

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

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет информационных
технологий и электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.03 -

Информационная безопасность
автоматизированных систем

Специализация -

Защищенные автоматизированные
системы управления

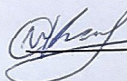
ДИПЛОМНЫЙ ПРОЕКТ

на тему

ЗАЩИЩЕННЫЙ ВИРТУАЛЬНЫЙ СТЕНД

ДЛЯ ДИСТАНЦИОННОГО ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

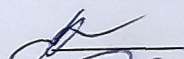
Студент

 Кошелев Максим Сергеевич

Руководитель

 Иванов А.П.

Нормоконтролер

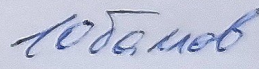
 Егорова Н.А.

Рецензент зам. генерального директора АО «ПНИЭИ»

 Сомкин С.А.

Работ допущена к защите (протокол заседания кафедры от 10.06.22г. №

9)

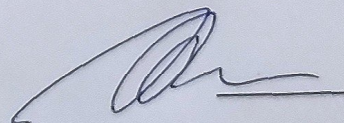


Заведующий кафедрой

 Зефирова С.Л.

Работа защищена с отметкой хорошо (протокол заседания ГЭК от 23.06.22г. № 7)

Секретарь ГЭК

 Иванов А.П.

Пенза 2022

Содержание

Введение.....	3
1 Анализ используемых технологий виртуализации.....	5
1.1 Предыстория виртуализации.....	5
1.2 Основные виды виртуализации.....	6
1.3 Выбор технологии виртуализации лабораторного стенда.....	9
1.4 Описание выбранной технологии виртуализации.....	10
2 Разработка структуры виртуального стенда.....	13
3 Разработка дерева событий виртуального стенда.....	20
4 Разработка виртуального стенда.....	22
5 Внедрение защитных мер виртуального стенда.....	26
5.1 Выявление угроз информационной безопасности для защищенного виртуального стенда для дистанционного выполнения лабораторных работ.....	26
5.2 Описание, разработка и внедрение защитных мер в виртуальный стенд.....	31
6 Проверка работоспособности виртуального стенда и действие его защитных средств.....	37
7 Вредные психофизические факторы, влияющие на органы зрения специалиста по информационной безопасности. Методы и средства физической культуры, снижающие их воздействие.....	49
Заключение.....	52
Список используемых источников.....	53

Введение

Виртуализация — это процесс создания виртуального (программного) представления выбранных ресурсов без привязки к аппаратному обеспечению. Наиболее популярным вариантами является виртуализация серверов, систем хранения данных, приложения и рабочие столы. Одним из самых главных достоинств виртуализации является их независимость. Виртуализированное программное обеспечение требует минимум физических ресурсов, чем полноценная система, не создает конфигурационных файлов, не загромождает реестр и не засоряет систему [1].

Такая технология имеет большой ряд преимуществ:

- совместное использование ресурсов несколькими операционными системами;
- в случае инцидента легко восстановить данные с помощью системы резервного копирования;
- безопасная и удобная среда для тестирования приложений и обучения персонала.

Целью настоящего дипломного проекта является разработка защищенного виртуального стенда для дистанционного выполнения лабораторных работ. Стенд предназначен для получения студентами специальности 10.05.03 — «Информационная безопасность автоматизированных систем» практических навыков в исследовании технического канала утечки информации по электромагнитным наводкам на соседние цепи в ходе выполнения лабораторного практикума по дисциплине «Техническая защита информации» с использованием дистанционных образовательных технологий.

Актуальность темы дипломного проекта заключается в том, что разработанное приложение доступно из любой точки мира, где есть сеть

Интернет. В случае незапланированного перевода Пензенского государственного университета на дистанционный формат обучения — данная технология позволит преподавателям также эффективно выполнять свою работу по обучению, за счёт чего процесс обучения студентов останется понятным и интересным, сохраняя все требования по выполнению учебной программы.

Защитные меры, внедренные в виртуальный стенд, закрывают угрозы, через которые может быть осуществлена компрометация методических материалов Пензенского государственного университета, а так же устанавливают честный порядок выполнения лабораторной работы студентами.

В дипломном проекте были использованы следующие методы исследования:

- анализ;
- моделирование;
- разработка;
- описание.

1 Анализ используемых технологий виртуализации

1.1 Предыстория виртуализации

Идея виртуализировать аппаратное обеспечение не новая, она берёт своё начало из 1960-х годов. Американская компания IBM, которая является одним из самых крупных производителей и поставщиков программного и аппаратного обеспечения, потратило очень много сил и времени на реализацию концепции под названием «Разделение времени». Суть концепции заключалась в том, что пользователи одновременно могли пользоваться процессором благодаря непрерывному сверхскоростному переключению контекстов. Благодаря проведенному исследованию было выявлено, что каждый пользователь успевает использовать лишь малую часть возможностей своего компьютера. Учитывая, что в те времена компьютер стоил очень большие деньги и занимал всю комнату — идея использовать его возможности по максимуму казалась целесообразной [2].

Параллельно с этими событиями департамент электротехники Университета Манчестера реализует проект, целью которого является возможность исполнения нескольких программ одновременно. Исследование проводилось на суперкомпьютере под названием «Atlas», в котором процессы были разделены. Данные исследования стали первыми шагами по созданию принципов, используемых в современной виртуализации [3].

Современные принципы виртуализации тоже построены на совместном использовании ресурсов машины, но с поддержанием логического разделения. В статье «Формальные требования к виртуализируемым архитектурам третьего поколения» Джеральд Попек и Роберт Голдберг вывели первую модель виртуализации, которая заложила основы применяемых по сегодняшний день концепций. Статья содержит базовые

принципы виртуализации и классификацию различных машинных команд. На рисунке 1 представлен обзор вышеупомянутых концепций.

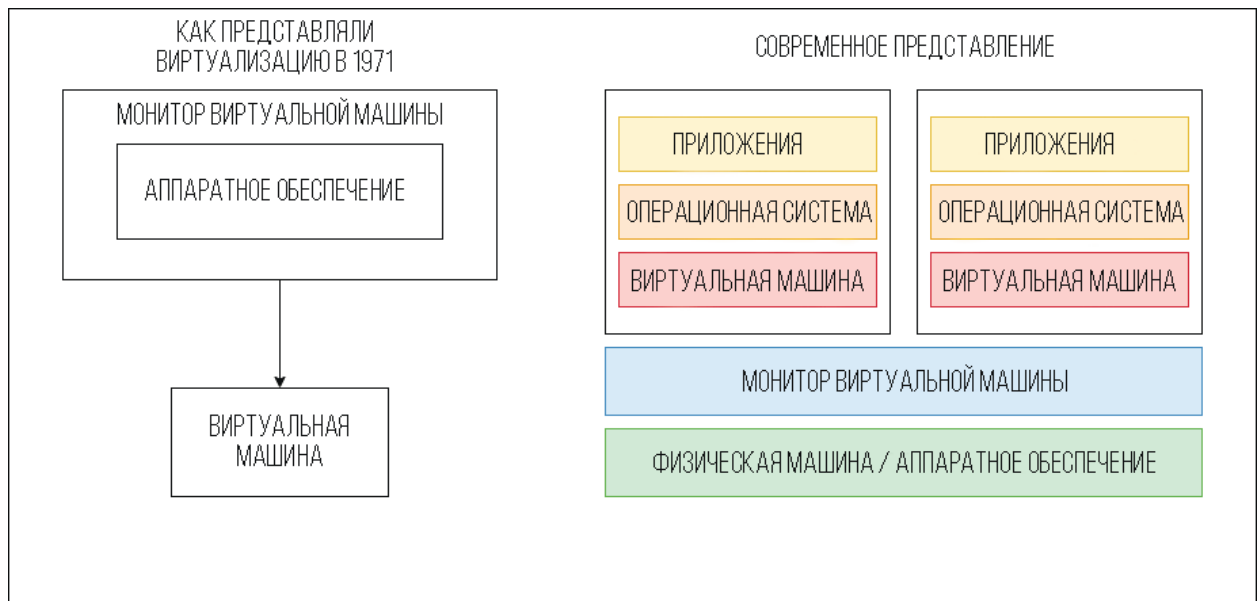


Рисунок 1 — Обзор концепций виртуализации в 1971 году
и в настоящее время

1.2 Основные виды виртуализации

Существует 3 основных принципа виртуализации:

- виртуализация представлений;
- виртуализация приложений;
- виртуализация серверов.

Виртуализация приложений является популярной технологией виртуализации. Самым понятным примером является терминальная служба Windows Server. Терминальный сервер представляет свои ресурсы клиентам, клиентское приложение выполняется на сервере, в то время как пользователь видит только «картинку», то есть представление. Такая технология позволяет снизить требования к программному и аппаратному обеспечению клиента, снижает требования к пропускной способности сети, а так же позволяет повысить безопасность.

В качестве оборудования могут использоваться компьютеры даже с самыми низкими характеристиками или смартфоны, но существуют и специализированные клиенты.

Например, рабочее место сотрудника можно оборудовать при помощи розетки Legrand, установленной в короб, монитора, клавиатуры и компьютерной мыши. Как было написано выше — для работы необязательно иметь высокоскоростное подключение к локальной сети. Достаточно пропускной способности в 15-20 кбит/с.

