17. Educational Community License. — URL: <https://opensource.org/licenses/ECL-2.0> (дата обращения 06.04.2020).

18. GNU Affero General Public License. — URL: <https://www.gnu.org/licenses/agpl-3.0.en.html> (дата обращения 06.04.2020).

19. Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing: RFC 7230. — URL: <https://tools.ietf.org/html/rfc7230> (дата обращения 06.04.2020).

20. Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content: RFC 7231. — URL: <https://tools.ietf.org/html/rfc7231> (дата обращения 06.04.2020).

21. Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests: RFC 7232. — URL: <https://tools.ietf.org/html/rfc7232> (дата обращения 06.04.2020).

22. Hypertext Transfer Protocol (HTTP/1.1): Range Requests: RFC 7233. — URL: <https://tools.ietf.org/html/rfc7233> (дата обращения 06.04.2020).

23. Hypertext Transfer Protocol (HTTP/1.1): Caching: RFC 7234. — URL: <https://tools.ietf.org/html/rfc7234> (дата обращения 06.04.2020).

24. Hypertext Transfer Protocol (HTTP/1.1): Authentication: RFC 7235. — URL: <https://tools.ietf.org/html/rfc7235> (дата обращения 06.04.2020).

25. HTTP Over TLS: RFC 2818. — URL: <https://tools.ietf.org/html/rfc2818> (дата обращения 06.04.2020).

26. Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols: RFC 3470. — URL: <https://tools.ietf.org/html/rfc3470> (дата обращения 06.04.2020).

27. Adobe's RTMFP Profile for Flash Communication: RFC 7425. — URL:

<https://tools.ietf.org/html/rfc7425> (дата обращения 06.04.2020).

28. The OAuth 2.0 Authorization Framework: RFC 6749. – URL: <https://tools.ietf.org/html/rfc6749> (дата обращения 06.04.2020).

29. OpenID Connect. – URL: <https://openid.net/connect/> (дата обращения 06.04.2020).

30. JSON Web Token (JWT): RFC 7519. – URL: <https://tools.ietf.org/html/rfc7519> (дата обращения 06.04.2020).

31. Cryptographic Algorithms for Digital Signatures and MACs: RFC 7518. – URL: <https://tools.ietf.org/html/rfc7518#section-3> (дата обращения 06.04.2020).

32. Moodle – the world's open source learning platform. – URL: <https://github.com/moodle/moodle> (дата обращения 15.04.2020).

33. Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms: RFC 4357. – URL: <https://tools.ietf.org/html/rfc4357> (дата обращения 20.04.2020).

34. ГОСТ 12.0.003-2015. Система стандартов безопасности труда (ССБТ). Опасные и вредные производственные факторы. Классификация. — М.: Стандартинформ, 2019. — 10 с.

35. Сборник статей по материалам седьмой Всероссийской межвузовской научно-практической конференции / под ред. Л.Р. Фионовой. — Пенза: Издательство ПГУ, 2020. — 425 с.

Приложение А
(обязательное)
Руководство по инсталляции

Учебный ресурс для исследования механизмов обеспечения информационной безопасности реляционных баз данных в языке программирования SQL

Руководство по инсталляции

Пенза 2020

Оглавление

A.1 Введение.....	3
A.2 Системные требования.....	3
A.2.1 Требования к программному обеспечению.....	3
A.2.2 Требования к аппаратному обеспечению.....	3
A.2.3 Требования к конфигурации сервера.....	4
A.3 Подготовка к инсталляции.....	4
A.4 Инсталляция учебного ресурса.....	4
A.4.1 Установка директории с данными учебного ресурса.....	4
A.4.2 Установка базы данных учебного ресурса.....	5
A.4.3 Установка веб-сайта учебного ресурса.....	6
A.4.4 Установка серверного антивируса ClamAV.....	8
A.4.5 Завершение инсталляции.....	8

А.1 Введение

Настоящее «Руководство по инсталляции» предназначено для администратора учебного ресурса. В документе представлена пошаговая инструкция развёртывания учебного ресурса на веб-сервере.

А.2 Системные требования

А.2.1 Требования к программному обеспечению

Для корректной работы учебного ресурса предъявляются следующие требования к программному обеспечению:

- для HTTP-сервера:
 - Apache HTTP Server версии не ниже 2.4.38;
 - PHP не ниже версии 7.3;
- для сервера баз данных — СУБД MySQL версии не ниже 8.0.18 или СУБД MariaDB версии не ниже 10.3.22;
- для клиентского рабочего места — веб-браузер, поддерживающий стандарты HTML5, CSS3 и ECMAScript2017 (ES8).

А.2.2 Требования к аппаратному обеспечению

Для корректной работы учебного ресурса предъявляются следующие минимальные требования к аппаратному обеспечению:

- для HTTP-сервера:
 - 1 ГБ ОЗУ;
 - 400 МБ ПЗУ;
 - 2 ГГц частота процессора;
- для сервера баз данных:
 - 4 ГБ ОЗУ;
 - 2 ГБ ПЗУ;
 - 2,4 ГГц частота процессора;
- для клиентского рабочего места:

- доступ к сети Интернет;
- 2 ГБ ОЗУ;
- 1,5 ГГц частота процессора.

А.2.3 Требования к конфигурации сервера

Для корректной работы учебного ресурса предъявляются следующие требования к конфигурации сервера:

- право создания, изменения, удаления директорий на HTTP-сервере;
- право создания, изменения, удаления баз данных на сервере баз данных;
- право изменения прав доступа на директории;
- право изменения файла `php.ini`.