Уровень безопасности данной технологии находится на высоком уровне. Пользователем можно разрешить запускать только ограниченный набор приложений и запретить устанавливать собственные. Конечно, так можно сделать и на обычном персональном компьютере, но на терминальной системе это сделать намного проще.

Одно из самых значимых достоинств виртуализации представлений — значительное упрощение администрирование системы. Приложения на всех рабочих местах можно обновить на сервере, а в случае возникновения проблем у сотрудника можно подключиться удаленно без установки дополнительного программного обеспечения. Но данное достоинство одновременно является и недостатком: так как все рабочие места зависят от одного сервера — появляется единая точка отказа. В случае возникновения проблем на сервере — ни одно из рабочих мест не будет функционировать [4].

Виртуализация серверов — это программная имитация с помощью специального программного обеспечения. Данная технология позволяет на одной физической машине запускать ещё несколько виртуальных машин, каждая из которых имитирует работу физической машины. Такая имитация затрагивает основные компоненты машины: память, процессор, накопитель и другие.

На такой виртуальный компьютер можно установить операционную систему, которая будет работать точно так же, как и на обычном физическом компьютере. Наиболее выдающееся преимущество этой технологии — на одной физической машине можно запустить несколько виртуальных, которые будут работать независимо друг от друга.

Данная технология виртуализации очень широко применима. Виртуальные машины можно использовать в целях обучения работников или для тестирования безопасности и работоспособности незнакомого программного обеспечения без риска для реальной системы. Так же появляется возможность сократить количество серверов благодаря консолидации, то есть там, где требуется несколько серверов, можно поставить один и запустить на нем необходимое количество гостевых систем.

Виртуализация серверов также, как и виртуализация представлений позволяет упростить процесс администрирования инфраструктуры при помощи удаленного доступа к консоли виртуальных серверов на виртуально-аппаратному уровню, независимо от установленной гостевой системы и её состояния. Например, для перезагрузки зависшего сервера не нужно будет куда-то идти, достаточно открыть консоль и нажать «Reset». Так же виртуальные машины способны сохранять свои состояния в виде «снимков», что делает восстановление и back-up виртуальных систем заметно легче.

Неоспоримое преимущество безопасности данной технологии виртуализации серверов заключается в том, что виртуальная машина «не видит» какое оборудование установлено на физической машине. При любых изменениях в физическом сервере виртуальный будет продолжать работать в штатном режиме [4].

Виртуализация приложений — одно из самых новых направлений в виртуализации. Данная технология выделяется тем, что позволяет запускать

приложение в своей собственной изолированной среде, что даёт ряд преимуществ:

- безопасность: приложение, которое запущено в изолированной среде никаким образом не способно навредить операционной системе или её компонентам;
- администрирование: все виртуальные приложения можно обновлять централизованно из одного источника;
- совместимость: технология позволяет одновременно запускать конфликтующие приложения или разные версии одного.

Виртуальные приложения не требуют установку в операционную систему. Достаточно лишь запустить его на выбранной машине. При этом имитируются те компоненты системы, которые нужны для работы. Каждое приложение использует свою изолированную среду, в которой работает независимо от другого программного обеспечения.

В этом и заключается главный плюс виртуализации — исключение конфликтов между программным обеспечением. Технология требует намного меньше ресурсов, чем имитация операционной системы. Приложение не загромождает реестр и не создает файлы конфигурации, засоряя систему [4].

1.3 Выбор технологии виртуализации лабораторного стенда

В ходе выполнения данного этапа дипломного проекта были рассмотрены и проанализированы современные технологии виртуализации, на основе которых возможна разработка виртуального стенда для дистанционного выполнения лабораторных работ.

По итогам произведенного анализа был сделан выбор в пользу технологии виртуализации приложений. Выбранная технология имеет ряд преимуществ, позволяющих реализовать поставленную задачу наиболее успешно.

Виртуализированные приложения работают быстрее и лучше, характеризуются высокой доступностью и адаптивностью, а так же поддерживают возможность аварийного восстановления и использования в облачной инфраструктуре. Данная технология позволяет сделать приложение доступным для пользовательских компьютеров без необходимости устанавливать их непосредственно на эти компьютеры, так как приложение работает в собственной, автономной виртуальной среде [5].

В отличие от технологии виртуализации серверов и виртуализации представлений, виртуализация приложений обеспечивает их использование в другой операционной системе или браузере без каких-либо зависимостей, а так же объединяет в пределах одного оборудования функции нескольких физических устройств, что является решающим фактором в выборе технологии виртуализации лабораторного стенда.

1.4 Описание выбранной технологии виртуализации

Исходя из того, что защищенный виртуальный стенд реализуется как web-приложение — этому понятию было дано конкретное определение.

Web-приложение — это сайт с элементами интерактива, который позволяет пользователям взаимодействовать: нажимать кнопки, заполнять формы или выбирать определенное действие из списка. С точки зрения архитектуры, web-приложения состоят из клиентской и серверной части. Клиентская часть является тем, что пользователь видит на экране своего устройства и с чем взаимодействует. Серверная часть — это программная часть сервиса, которая представляет собой набор правил и средств, реализующие логику приложения [6].

В ходе анализа доступных технологий для реализации web-приложения были выделены следующие:

- Single Page Application (SPA) – одностороннее web-приложение, на одной HTML-странице;

- Multi Page Application (MPA) – многостраничное web-приложение;
- Progressive Web Application (PWA) – гибрид сайта и мобильного приложения.

Принципы MPA и PWA не подходят под заданные требования, так как нам не требуется многостраничное приложение, на котором страница будет обновляться при каждом изменении данных или загрузке информации. Так же не стоит цель делать гибрид сайта и мобильного приложения. Исходя из этого, принцип SPA идеально подходит под поставленные требования. Пользователю не нужно перезагружать или подгружать дополнительные страницы благодаря динамическому обновлению с использованием JavaScript. В браузере находится весь основной контент, а когда вводятся данные — нужные элементы просто подгружаются.

Клиентская часть приложения представляет собой интерактивную часть программы, которая выполняется в браузере на любом устройстве с выходом в интернет. Она загружается в виде динамической страницы и реализуется пользовательский интерфейс.

Основной стек компонентов интерфейса состоит из следующих элементов:

- HTML – стандартный язык разметки, который активно применяется для создание web-проектов. Он позволяет отображать основные блоки страниц, а так же форматированный текст на них, таблицы, изображение и т.д. Когда браузер направляет запрос URL-адреса, чтобы получить приложение, в первую очередь возвращается HTML;
- CSS – каскадные таблицы стилей. Это язык разметки, который определяет макет и стиль элементов HTML;
- JavaScript – язык программирования, который помогает реализовать сложное поведение web-страницы. В нашем случае JavaScript

будет использоваться для создания адаптивных интерактивных элементов, через которые пользователь сможет взаимодействовать с виртуальным стендом.

Под серверной частью приложения понимается набор программно-аппаратных средств, с помощью которых построена логика работы web-приложения. Такая работа происходит вне браузера и компьютера пользователя. Сюда относится панель администрирования, управление данным и логика их передачи клиентской части.

PHP является одним из самых распространенных языков web-разработки.

В нашем случае во время работы приложения требуется отображать актуальное состояние информации. При использовании только HTML подобную задачу решить не удастся. Необходимо использовать PHP – он принимает входящий запрос, выполняет сценарий и возвращает результат в виде готового HTML-кода. Сервер отправляет этот результат в браузер, который отображает информацию пользователю. С помощью данной технологии пользователь сможет видеть актуальную информацию на приборах при заданном им наборе значений.

2 Разработка структуры виртуального стенда

На данном этапе дипломного проекта была разработана структура защищенного виртуального стенда для выполнения лабораторных работ. Для наглядности и более подробного описания структуры были разработаны следующие диаграммы:

- диаграмма вариантов использования;
- диаграмма последовательности;
- диаграмма коммуникации;
- диаграмма компонентов.

Диаграмма вариантов использования — это диаграмма, которая описывает какой функционал разрабатываемого проекта доступен каждой группе пользователей [7]. В данном случае группа пользователей состоит из «Студента» и «Преподавателя».

Студент может выполнять лабораторную работу. Преподаватель может разместить лабораторную работу и регистрировать или удалять студентов. Для выполнения этих действий пользователям необходимо авторизоваться. Разработанная диаграмма вариантов использования представлена на рисунке 2.

Диаграмма последовательности является одной из видов диаграмм взаимодействия в языке UML, которые описывают взаимоотношения объектов в различных условиях. Она иллюстрирует как различные части системы взаимодействуют друг с другом для выполнения своих функций, а также порядок, в котором происходит взаимодействие при выполнении конкретного случая.

Схема построена таким образом, что представляет собой временную шкалу, которая начинается сверху и постепенно опускается, чтобы отметить последовательность взаимодействия. Каждый объект имеет иконку, а стрелками представлены сообщения, которыми они обмениваются [8].