Для установки и работы серверного антивируса ClamAV дополнительно требуются root-права и доступ к серверу по SSH.

А.3 Подготовка к инсталляции

Перед началом инсталляции учебного ресурса проверьте комплектность файлов. У вас должны быть:

- директория `moodledata` — данные учебного ресурса;
- директория `moodleprovider` – веб-сайт учебного ресурса;
- файл `moodle_provider.sql` – образ базы данных учебного ресурса;
- файл `checksum.txt` — контрольные суммы на таблицы базы данных и файлы учебного ресурса.

А.4 Инсталляция учебного ресурса

А.4.1 Установка директории с данными учебного ресурса

Создайте на сервере директорию `moodledata`.

Установите на директорию `moodledata` права чтения, записи и просмотра для «Owner». Отключите права чтения, записи и просмотра для «Group» и «Public». В числовом виде это правило выглядит как 700.

Загрузите в директорию moodledata (на сервере) содержимое директории moodledata (имеющейся на вашем локальном устройстве). ВНИМАНИЕ: загрузка должна производиться в режиме «Binary».

А.4.2 Установка базы данных учебного ресурса

Создайте базу данных (далее — БД), которая будет использоваться учебным ресурсом. Создайте пользователя, от имени которого учебный ресурс будет выполнять запросы к этой БД. Пользователь должен иметь право чтения и записи в БД. Использовать root-пользователя не рекомендуется.

Выполните импорт файла moodle-provider.sql в БД учебного ресурса. Дождитесь окончания импорта.

Если вы хотите создать, изменить или удалить пользователей учебного ресурса, то выберите таблицу known_users. Данная таблица имеет следующие столбцы:

- first_name — имя пользователя; обязателен к заполнению;
- last_name — фамилия пользователя; обязателен к заполнению;
- email_address — электронная почта пользователя; обязателен к заполнению;
- user_active — право доступа пользователя к учебному ресурсу; укажите TRUE, чтобы разрешить пользователю доступ к учебному ресурсу, и FALSE, чтобы запретить; обязателен к заполнению;
- user_role — роль пользователя; «admin» для администратора, «teacher» для преподавателя; обязателен к заполнению;
- user_login — логин пользователя; обязателен к заполнению;
- user_id — идентификатор пользователя; устанавливается автоматически
- last_login_time — время последнего входа пользователя на учебный ресурс; не обязателен к заполнению;
- last_logout_time — время последнего выхода пользователя с учебного

ресурса; не обязателен к заполнению;

- moodle_id – идентификатор пользователя в Moodle; не обязателен к заполнению;

- lastip – IP-адрес пользователя, с которого он последний раз посещал учебный ресурс; не обязателен к заполнению.

ВНИМАНИЕ: создавайте только пользователей с ролями «администратор» и «преподаватель»; политика безопасности учебного ресурса разрешает доступ к ресурсу пользователям с ролью «студент» только через интерфейс LTI (в связи с угрозой несанкционированного повышения привилегий).

А.4.3 Установка веб-сайта учебного ресурса

Создайте на сервере домен или поддомен или выберите уже имеющийся. Далее данный домен или поддомен будет называться «корневая директория».

Установите на корневую директорию права чтения, записи и просмотра для «Owner». Установите права чтения и просмотра для «Group» и «Public». В числовом виде это правило выглядит как 755.

Загрузите в корневую директорию содержимое директории moodleprovider. **ВНИМАНИЕ:** загрузка должна производиться в режиме «Binary».

После загрузки файлов перейдите в корень директории. Выберите файл config.php и измените его следующим образом:

- в значении переменной \$CFG->dbhost укажите название сервера ваших баз данных;

- в значении переменной \$CFG->dbname укажите название базы данных, которая будет использоваться учебным ресурсом;

- в значении переменной \$CFG->dbuser укажите пользователя, от имени которого будет выполняться доступ к базе данных учебного ресурса; пользователь должен иметь право чтения и записи в базу данных; использовать

для этих целей root-пользователя не рекомендуется;

- в значении переменной `$CFG->dbpass` укажите пароль от базы данных;

- в значении переменной `$CFG->wwwroot` укажите URL корневой директории учебного ресурса;

- в значении переменной `$CFG->dataroot` укажите путь от корня сервера до папки с данными учебного ресурса (например, `/home/www/moodledata/`, `/var/www/moodledata/`, `/var/public_html/moodledata/`).

Перейдите в директорию `{wwwroot}/services`. Выберите файл `custom_config.php` и измените его следующим образом:

- в значении переменной `$servername` укажите название сервера ваших баз данных;

- в значении переменной `$dbname` укажите название базы данных, которая будет использоваться учебным ресурсом;

- в значении переменной `$username` укажите пользователя, от имени которого будет выполняться доступ к базе данных учебного ресурса; пользователь должен иметь право чтения и записи в базу данных; использовать для этих целей root-пользователя не рекомендуется;

- в значении переменной `$password` укажите пароль от базы данных.

После вышеописанных действий зайдите на учебный ресурс. В левом верхнем углу можно переключить язык сайта. Перейдите на страницу `{wwwroot}/admin/tool/replace/index.php` и выполните замену «`http://localmoodleprovider.atwebpages.com`» на URL вашего учебного ресурса.