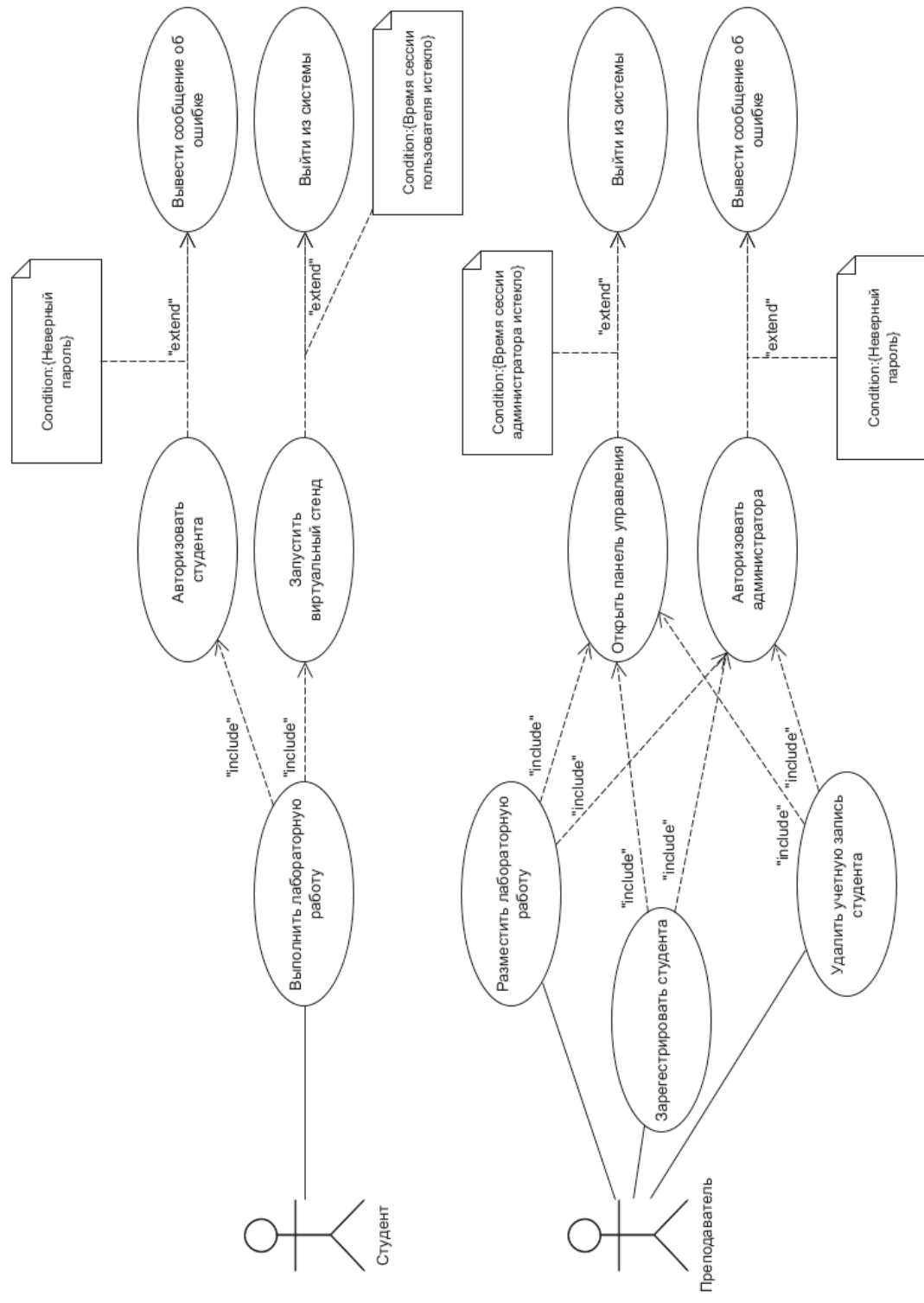


Рисунок 2 — Диаграмма вариантов использования

В нашем случае было построено две диаграммы последовательности — для администратора и студента. Схема построена таким образом, что представляет собой временную шкалу, которая начинается сверху и опускается постепенно вниз, чтобы отметить последовательность взаимодействия. Каждый объект имеет иконку, а стрелками представлены сообщения, которыми они обмениваются.

Чтобы администратору создать учетную запись студента, ему нужно авторизоваться, предъявив логин и пароль. Входные данные хэшируются и проверяются по базе данных и, в случае если есть совпадение, ответственные за авторизацию компонент пропускает администратора в систему. Если в базе данных нет совпадений по введенным логину и паролю, появляется ошибка. Далее администратор создает учетную запись студента, которая заносится в базу данных, благодаря чему отражается в списке пользователей. Наконец, администратор завершает сессию.

Чтобы администратору удалить учетную запись студента, ему нужно авторизоваться, как в предыдущем случае при создании учетной записи. При успешной авторизации администратор выбирает нужную учетную запись и стирает её из базы данных. При успешном удалении учетные данные пропадают из списка. Закончив работу в панели администратора, преподаватель завершает сессию.

Чтобы студент получил доступ к выполнению лабораторной работы, ему нужно авторизоваться, предъявив логин и пароль. Входные данные хэшируются и проверяются по базе данных и, в случае если есть совпадение, ответственные за авторизацию компонент пропускает студента в рабочее пространство. Если в базе данных нет совпадений по введенным логину и паролю, появляется ошибка.

На следующем этапе из базы данных подгружаются материалы лабораторной работы, и студент может работать со стендом. При

неправильной настройке приборов появляется ошибка. Закончив работу на стенде студент завершает сессию.

Разработанные диаграммы последовательности администратора и студента представлены на рисунках 3 и 4 соответственно.

Диаграмма коммуникаций является особым видом диаграммы взаимодействия, которая сосредоточена на обмене данными между различными компонентами. Вместо того, чтобы рисовать каждого участника в виде линии жизни и показывать последовательность сообщений, как это делается в диаграмме последовательности, коммуникационные диаграммы допускают произвольное размещение участников, и использовать нумерацию для представления этих сообщений [9].

В данном случае диаграмма коммуникаций представляет последовательность действий не по времени, а в пространстве. Диаграмма данного вида была составлена для администратора и студента.

Чтобы администратору пройти весь цикл потребуется 8 взаимосвязей между компонентами:

- ввести авторизационные данные;
 - шифровать авторизационные данные;
 - сверить пароль;
 - вернуть положительный ответ;
 - авторизовать администратора в системе;
 - добавить или удалить учетную запись;
 - шифровать данные учетной записи студента (при добавлении);
- завершить сессию.