Если учебный ресурс находится в режиме технического обслуживания (Maintenance mode), то перейдите к `{wwwroot}/admin`, выберите раздел «Сервер», затем выберите «Режим технического обслуживания» и отключите его.

На учебном ресурсе созданы 2 пользователя: один администратор (логин

admin) и один преподаватель (логин mali.v.a). Пароль у пользователей: LlkMT13hffs_prng. Рекомендуется сменить пароли пользователей.

Вы можете создавать, изменять и удалять пользователей, перейдя на вкладку «Администрирование» > «Пользователи» > «Учётные записи» > «Список пользователей». ВНИМАНИЕ: создавайте только пользователей с ролями «администратор» и «преподаватель»; политика безопасности учебного ресурса разрешает доступ к ресурсу пользователям с ролью «студент» только через интерфейс LTI (в связи с угрозой несанкционированного повышения привилегий).

Проверьте, чтобы записи о локальных пользователях в таблице known_users базы данных учебного ресурса совпадали с созданными на учебном ресурсе пользователями.

А.4.4 Установка серверного антивируса ClamAV

Серверный антивирус ClamAV устанавливается по желанию администратора для проверки загружаемых на учебный ресурс файлов на предмет наличия в них вредоносного ПО и/или деструктивных конструкций.

Установка серверного антивируса специфична в каждом отдельном случае, в связи с чем установку антивируса производить стоит в соответствии с его документацией: <https://www.clamav.net/documents/clam-antivirus-user-manual>.

Для установки серверного антивируса требуется право подключения к серверу по SSH.

А.4.5 Завершение инсталляции

Выполните вход от имени администратора учебного ресурса. Перейдите в модуль управления учебным ресурсом {wwwroot}/services/admin_module.php. Выберите «Контроль целостности». Сравните вычисленные контрольные суммы с эталонными контрольными суммами, представленными в файле checksum.txt, находящемся на вашем локальном устройстве в исходной директории файлов учебного ресурса. Вычисленные контрольные суммы могут различаться с эталонными у следующих объектов учебного ресурса и по

следующим причинам:

- таблица `known_users` – обновилась дата вашего входа в систему и IP-адрес;
- `eventlog.txt` – в файл записано событие вашего входа в систему;
- `checksum.txt` – если вы уже сохранили рассчитанные контрольные суммы в файл;
- `custom_config.php` – вы изменили переменные в файле в соответствии с настройками своего сервера.

Несоответствие вычисленных и эталонных контрольных сумм у вышеперечисленных файлов не сигнализирует об ошибках при инсталляции.

Если отличаются контрольные суммы отдельных файлов, то удалите эти файлы и загрузите их заново из исходной директории файлов учебного ресурса. Если ситуация повторяется, либо файлов с контрольной суммой, отличающейся от эталонной, много, то возможны следующие ситуации:

- файлы в исходной директории учебного ресурса повреждены; необходимо получить целые файлы;
- установка учебного ресурса была проведена некорректно; необходимо удалить все установленные файлы и провести инсталляцию заново;
- загрузка файлов выполнялась не в режиме «Binary» и файлы при загрузке на сервер были повреждены; необходимо удалить все установленные файлы и провести инсталляцию заново, загружая файлы на сервер в режиме «Binary».

Приложение Б
(обязательное)
Руководство по эксплуатации

Учебный ресурс для исследования механизмов обеспечения информационной безопасности реляционных баз данных в языке программирования SQL

Руководство по эксплуатации

Пенза 2020

Оглавление

Б.1 Введение.....	3
Б.2 Краткое описание и принципы работы.....	3
Б.3 Правила обслуживания.....	3
Б.4 Функционал администратора.....	4
Б.4.1 Общие сведения о функционале администратора.....	4
Б.4.2 Управление полномочиями доступа пользователей.....	5
Б.4.3 Просмотр журнала событий учебного ресурса.....	7
Б.4.4 Контроль целостности учебного ресурса.....	7
Б.4.5 Блокировка IP-адресов.....	9
Б.5 Функционал преподавателя.....	9
Б.5.1 Управление учебными курсами и их контентом.....	9
Б.5.2 Разрешение доступа к курсам и контенту с других учебных платформ.....	10

Б.1 Введение

Настоящее «Руководство по эксплуатации» предназначено для администратора и преподавателя учебного ресурса. В документе представлены обслуживание учебного ресурса и функционал, доступный администратору и преподавателю.

Б.2 Краткое описание и принципы работы

Учебный ресурс для исследования механизмов обеспечения информационной безопасности реляционных баз данных в языке программирования SQL (далее — учебный ресурс) — это ресурс, содержащий тестовое задание, определяющее уровень знаний студента о возможностях СУБД MySQL и MariaDB в вопросах защиты данных, хранящихся в базах данных. В учебном ресурсе реализованы механизмы обеспечения информационной безопасности, обеспечивающие конфиденциальность данных, хранящихся на нём.

Учебный ресурс спроектирован в архитектурном стиле REST, используя такие стандарты, как HTTP, URL, JSON, XML. Взаимодействие с пользователями реализовано в виде REST-запросов и REST-ответов.

Контент учебного ресурса может быть свободно изменён под конкретные нужды, оставаясь при этом надёжно защищённым.

Привилегированные пользователи (администраторы и преподаватели) выполняют вход на учебный ресурс через веб-интерфейс учебного ресурса; студенты выполняют вход на учебный ресурс через интерфейс LTI.