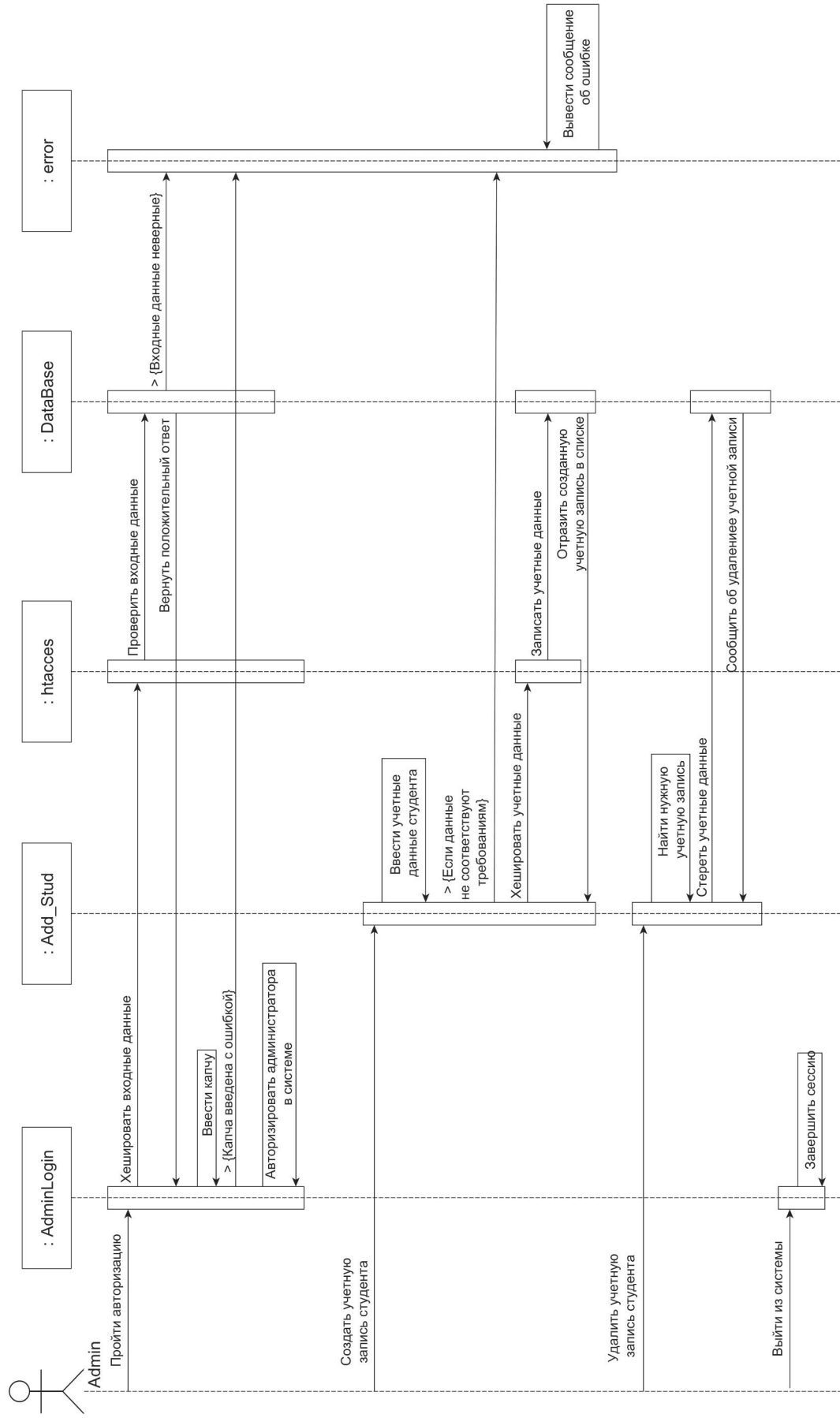


Рисунок 3 — Диаграмма последовательности Администратора

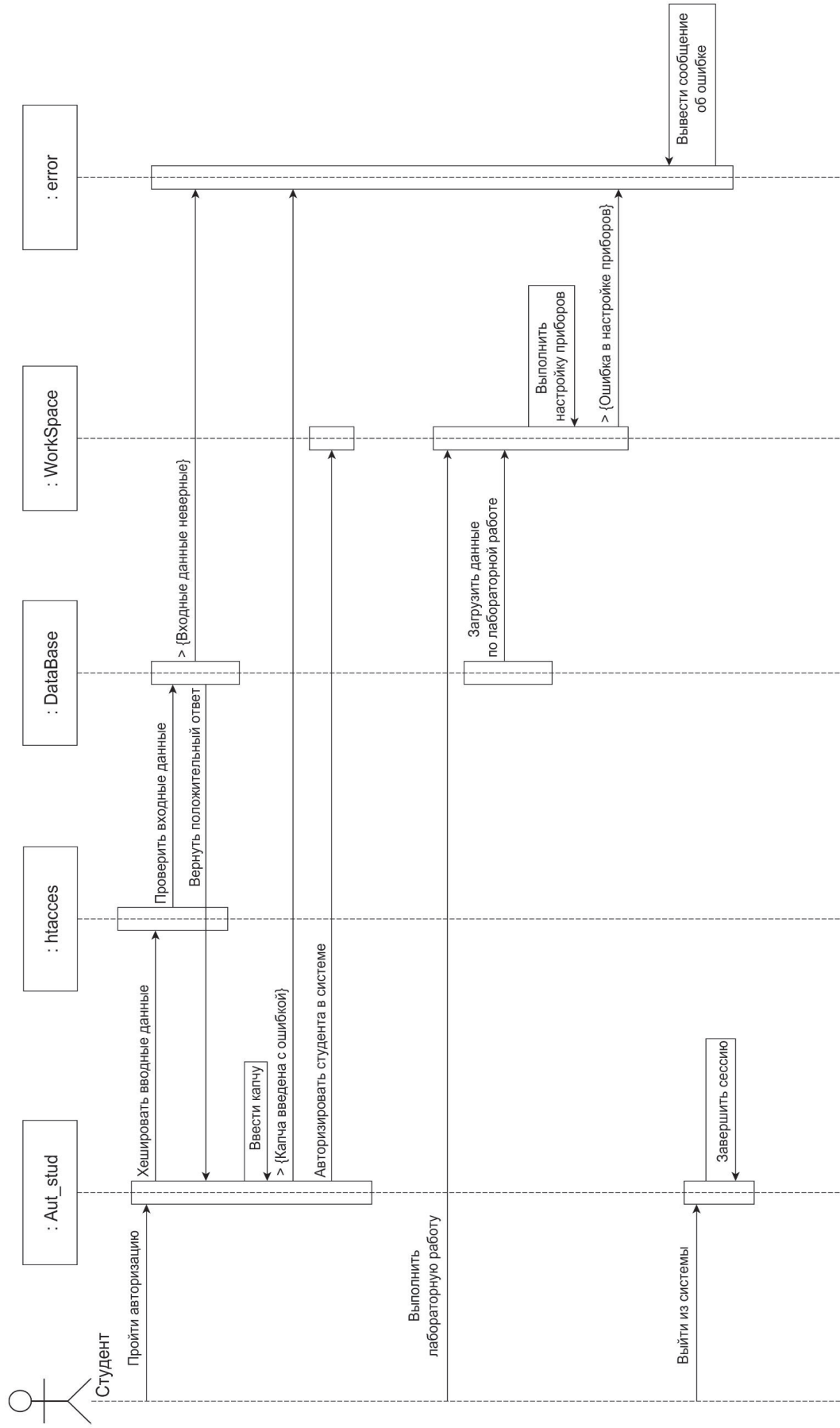


Рисунок 4 — Диаграмма последовательности Студента

Чтобы студенту пройти весь цикл потребуется 8 взаимосвязей между компонентами:

- ввести авторизационные данные;
- шифровать авторизационные данные;
- сверить пароль;
- вернуть положительный ответ;
- авторизовать студента в системе;
- загрузить данные лабораторной работы;
- выполнить лабораторную работу;
- завершить сессию.

Разработанные диаграммы коммуникаций для администратора и студента представлены на рисунке 5 и 6 соответственно.

Диаграмма компонентов, в отличие от ранее рассмотренных диаграмм, описывает особенности физического представления системы. Диаграмма компонентов позволяет определить архитектуру разрабатываемой системы, установив зависимости между программными компонентами [10].

В нашем случае необходимостью создания такой диаграммы является визуализация общей инфраструктуры исходного кода web-системы. При создании диаграммы были определены интерфейсы, которые могут взаимодействовать с системой — администратор и клиент (студент).

Чтобы администратор мог пользоваться компонентом AdminSystem он должен пройти авторизацию через `htaccess` и `htpassword`. Данные компоненты работают вместе и отвечают за безопасное логирование пользователей и защиту пароля. Авторизация происходит при помощи компонента `admin_login`, который получает информацию о предыдущих двух компонентах. Далее включается компонент, который устанавливает сессию администратора `setadmin`. За завершение сессии отвечает `outadmin`.