Б.3 Правила обслуживания

Являясь программным обеспечением, учебный ресурс не нуждается в периодическом техническом обслуживании. Администратору достаточно периодически контролировать журнал событий, а также производить контроль целостности для удостоверения в корректности работы учебного ресурса.

При возникновении ошибок при работе с учебным ресурсом или при некорректной его работе администратор может перевести учебный ресурс в

режим технического обслуживания (во время которого к ресурсу может получить доступ только администратор) для поиска неисправностей и восстановления работоспособности учебного ресурса. Перевести учебный ресурс в режим технического обслуживания администратор может, перейдя в раздел «Администрирование» > «Сервер» > «Режим технического обслуживания». Вывод учебного ресурса из режима технического обслуживания производится там же. На рисунке Б.1 представлен интерфейс перевода учебного ресурса в режим технического обслуживания.

SQL Tool Provider

[Личный кабинет](#) / [Администрирование](#) / [Сервер](#) / [Режим технического обслуживания](#)

Режим технического обслуживания

Режим технического обслуживания
maintenance_enabled

Отключить ▾

Значение по умолчанию: Отключить

Для обновления и других работ по обслуживанию системы

Рисунок Б.1 — Интерфейс перевода учебного ресурса в режим технического обслуживания

Б.4 Функционал администратора

Б.4.1 Общие сведения о функционале администратора

У администратора есть два метода управления учебным ресурсом:

- «Администрирование» - панель управления, доступная из личного кабинета администратора; в данной панели управления администратор решает все типичные административные задачи: создание/изменение/удаление пользователей и контента учебного ресурса; установка времени продолжительности пользовательской сессии; включение режима технического обслуживания и другое;
- «Модуль управления учебным ресурсом» - модуль учебного ресурса, позволяющий администратору настроить политики безопасности

учебного ресурса: полномочия доступа пользователей, просмотр журнала событий, контроль целостности, блокировка IP-адресов; модуль управления учебным ресурсом доступен по адресу `./services/admin_module.php`.

На рисунке Б.2 представлен интерфейс модуля управления учебным ресурсом.

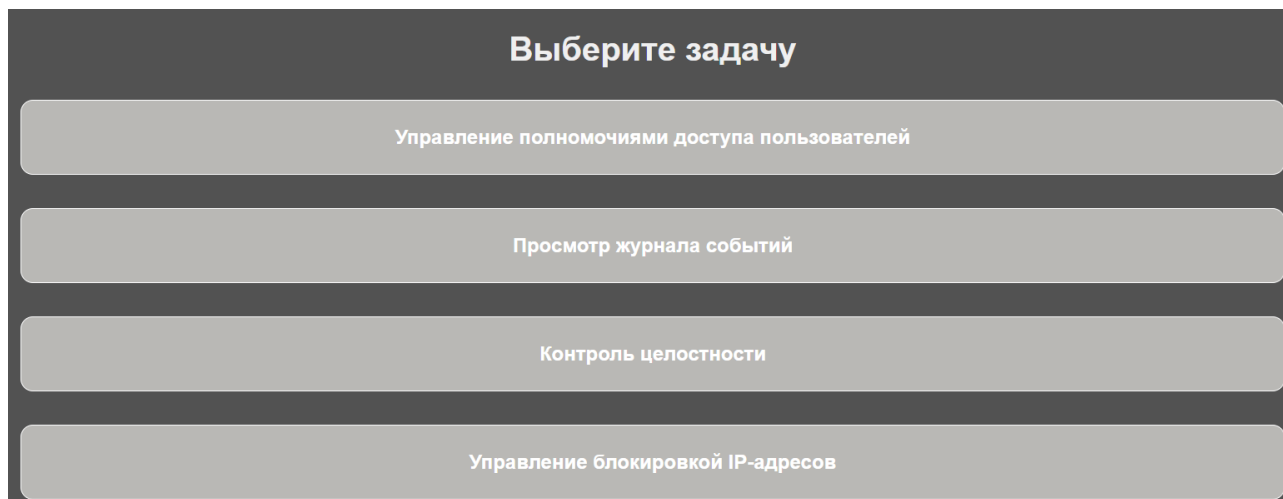


Рисунок Б.2 — Интерфейс модуля управления учебным ресурсом

Б.4.2 Управление полномочиями доступа пользователей

Администратор может управлять правами чтения и записи у пользователей.

Право записи имеют только администратор и преподаватель, при этом право записи у администратора отключить нельзя (иначе он потеряет возможность управления учебным ресурсом). Право записи преподавателей настраивается переходом в раздел «Администрирование» > «Пользователи» > «Права» > «Назначить глобальные роли». Для того, чтобы отключить у преподавателя право записи на учебном ресурсе, необходимо удалить его из «Создателей курса». Соответственно, для добавления преподавателю права на запись его необходимо внести в группу «Создатели курса».

Право доступа (право чтения учебного ресурса) имеют все пользователи учебного ресурса, при этом право доступа у администратора отключить нельзя (иначе он потеряет возможность управления учебным ресурсом). Право доступа у студентов и преподавателей настраивается переходом в «Модуль управления

учебным ресурсом» > «Управление полномочиями доступа пользователей». На рисунке Б.3 представлен интерфейс управления полномочиями доступа пользователей.

Управление полномочиями доступа пользователей

Блокировка с указанием параметров

Логин (l):

email (t):

Роль (r):

Имя:

Фамилия:

Заблокированные пользователи

ID	Имя	Фамилия	Эл. почта	Роль	Логин	Последний вход	Последний выход	IP-адрес	Действие
2	Vladimir	Mali	advancytheslayer@gmail.com	teacher	mali.v.a	2020-05-29 15:50:40	2020-05-29 00:26:39	127.0.0.1	<input type="button" value="Заблокировать"/>

Активные пользователи

ID	Имя	Фамилия	Эл. почта	Роль	Логин	Последний вход	Последний выход	IP-адрес	Действие
2	Vladimir	Mali	advancytheslayer@gmail.com	teacher	mali.v.a	2020-05-29 15:50:40	2020-05-29 00:26:39	127.0.0.1	<input type="button" value="Заблокировать"/>

Рисунок Б.3 — Интерфейс управления полномочиями доступа пользователей

Управление полномочиями (правом) доступа пользователей администратор может производить двумя способами:

— самостоятельным вводом данных о пользователе, которого необходимо заблокировать или разблокировать; при таком способе обязательными параметрами являются «Логин», «email» и «Роль»;

— нажатием кнопок «Разблокировать» или «Заблокировать» напротив пользователей в таблицах «Заблокированные пользователи» и «Активные пользователи», представленных на веб-странице.

При самостоятельном вводе данных обязательными параметрами являются «Логин», «email» и «Роль»; дополнительно для блокировки пользователя можно указать параметры «Имя» и «Фамилия» (если параметры оставлены пустыми, то они будут заменены на «%DEFAULT%»). «Имя» и «Фамилия» будут использоваться программой только при создании новой записи о заблокированном пользователе (т. к. для однозначной идентификации пользователя достаточно комбинации электронной почты, логина и его роли).

Б.4.3 Просмотр журнала событий учебного ресурса

Администратор может просмотреть журнал событий, перейдя в «Модуль управления учебным ресурсом» > «Просмотр журнала событий». На рисунке Б.4 представлен интерфейс просмотра журнала событий.

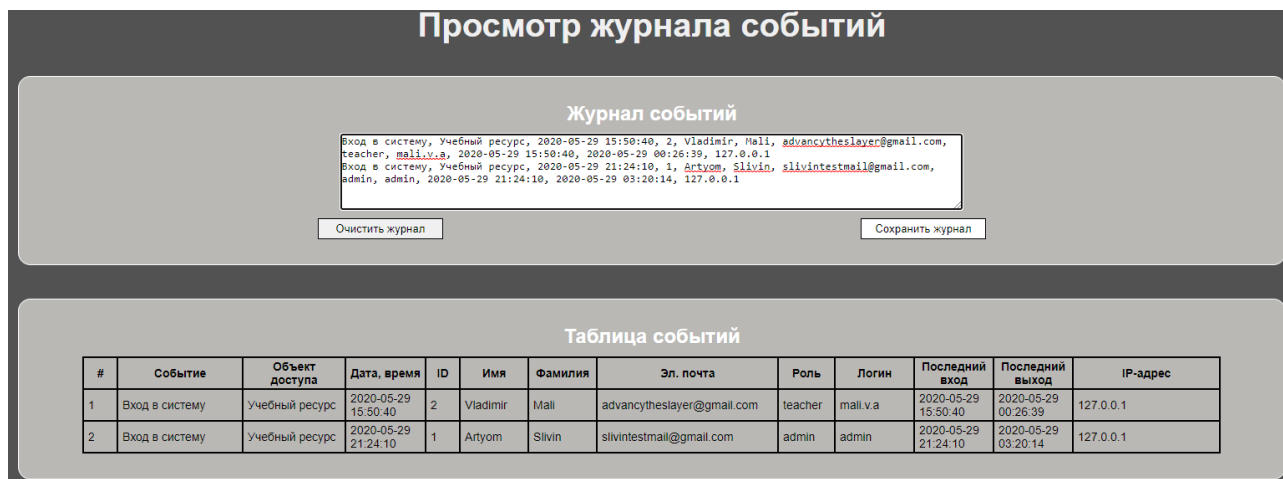


Рисунок Б.4 — Интерфейс просмотра журнала событий

Журнал событий представлен администратору в двух видах:

— непосредственно содержимое файла журнала событий; администратор может либо изменить содержимое файла, после чего нажать кнопку «Сохранить журнал» для применения изменений, либо очистить журнал событий, нажав кнопку «Очистить журнал»;

— таблица событий, в которой содержимое журнала событий представлено в удобном для чтения виде.

Журнал событий (файл eventlog.txt) находится на учебном ресурсе в директории *./services/admin/*.

Б.4.4 Контроль целостности учебного ресурса

Механизм контроля целостности доступен администратору в разделе «Модуль управления учебным ресурсом» > «Контроль целостности». На рисунке Б.5 представлен интерфейс контроля целостности учебного ресурса.