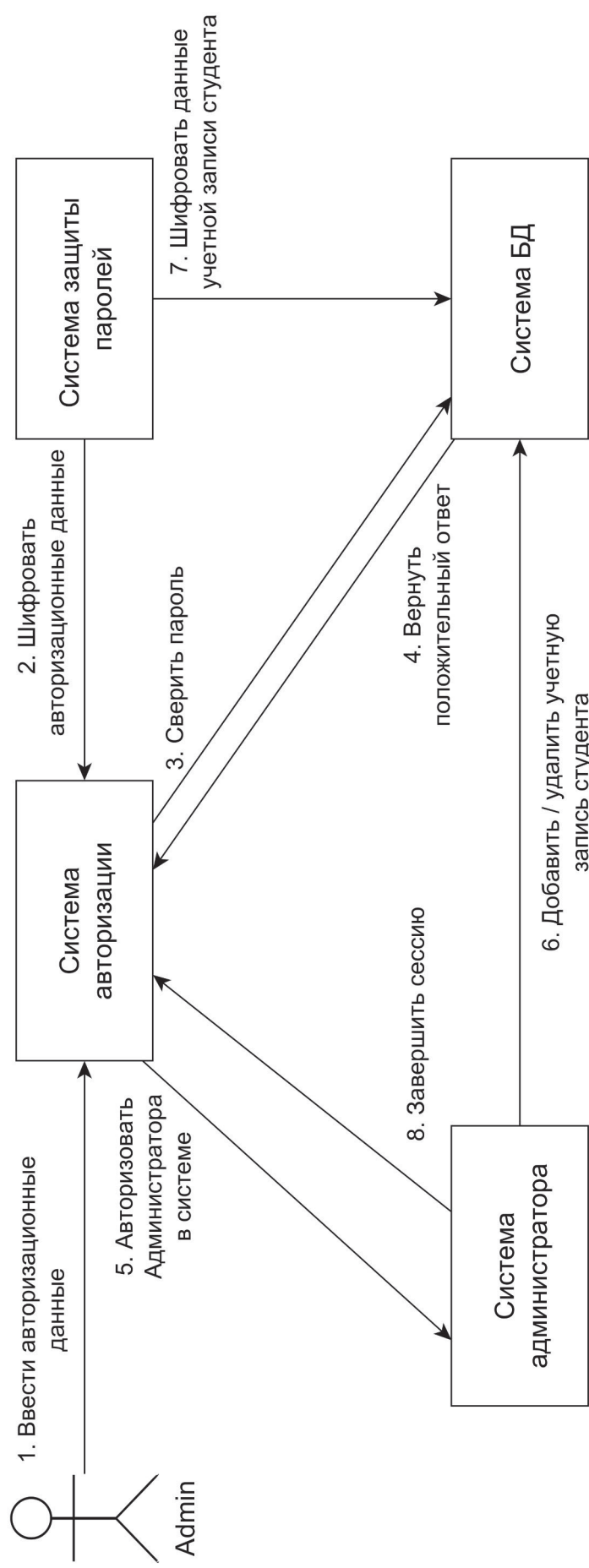


Рисунок 5 — Диаграмма коммуникаций администратора

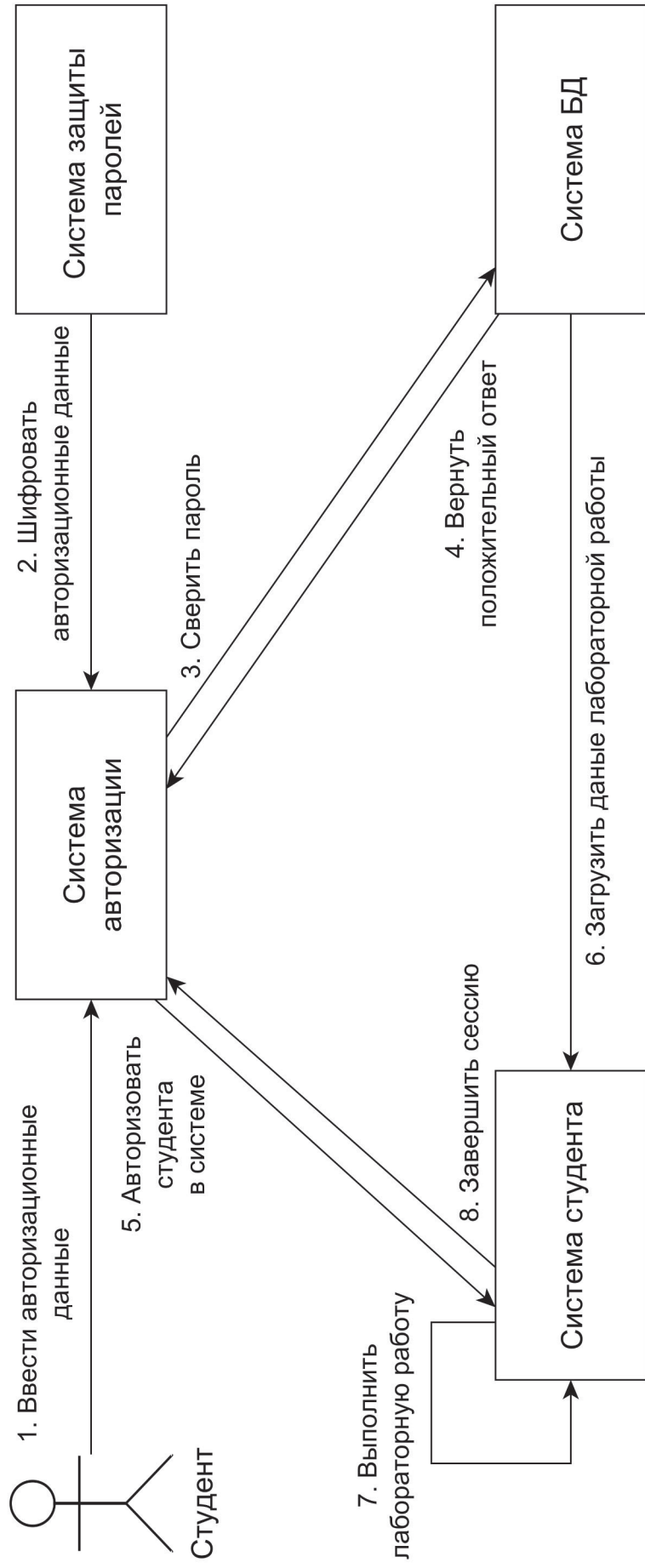


Рисунок 6 — Диаграмма коммуникаций студента

Компоненты `add_stud` и `filter_stud` отвечают за добавление и сортировку списка студентов. База данных хранит в себе информацию о студентах, материалах лабораторной логи и подключена напрямую к системе.

Студент имеет доступ к `ClientSystem` при условии успешной авторизации (при созданном аккаунте) через компонент `aut_stud`. Выполнение лабораторной работы реализовано в компоненте `workspace`. База данных подключается напрямую и подгружает всю необходимую информацию по мере необходимости. Диаграмма компонентов представлена на рисунке 7.

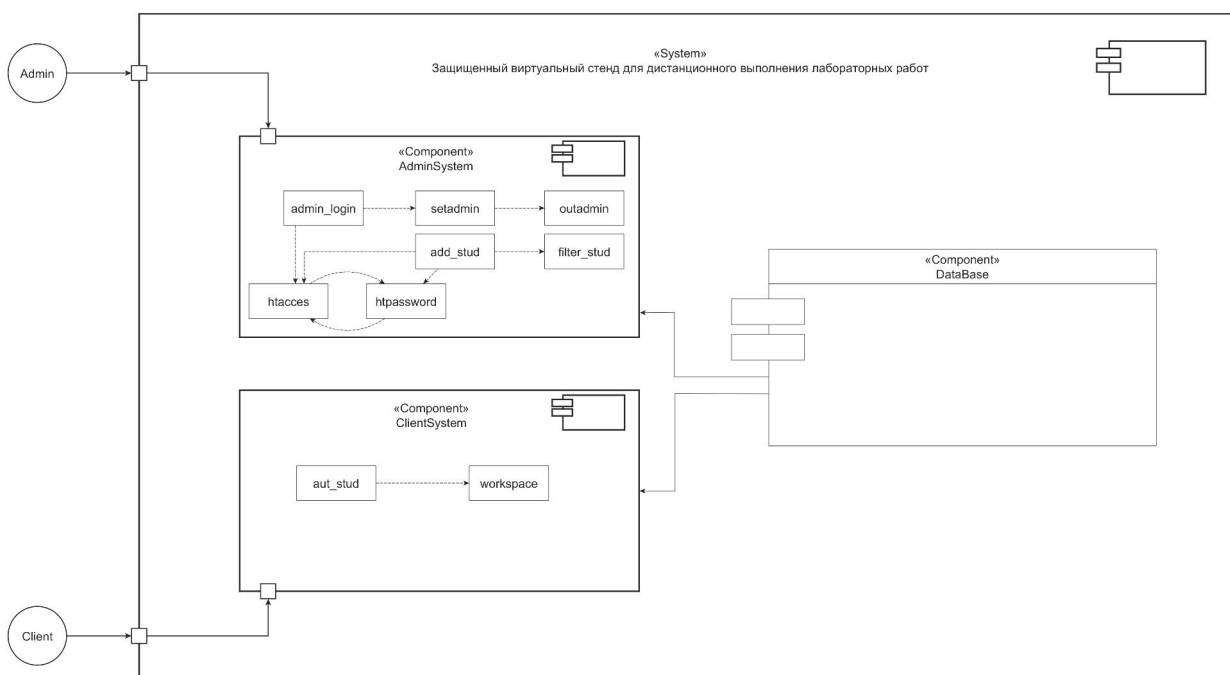


Рисунок 7 — Диаграмма компонентов

3 Разработка дерева событий виртуального стенда

В рамках данного этапа дипломного проекта было разработано дерево событий при выполнении лабораторного практикума. Поскольку выполнение лабораторной работы на виртуальном стенде подразумевает созданную у студента учетную запись — функции администратора рассматриваться не будут.

В данном случае дерево событий было представлено в виде блок-схемы. Это самый распространенный тип схем, который описывает алгоритмы или процессы, где отдельные шаги изображаются в виде блоков различной формы. Блоки соединены линиями со стрелкой, которая указывает направление последовательности [11].

Прежде чем студент приступит к выполнению лабораторной работы — ему необходимо авторизоваться в системе. Данное действие возможно только при условии, что администратор создал для него учетную запись и сообщил ему логин и пароль. В противном случае студенту необходимо запросить доступ у администратора.

В случае успешной авторизации студент должен ввести значения в соответствующие окна. При условии, что пользователь ввёл значения правильно и в соответствии с заданным вариантом — ему откроется доступ к управлению конфигурацией приборов. В случае, если доступ к приборам не открылся — необходимо проверить правильность введенных значений.

После успешной настройки приборов — пользователь снимает необходимые показания и завершает сессию. Стоит учесть, что сессия может автоматически завершиться в случае бездействия определенное количество времени.

Блок схема дерева событий при выполнении лабораторного практикума представлена на рисунке 8.



Рисунок 8 — Блок схема дерева событий при выполнении лабораторного практикума

4 Разработка виртуального стенда

На данном этапе выполнения дипломного проекта была произведена реализация защищенного виртуального стенда для дистанционного выполнения лабораторных работ. Система была реализована на языке PHP версии 8.0 в полном соответствии с поставленным техническим заданием.

В первую очередь была реализована панель администратора, которая является серверной частью разрабатываемого стенда. При помощи данной панели администратор может управлять учетными записями студентов. Функции, доступные администратору для работы перечислены ниже:

- авторизация в панели администратора;
- добавление данных учетной записи студента (группа, фамилия, имя, отчество, логин, пароль, примечание);
- изменение данных учетной записи студента (группа, фамилия, имя, отчество, логин, пароль, примечание);
- удаление учетной записи студента (группа, фамилия, имя, отчество, логин, пароль, примечание);
- завершение активной сессии администратора.

Добавление учетной записи студента осуществляется с помощью ввода группы и фамилии в окно поиска. Если поиск не дал результатов, администратор должен нажать кнопку «Добавить». Таким образом учетная запись появляется в списке. Чтобы внести дополнительную информацию (имя, отчество, логин, пароль, примечание) администратору необходимо совершить двойное нажатие левой клавишей мыши по соответствующему полю в строке необходимой учетной записи.