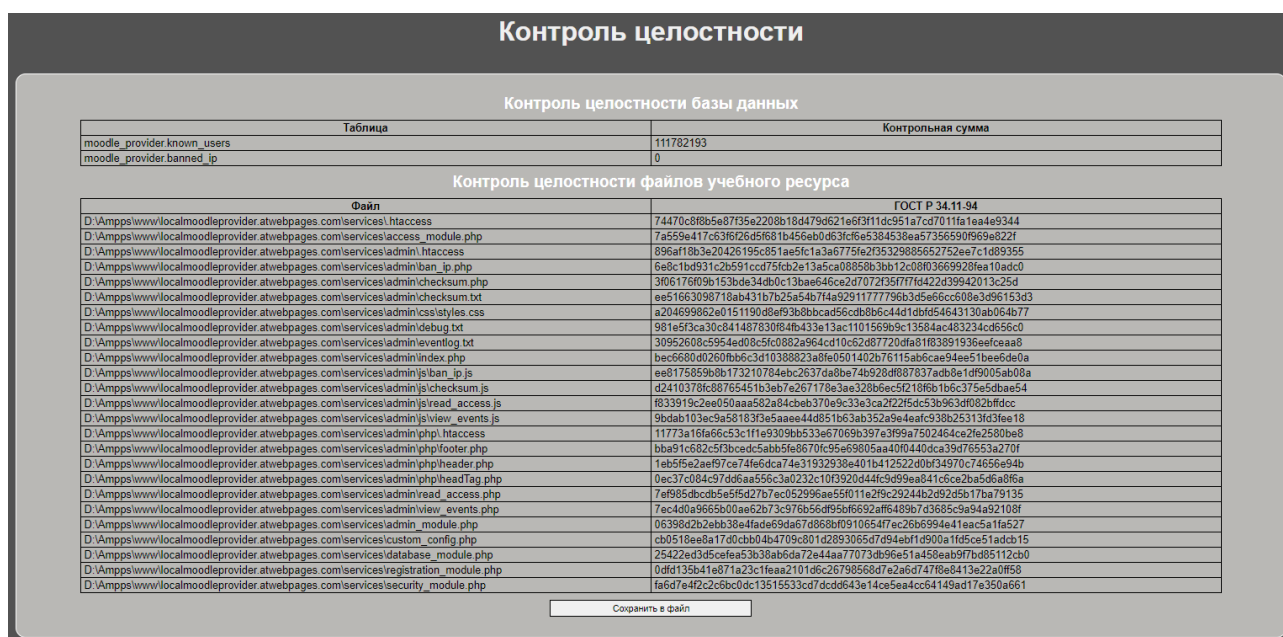


Рисунок Б.5 — Интерфейс контроля целостности учебного ресурса

Механизм контроля целостности учебного ресурса может использоваться администратором для достижения следующих целей:

- при инсталляции учебного ресурса — убедиться, что файлы не были заранее подменены, а также не были повреждены во время их передачи или установки;
- при эксплуатации учебного ресурса — убедиться в том, что файлы не были несанкционированно изменены.

По умолчанию MySQL версии 8.0.18 и выше и MariaDB версии не ниже 10.3.22 для расчёта контрольных сумм таблиц баз данных используют алгоритм CRC32. Однако доступные алгоритмы расчёта контрольных сумм в разных версиях вышеописанных СУБД отличаются и могут быть заданы хостингом самостоятельно.

Контрольные суммы для файлов модулей учебного ресурса рассчитываются в виде криптографической хеш-функции ГОСТ Р 34.11-94 с параметрами из RFC 4357 (раздел 11.2).

Администратор может сохранить рассчитанные контрольные суммы в файл checksum.txt, нажав на веб-странице кнопку «Сохранить в файл». Файл checksum.txt находится на учебном ресурсе в директории ./services/admin/.

Б.4.5 Блокировка IP-адресов

Механизм блокировки IP-адресов (IPv4 и IPv6) доступен администратору в разделе «Модуль управления учебным ресурсом» > «Управление блокировкой IP-адресов». На рисунке Б.6 представлен интерфейс управления блокировкой IP-адресов.

Известные IP-адреса						
Эл. почта	Роль	Логин	Последний вход	Последний выход	IP-адрес	Действие
slivintestmail@gmail.com	admin	admin	2020-05-29 21:24:10	2020-05-29 03:20:14	127.0.0.1	Заблокировать
advancytheslayer@gmail.com	teacher	mail.v.a	2020-05-29 15:50:40	2020-05-29 00:26:39	127.0.0.1	Заблокировать

Рисунок Б.6 — Интерфейс управления блокировкой IP-адресов

Управление блокировкой IP-адресов администратор может производить двумя способами:

- самостоятельным вводом IP-адреса, который необходимо заблокировать или разблокировать;
- нажатием кнопок «Разблокировать» или «Заблокировать» напротив IP-адресов в таблицах «Заблокированные IP-адреса» и «Известные IP-адреса», представленных на веб-странице.

Б.5 Функционал преподавателя

Б.5.1 Управление учебными курсами и их контентом

Модуль контроля учебного процесса обеспечивает преподавателей учебного ресурса функционалом для настройки и наблюдения за учебным процессом. Все пользователи учебного ресурса, которым присвоена роль «преподаватель», могут создавать и модифицировать курсы учебного ресурса (однако право создания и изменения курсов и заданий может у вас быть

отключено администратором).

Для создания нового учебного курса из личного кабинета перейдите в «Администрирование» > «Управление курсами и категориями». На рисунке Б.7 представлен интерфейс управления курсами и категориями.

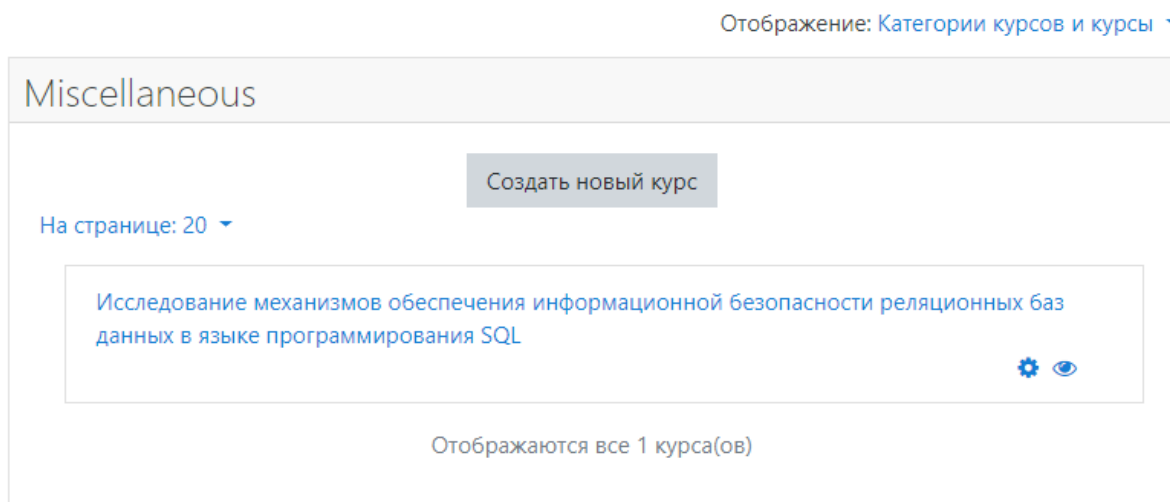


Рисунок Б.7 — Интерфейс управления курсами и категориями

На появившейся странице нажмите «Создать новый курс», после чего заполните все обязательные поля.

Для изменения настроек учебного курса из своего личного кабинета перейдите в раздел «Домашняя страница». В разделе «Доступные курсы» выберите курс, который вы хотите изменить. Перейдя на страницу курса, в настройках курса вы можете выбрать нужное вам действие, как показано на рисунке Б.8 (значок шестерни).

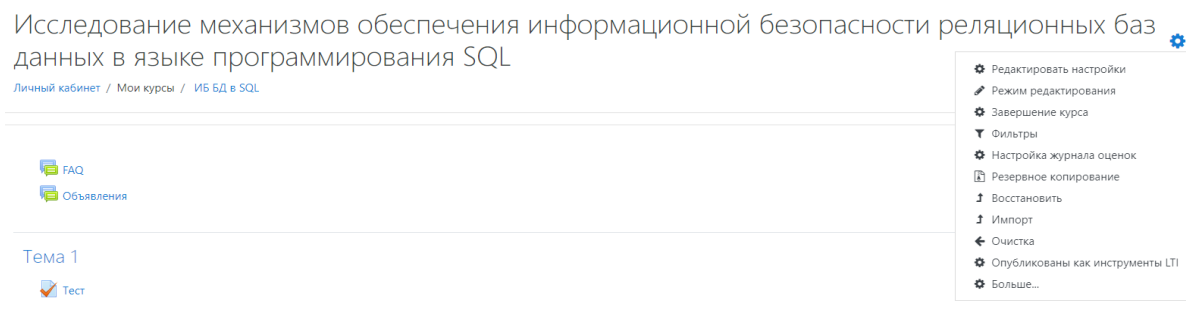


Рисунок Б.8 — Вызов меню управления курсом

Для изменения контента учебного курса из своего личного кабинета перейдите в раздел «Домашняя страница». В разделе «Доступные курсы»

выберите курс, который вы хотите изменить. Перейдя на страницу курса, в настройках курса выберите «Режим редактирования» (значок шестерни > «Режим редактирования»). Затем нажмите «Редактировать» напротив объекта, который вы хотите модифицировать, и выберите нужное вам действие, или «Добавить элемент или ресурс», если вы хотите создать новый объект.

Преподаватели не могут удалять созданные курсы. Для удаления курса обратитесь к администратору учебного ресурса.

Нажав на панели слева раздел «Оценки», преподаватели получают доступ к журналу оценок. Журнал оценок предоставляет широкие возможности фильтрации, сортировки, поиска, просмотра статистики определённых студентов или определённых заданий. На рисунке Б.9 представлен интерфейс журнала оценок.

Отчет по оценкам

Просмотр Настройки Шкалы Буквы Импорт Экспорт

Отчет по оценкам История оценок Отчет по показателям Обзорный отчет Одиночный вид Отчет по пользователю

Все участники: 1/1

Имя Все А Б В Г Д Е Ё Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Э Ю Я

Фамилия Все А Б В Г Д Е Ё Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Э Ю Я

		Исследование механизм...	
Имя / Фамилия	Адрес электронной почты	Тест	Итоговая оценка за курс
Ученик Прилежный	unusalspecimen70@gmail.com	10,00	10,00
Общее среднее		10,00	10,00

Рисунок Б.9 — Интерфейс журнала оценок

Б.5.2 Разрешение доступа к курсам и контенту с других учебных платформ

Б.5.2.1 Управление объектами со стороны платформы-провайдера услуг.

Если вы хотите разрешить доступ к курсам или их контенту для пользователей с других учебных платформ, то выполните следующие шаги:

— перейдите в раздел «Домашняя страница». В разделе «Доступные курсы» выберите курс, который вы хотите изменить. Перейдя на страницу курса, в настройках курса выберите «Опубликованы как инструменты LTI»;

— если вы хотите убрать доступ к объекту с других учебных платформ, то нажмите «удалить» напротив объекта (значок корзины);

— если вы хотите изменить параметры доступа к объекту с других учебных платформ, то нажмите «редактировать» напротив объекта (значок шестерни);

— если вы хотите разрешить доступ к объекту с других учебных платформ, то нажмите кнопку «Добавить» внизу раздела «Опубликованные инструменты»; в появившемся окне укажите объект, к которому вы хотите разрешить доступ и заполните представленные поля формы «Опубликовать как инструмент ЛТИ»; запишите для себя сгенерированное значение из поля «Секретный ключ» (его можно изменить, но этого делать не рекомендуется в целях безопасности подключения); после вышеописанных действий нажмите кнопку «Добавить способ».