Удаление учетной записи студента осуществляется вводом команды «del» в название группы. Впоследствии появляется соответствующее уведомление об успешном удалении учетной записи.

После внедрения функционала управления учетными записями, в панель управления администратора были добавлены защитные меры, описанные в разделе 5.

Далее было реализовано рабочее пространство студента, которое является клиентской частью разрабатываемого стенда. Клиентская часть является рабочей средой студента, где он, при наличии доступа к ней, может получить базовое представление о работе с измерительными приборами путём выполнения лабораторной работы.

Перед началом выполнения лабораторной работы студент проходит процесс авторизации. При успешном входе в аккаунт студенту открывается доступ к использованию лабораторного стенда. В случае неправильного ввода логина или пароля появляется ошибка.

Прежде чем задать приборам необходимую конфигурацию, студент должен ввести 3 параметра:

- значение количества пикселей по горизонтали $N_{гор}$;
- значение количества пикселей по вертикали $N_{верт}$;
- частота кадровой развертки F_k .

Так как работа приборов виртуализирована с определенными параметрами, было задано несколько наборов значений, допустимых для ввода. Для удобства наборы были поделены на варианты, которые преподаватель сможет раздавать студентам. Доступные для ввода наборы значений представлены в таблице 1.

Таблица 1 — Наборы значений в соответствии с вариантом

Вариант ввода	$N_{гор}$	$N_{верт}$	F_k
1	1280	720	50
2	1600	900	40
3	1140	1080	35
4	1024	1600	30

Параметры вводятся в соответствии с вариантом и не могут комбинироваться с другими. Каждое поле ввода проверяется на правильность введенных значений в соответствии с вариантом. Например, если студент вводит $N_{ГОР} = 1280$, а $N_{ВЕРТ} = 900$ – появляется ошибка, так как заданы значения из разных вариантов. Когда все значения введены верно, студент нажимает на кнопку «Высчитать» и получает значение спектра сигнала F_T , которые считается по формуле (1).

$$F_T = \frac{N_{ВЕРТ} * N_{ГОР} * F_K * 1,414}{2} \quad (1)$$

Приборы представлены в виде изображений с актуальной информацией о состоянии прибора. Например, если прибор выключен — стенд демонстрирует изображение выключенного прибора. Чтобы задать приборам необходимую конфигурацию, студенту необходимо их включить.

Генератор сигналов имеет меню выбора режима работы: «Модуляция» или «Пачка», а так же меню выбора вида модуляции: «Default» и «Triangle». При выборе необходимых параметров подгружается изображение, которое отражает полученные данные и выбранный режим работы. В случае неверной конфигурации прибора появится ошибка. После настройки генератора сигналов студенту доступна настройка цифрового осциллографа и анализатора спектра.

Цифровой осциллограф имеет меню выбора режима работы: «Форма сигнала» и «Спектр сигнала». В зависимости от выбранного режима подгружается изображение, которое отражает полученные данные и выбранный режим работы. Однако, данные подгрузятся в случае верно настроенного генератора сигналов, иначе появится ошибка.

При проведении исследований с Анализатором спектра используется Генератор шума. Данный прибор представлен на стенде в виде кнопки и имеет два состояния: «Включен» и «Выключен». Анализатор спектра имеет

меню выбора режима работы, каждый из которых будет работать при соблюдении определенных условий:

- «Тестовый сигнал + объектовый шум», работает при включенном в режиме «Модуляция» генераторе сигналов и отключенном генераторе шума;
- «Объектовый шум», работает при включенном в режиме «Пачка» генераторе сигналов и отключенном генераторе шума;
- «Тестовый сигнал + объектовый шум + зашумление», работает при включенном в режиме «Модуляция» генераторе сигналов и включенном генераторе шума;
- «Объектовый шум + зашумление», работает при включенном в режим «Пачка» генераторе сигналов и включенном генераторе шума.

Данные подгружаются в случае правильно настроенных приборов, иначе появится ошибка. После внедрения функционала выполнения лабораторной работы, в рабочее пространство студента были добавлены защитные меры, описанные в разделе 5.

5 Внедрение защитных мер виртуального стенда

5.1 Выявление угроз информационной безопасности для защищенного виртуального стенда для дистанционного выполнения лабораторных работ

На данном этапе дипломного проекта были разработаны и внедрены защитные меры, нейтрализующие идентифицированные угрозы информационной безопасности.

В первую очередь были выявлены объекты воздействия защищенного виртуального стенда для дистанционного выполнения лабораторных работ, свойства безопасности которых могут быть нарушены. В таблице 2 представлен список объектов воздействия для серверной и клиентской части разработанного web-приложения.

Таблица 2 — Объекты воздействия

Серверная часть	
№ О/В	Объект воздействия
1	Аутентификационная информация
Клиентская часть	
№ О/В	Объект воздействия
1	Методические указания к лабораторной работе
2	Изображения приборов
3	Код HTML-разметки клиентской части web-приложения

Для идентификации угроз информационной безопасности был использован Банк данных угроз безопасности информации ФСТЭК [12]. Для защищенного виртуального стенда для дистанционного выполнения лабораторных работ были выбраны угрозы, представленные в таблицах 3 — 7.

Таблица 3 — Описание угрозы УБИ.01: «Угроза утечки информации»

Описание угрозы	Угроза заключается в возможности противоправного получения либо передачи информации (конфиденциальной, конфигурационной, аутентификационной и др.). Например, утечка персональных данных вследствие нарушения хранения или нарушения конфигурации
Источники угрозы	Все нарушители
Объект воздействия	Защищаемая информация
Последствия реализации угрозы	Нарушение конфиденциальности

Таблица 4 — Описание угрозы УБИ.02: «Угроза несанкционированного доступа»

Описание угрозы	Угроза заключается в получении доступа к информационным ресурсам, нарушающего установленные в информационной системе правила разграничения доступа. Например, несанкционированный доступ к информации, хранимой на файловом хранилище
Источники угрозы	Все нарушители
Объект воздействия	Модуль аутентификации
Последствия реализации угрозы	Нарушение конфиденциальности, целостности, доступности

Таблица 5 — Описание угрозы УБИ.036: «Угроза исследования механизмов работы программы»

Описание угрозы	Угроза заключается в возможности проведения нарушителем обратного инжиниринга кода программы и исследования его структуры, функционала и состава в интересах алгоритма работы программы и поиска в ней уязвимостей. Угроза обусловлена слабостями механизма защиты кода от исследования. Реализация угрозы возможна в случае: наличия у нарушителя доступа к исходным файлам; наличия у нарушителя доступа к дистрибутиву программы и отсутствия механизма защиты кода программы от исследования
-----------------	--

Продолжение таблицы 5

Источники угрозы	Внутренний нарушитель со средним потенциалом Внешний нарушитель со средним потенциалом
Объект воздействия	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение
Последствия реализации угрозы	Нарушение конфиденциальности Нарушение доступности

Таблица 6 — Описание угрозы УБИ.086 «Угроза несанкционированного изменения аутентификационной информации»

Описание угрозы	Угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств. Данная угроза обусловлена наличием слабостей мер разграничения доступа к информации аутентификации. Реализация данной угрозы может способствовать дальнейшему проникновению нарушителя в систему под учётной записью дискредитированного пользователя
Источники угрозы	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом
Объект воздействия	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр
Последствия реализации угрозы	Нарушение целостности Нарушение доступности

Таблица 7 — Описание угрозы УБИ.088 «Угроза несанкционированного копирования защищаемой информации»

Описание угрозы	Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне. Реализация данной угрозы возможна в случае отсутствия криптографических мер защиты или снятия копии в момент обработки защищаемой информации в нешифрованном виде
Источники угрозы	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом
Объект воздействия	Объекты файловой системы, машинный носитель информации
Последствия реализации угрозы	Нарушение конфиденциальности

На основании идентифицированных угроз были разработаны и внедрены защитные меры, нейтрализующие идентифицированные угрозы информационной безопасности. В таблице 6 представлены угрозы информационной безопасности и нейтрализующие их меры защиты информации соответственно.

Таблица 8 — Соответствие угроз информационной безопасности и защитных мер

Серверная часть	
Угроза информационной безопасности	Защитные меры
УБИ.02: «Угроза несанкционированного доступа»	Встроен модуль двухфакторной аутентификации;

Продолжение таблицы 8

Серверная часть	
Угроза информационной безопасности	Защитные меры
	Встроена каптча
УБИ.086 «Угроза несанкционированного изменения аутентификационной информации»	В панели администратора запрещен поиск аутентификационных данных администратора
Клиентская часть	
Угроза информационной безопасности	Защитные меры
УБИ.01: «Угроза утечки информации»	Запрещены действия, позволяющие открыть консоль разработчика (нажатие клавиши «F12», сочетание клавиш «Ctrl+Shift+J»); Запрещено нажатие правой кнопкой мыши (блокирование способа открыть консоль разработчика, блокирование возможности копировать изображения)
УБИ.02: «Угроза несанкционированного доступа»	Встроен модуль аутентификации; Встроена каптча
УБИ.036: «Угроза исследования механизмов работы программы»	Запрещены действия, позволяющие открыть консоль разработчика (нажатие клавиши «F12», сочетание клавиш «Ctrl+Shift+J»);
УБИ.088 «Угроза несанкционированного копирования защищаемой информации»	Запрещено нажатие правой кнопкой мыши (блокирование способа открыть консоль разработчика, блокирование возможности копировать изображения); Файлы лабораторной работы доступны только для авторизованных пользователей

5.2 Описание, разработка и внедрение защитных мер в виртуальный стенд

Был разработан модуль двухфакторной аутентификации, который запрашивает у администратора на входе логин и первый пароль. После успешной авторизации, модуль запрашивает второй пароль и, в качестве дополнительной меры защиты, требует ввод каптчи. В случае неправильно введенных аутентификационных данных на первом этапе, оба поля ввода обновляются. В случае ошибок при вводе на втором этапе, появляется ошибка с сообщением о неправильном пароле или каптчи, а так же обновляются поля ввода и каптча. Код реализации компонентов модуля двухфакторной аутентификации представлен ниже:

Компонент .htaccess

```
AuthType Basic
AuthName "Hello from stend-tzi.ru"
AuthUserFile
/var/www/user_maxpnz/data/www/stend-tzi.ru/admin/.htpasswd
Require valid-user
<Files .htpasswd>
    deny from all #запрет доступа из браузера к .htpasswd
</Files>
```

Компонент .htpasswd

```
admin:$apr1$s18wnx4h$BuZlr.HOKAPc50geA4/SB1
```

Компонент setadmin.php

```
<?php
define('DbSimple',true);
require_once '../..'/functions/functions.php';

if (

md5(trim($_POST['pass']))=='c4ca4238a0b923820dcc509a6f75849b'
AND
```

```

        substr(hexdec(md5("".date("Fj")."".
$_SESSION['captcha']."sfgnsffhgsrcge4t34tq34t")), 2, 6) ==
intval($_POST['cap'])
    )

    {
        $_SESSION['admin'] = 1;
        $out['setadmin'] = 1;
        $_SESSION['admin_start'] = time();
    } else {
        $_SESSION['admin'] = 0;
        $out['setadmin'] = 0;
    }

    $_SESSION['captcha'] = '';
    echo json_encode($out);

?>

```

Был разработан модуль однофакторной аутентификации, который запрашивает у пользователя логин, пароль и каптчу. В случае успешного входа — пользователь попадает в систему. В случае ошибки при вводе, появляется ошибка о том, что логин, пароль или каптча написан с ошибкой, а так же обновляются поля ввода и каптча. Код реализации модуля однофакторной аутентификации представлен ниже:

```

<?php
define('DbSimple',true);
require_once '../functions/functions.php';
require_once '../DbSimple/connect.php';

    $login      =      preg_replace('/[^a-zA-Z0-9-_]/sui',      '',
$_POST['login']);
    $pass       =      preg_replace('/[^a-zA-Z0-9-_]/sui',      '',
$_POST['pass']);

    $coll  =  $DB->selectCell('SELECT  id  FROM  ?_users  WHERE
login=? AND pass=?', $login, main_md5($pass));

    if (
        $coll > 0

```

```

        AND
        substr(hexdec(md5("".date("Fj")."").
$_SESSION['captcha']."sfgnsffhgsrge4t34tq34t")), 2, 6) ==
intval($_POST['cap'])
    )
    {
        $out['setuser'] = 1;
        $_SESSION['user'] = 1;
        $_SESSION['user_start'] = time();
        $_SESSION['user_pr']['pGS']['power'] = -1;
        $_SESSION['user_pr']['pGS']['rezgener'] = '';
        $_SESSION['user_pr']['pGS']['vidmodul'] = '';
        $_SESSION['user_token'] =
main_md5(time(). 'dvsv&')^vreb43t(&^sdb3466earbaerbata');
    } else {
        $out['setuser'] = 0;
        $_SESSION['user'] = 0;
        $_SESSION['user_start'] = 0;
        unset($_SESSION['user_pr']);
    }

    $_SESSION['captcha'] = '';

    echo json_encode($out);

?>

```

Капча была протестирована сервисами распознавания текста на пробиваемость. Были использованы следующие сервисы:

- ONLINE-CONVERT;
- img.txt;
- Convertio.

Ни один из перечисленных сервисов не справился с распознаванием. Капча, используемая в модулях аутентификации входит в их состав.

В панели администратора был запрещен поиск учетной записи администратора. При попытке поиска, поля ввода обновляются и появляется ошибка, содержащая фразу «Нельзя искать администратора». Код реализации данной защитной меры представлен ниже:

```
if      (      preg_match('/admin/sui',      $find_gruppa)      OR
preg_match('/admin/sui', $find_fio_f) ) {
    $out['err'] = 'Нельзя искать админа';
    echo json_encode($out);
    die();
}
```

Были запрещены действия, позволяющие открыть консоль разработчика. Нажатие клавиши «F12» или сочетания клавиш «Ctl+Schift+J» не дают ожидаемого результата. Код реализации данной защитной меры представлен ниже:

```
document.onkeydown = function(e) {
    if(event.keyCode == 123) {
        return false;
    }
    if(e.ctrlKey      &&      e.shiftKey      &&      e.keyCode      ==
'I'.charCodeAt(0)) {
        return false;
    }
    if(e.ctrlKey      &&      e.shiftKey      &&      e.keyCode      ==
'J'.charCodeAt(0)) {
        return false;
    }
    if(e.ctrlKey && e.keyCode == 'U'.charCodeAt(0)) {
        return false;
    }
}
```

Так как меню, вызываемое нажатием правой кнопки мыши, позволяет сохранять изображения и получить доступ к консоли разработчика, данная функция была заблокирована. Код реализации данной защитной меры представлен ниже:

```
document.oncontextmenu = cmenu; function cmenu() { return false; }
```

Был разработан функционал, который запрещает настройку конфигурации приборов при их выключенном питании, в случае если нарушитель обошел защитные меры и открыл консоль разработчика. Код разработанной защитной меры на примере работы генератора сигналов представлен ниже:

```
if ( $_POST['idPr'] == 'pGS' ) {

    if ( $_POST['power'] == 'on' ) {
        $_SESSION['user_pr']['pGS']

['power'] = 1;

    } elseif ( $_POST['power'] == 'off' ) {
        $_SESSION['user_pr']['pGS']

['power'] = -1;

        $_SESSION['user_pr']['pGS']

['rezgener'] = '';

        $_SESSION['user_pr']['pGS']

['vidmodul'] = '';

    }

    if ( isset($_POST['setrezim']) ) {
        if ( $_SESSION['user_pr']['pGS']

['power'] == 1 ) {

            if ( $_POST['setrezim'] ==

'Modulacia' ) {

                $_SESSION['user_pr']

['pGS']['rezgener'] = 'Modulacia';
```

```

$_SESSION['user_pr']
['img'] = 'img/on/' . $ng . '-' . $nv . '-' . $fk . '/GS_modul.jpeg';
$_out['img_pr'] = 1;
} elseif ( $_POST['setrezim']
== 'Pachka' ) {
$_SESSION['user_pr']
['pGS']['rezgener'] = 'Pachka';
$_SESSION['user_pr']
['img'] = 'img/on/' . $ng . '-' . $nv . '-' . $fk . '/GS_pachka.jpeg';
$_out['img_pr'] = 1;
}
} elseif ( $_SESSION['user_pr']
['pGS']['power'] != 1 ) {
$_out['err']['poradok'] =
'Нарушен порядок включения приборов';
}
}
}

```

Поскольку файлы лабораторной работы предназначены для студентов Пензенского государственного университета, доступ к ним разрешен лишь для пользователей, прошедших авторизацию.

Для скрытия реального местонахождения файла с методическими указаниями было реализовано скрытие реального местонахождения файла: при наведении курсора мыши на ссылку пользователь видит абстрактный адрес на сервере, по которому, если убрать защиту, пользователь не сможет найти никакой файл. Чтобы отобразить файл с методическими указаниями используется редирект (виртуальная переадресация) с помощью файла .htaccess. Код реализации данной защитной функции приведен ниже:

```

RewriteEngine On
RewriteBase /

```

```
RewriteRule m1.pdf$      downloads.php?f=m1  [L,NC]
```

В файле `download.php` был переопределен параметр `f` с абстрактного на реальное имя файла. Скрипт получает содержимое `TZI_Laboratornaja_rabota_2.pdf` и выводит в браузере на новой вкладке.

Код компонента `downloads.php` представлен ниже:

```
if (is_user()) {

    if ( $_GET['f']=='m1' )
    {
        $_GET['f']='TZI_Laboratornaja_rabota_2.pdf';
    }
    $filename = 'pdf/' . ($_GET['f']);
    $fctype = '';
    if (substr($filename, -4)=='pdf') { $fctype =
'pdf'; }
    elseif (substr($filename, -3)=='zip') {
        $fctype = 'zip'; }

    header('Content-Type: application/' . $fctype . ';');
    header('Content-Disposition: inline; filename=' .
(preg_replace('/pdf\\/\\/sui', '', $filename)));
    echo file_get_contents($filename);
    die();
}
```

Если пользователь каким-либо способом догадается или захочет проверить реальное местонахождение файла, то реализованы следующие защитные функции:

— для всех каталогов, расположенных на сервере действует правило «не отображать файлов директории, даже если в этом каталоге нет файла `index.php` или `index.html`». Данная защитная функция реализована с помощью следующего правила корневого `.htaccess`:

```
Options -Indexes;
```

— для защиты каталога PDF, в котором лежит файл с методическими указаниями, реализовано дополнительно правило, которое запрещает для всех прямой доступ к содержимому этого каталога. Реализация данной защитной функции представлена ниже:

```
deny from all
```

Также в качестве дополнительной защитной меры был установлен таймер сессии. При бездействии пользователя в течении 10 минут система блокирует доступ к стенду и в появившемся диалоговом окне предлагает пользователю пройти повторную авторизацию.