Пример настройки разрешения доступа к курсу с других учебных платформ представлен на рисунке Б.10.

Для того, чтобы просмотреть параметры созданного ЛТИ-объекта, перейдите на страницу курса и в настройках курса выберите «Опубликованы как инструменты ЛТИ».

Б.5.2.2 Управление объектами со стороны платформы-потребителя услуг.

Если вы хотите добавить в ваш курс объект с другой учебной платформы, то выполните следующие шаги:

— из своего личного кабинета перейдите в раздел «Домашняя страница»;

— в разделе «Доступные курсы» выберите курс, в который вы хотите добавить новый объект;

— перейдя на страницу курса, в настройках курса выберите «Режим редактирования» (значок шестерни > «Режим редактирования»);

— нажмите «Добавить элемент или ресурс»;

▼ Опубликовать как инструмент LTI

Название способа	<input type="text" value="Курс по ИБ БД"/>
Инструмент, который должен быть опубликован	<input type="text" value="Курс"/>
Продолжительность обучения	<input type="text" value="0"/> дн. ☐ Включить
Дата начала	<input type="text" value="29"/> <input type="text" value="Май"/> <input type="text" value="2020"/> <input type="text" value="21"/> <input type="text" value="51"/> ☐ Включить
Дата окончания	<input type="text" value="29"/> <input type="text" value="Май"/> <input type="text" value="2020"/> <input type="text" value="21"/> <input type="text" value="51"/> ☐ Включить
Максимальное число записанных пользователей	<input type="text" value="0"/>
Роль для учителя	<input type="text" value="Студент"/>
Роль для студента	<input type="text" value="Студент"/>

▼ Внешняя система

Секретный ключ	<input type="text" value="abcdefghijklmnopqrstuvwxyz12"/>
Синхронизация оценок	<input type="text" value="Да"/>
Требуется завершение выполнения курса или элемента до синхронизации оценок	<input type="text" value="Нет"/>
Синхронизация пользователей	<input type="text" value="Да"/>
Режим синхронизации пользователей	<input type="text" value="Зачислять новых и отчислять отсутствующих пользователей"/>

► Значения по умолчанию для пользователей

Рисунок Б.10 — Пример настройки разрешения доступа к курсу с других учебных платформ

- выберите «Внешний инструмент»;
- в открывшемся окне заполните поле «Название элемента курса»; объект будет отображаться в вашем курсе под этим названием;
- получите от создателя объекта, который вы хотите добавить в свой учебный ресурс, URL картриджа интересующего вас объекта и вставьте его в поле «URL-адрес запуска / URL картриджа»;
- в поле «Ключ клиента» укажите, под каким названием ваша учебная платформа будет отображаться у платформы-провайдера при интеграции её учебного объекта в ваш курс;

- получите от создателя объекта, который вы хотите добавить в свой учебный ресурс, секретный ключ LTI-объекта и внесите это значение в поле «Общий секретный ключ»;

- остальные поля опциональны и настраиваются по вашему желанию;

- нажмите «Сохранить и вернуться к курсу»;

- попробуйте подключиться к внешнему объекту через созданный в вашем курсе LTI-объект;

- если при подключении к внешнему объекту вы получаете XML файл, то получите от создателя объекта, который вы хотите добавить в свой учебный ресурс, URL-адрес запуска интересующего вас объекта, нажмите «Редактировать» напротив созданного LTI-объекта и в поле «URL-адрес запуска / URL картриджа» вставьте URL-адрес запуска интересующего вас объекта;

- попробуйте подключиться к внешнему объекту через созданный в вашем курсе LTI-объект; если вы по-прежнему не получаете доступ к внешнему объекту, то в процессе настройки LTI-объекта была допущена ошибка; необходимо удалить созданный вами LTI-объект из курса и выполнить вышеописанные шаги заново.

Пример добавления в курс объекта с другой учебной платформы представлен на рисунке Б.11.

Общее

Название элемента курса

Описание элемента курса

Предварительно настроенный инструмент

URL-адрес запуска/URL картриджа

URL-адрес защищенного запуска

Контейнер запуска

Ключ клиента

Общий секретный ключ



Внешний курс по ИБ БД



Rich text editor toolbar with icons for undo, redo, bold, italic, bulleted list, numbered list, link, unlink, image, video, audio, and source code. Below the toolbar is a large empty text area for the description.

☐ Отображать описание / вступление на странице курса ! ?

☒ Отображать название элемента курса при запуске ! ?

☐ Отображать описание элемента курса при запуске ! ?



Автоматически, на основе URL запуска + - x

Выбрать содержимое



http://localmoodleprovider.atwebpages.com/enrol/lti/cartridge.php/3/b?

✓ Испо.



Empty text input field for the protected launch URL.



В новом окне



ЗИОС ПГУ



Text input field for the common secret key, currently showing masked characters (dots).



Нажмите Enter, чтобы сохранить изменения

Рисунок Б.11 — Пример добавления в курс объекта с другой учебной платформы