Код реализации данной защитной меры представлен ниже:

```
<?php
    define('DbSimple',true);
    require_once '../functions/functions.php';

    if ( time() - $_SESSION['user_start'] > $t_limit ) {
        $out['err']['rez'] = 'time_is_out';
        echo json_encode($out);
    } else {
        $out['err']['rez'] = 'time_is_gut';
        echo json_encode($out);
    }

?>
```

6 Проверка работоспособности виртуального стенда и действие его защитных средств

В рамках данного этапа дипломного проекта была выполнена проверка функционала панели администратора, рабочего пространства виртуального стенда и действие его защитных мер.

В первую очередь проверялся функционал панели администратора и её защитных мер. Прежде чем приступить к работе, администратор проходит двухфакторную аутентификацию. Процесс представлен на рисунках 9 и 10.

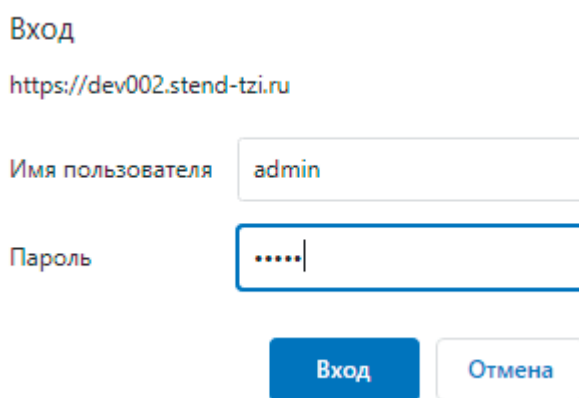


Рисунок 9 — Первый этап идентификации

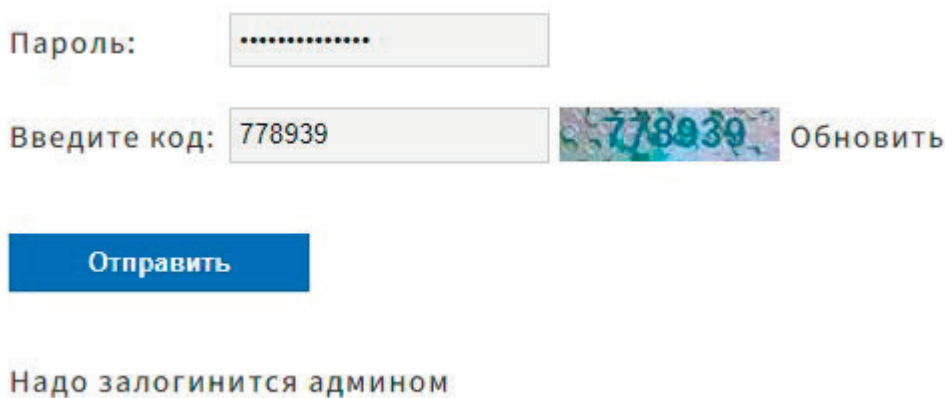


Рисунок 10 — Второй этап идентификации

После успешной авторизации администратор может добавить учетную запись студента, найти, удалить или изменить. Для добавления учетной

записи необходимо ввести группу и фамилию в необходимые поля и нажать кнопку «Добавить». Незаполненные данные будут иметь значения null. Администратору необходимо задать логин и пароль, чтобы студент получил доступ к стенду. Остальные поля заполняются по желанию преподавателя. Результат представлен на рисунках 11-12.

Поиск ::: Группа: Фамилия: [Добавить](#) [Выход](#)

Группа	Фамилия	Имя	Отчество	Логин	Пароль	Примечание
Совпадений не найдено						



Рисунок 11 — Заполненные поля для добавления учетной записи

Поиск ::: Группа: Фамилия: [Добавить](#) [Выход](#)

Группа	Фамилия	Имя	Отчество	Логин	Пароль	Примечание
19ПИ1	Водянов	null	null	null	*****	null

Рисунок 12 — Добавленный пользователь

Поиск пользователя доступен по группе и по фамилии. Была произведена попытка поиска студента с фамилией «Барминов» с целью его последующего удаления из системы. Удаление производится введением команды «del» в поле «группа». После ввода команды студент пропадает из списка. Результат представлен на рисунках 13 — 14 соответственно.

Поиск ::: Группа: Фамилия: [Добавить](#) [Выход](#)

Группа	Фамилия	Имя	Отчество	Логин	Пароль	Примечание
18ПИ1	Барминов	Максим	Витальевич	Barminov	*****	Отчислен

Рисунок 13 — Поиск студента

Поиск ::: Группа: Фамилия: [Добавить](#) [Выход](#)

Группа	Фамилия	Имя	Отчество	Логин	Пароль	Примечание
del	Барминов	Максим	Витальевич	Barminov	*****	Отчислен

Рисунок 14 — Удаление студента

После завершения работы в панели администратора преподавателю необходимо нажать кнопку «Выход» для завершения сессии. Если сессия не была завершена или администратор бездействовал в течении 10 минут — система завершит сессию и попросит повторную аутентификацию. Результат представлен на рисунке 15.

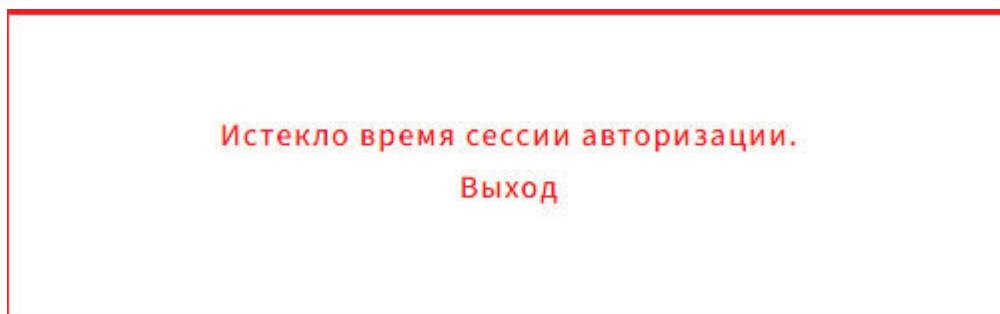


Рисунок 15 — Таймер активной сессии

Была произведена проверка работы защитной меры реализующей запрет поиска аутентификационных данных администратора. Поиск осуществлялся по слову admin. Результат представлен на рисунке 16

Поиск ::: Группа: Фамилия: [Добавить](#) [Выход](#)

Группа	Фамилия	Имя	Отчество	Логин	Пароль	Примечание
Нельзя искать админа						

Рисунок 16 — Запрет поиска аутентификационных данных администратора

В следующую очередь проверялся функционал рабочего пространства виртуального стенда. Прежде чем приступить к работе, студенту необходимо авторизоваться. Процесс авторизации представлен на рисунке 17.

Логин:

Пароль:

Введите код:  [Обновить](#)

[Отправить](#)

Рисунок 17 — Авторизация пользователя.

Далее студенту необходимо ввести исходные данные. Проверка будет производится со значениями варианта №3. В соответствующие поля были введены значения $N_{гор}$, $N_{верт}$, F_k в соответствии с вариантом 3. Параметр F_t посчитался автоматически. Результат представлен на рисунке 18.

ИСХОДНЫЕ ДАННЫЕ

Количество пикселей
по горизонтали ($N_{гор}$)

1140

Количества пикселей
по вертикали ($N_{верт}$)

1080

Частота кадровой
развертки (F_k), Гц

35

Вычислить
спектр сигнала (F_t), МГц

30.46

Рисунок 18 — Расчет исходных параметров

Стоит отметить, что при ошибке в любом поле исходных данных, стенд высвечивает ошибку, в которой сообщает, что значения введены неверно. Демонстрация ошибки представлена на рисунке 19.

После того как всё верно рассчитано, доступна настройка приборов. Была произведена проверка работы генератора сигнала в двух режимах работы. Включенный генератор имеет зелёную индикацию. При ошибке в настройках вида модуляции — режим работы сбросится, а изображение генератора сменится на исходное. Вид модуляции был выставлен прямоугольный, так как режим «по умолчанию» не несет функциональных свойств. Результат представлен на рисунках 20 — 22.

ИСХОДНЫЕ ДАННЫЕ

Количество пикселей
по горизонтали ($N_{гор}$)

1140

Количества пикселей
по вертикали ($N_{верт}$)

1080

Частота кадровой
развертки (F_k), Гц

30

Вычислить
спектр сигнала (F_t), МГц

Введите параметры в
соответствии с вашим
вариантом

Рисунок 19 — Ошибка при вводе неверных значений

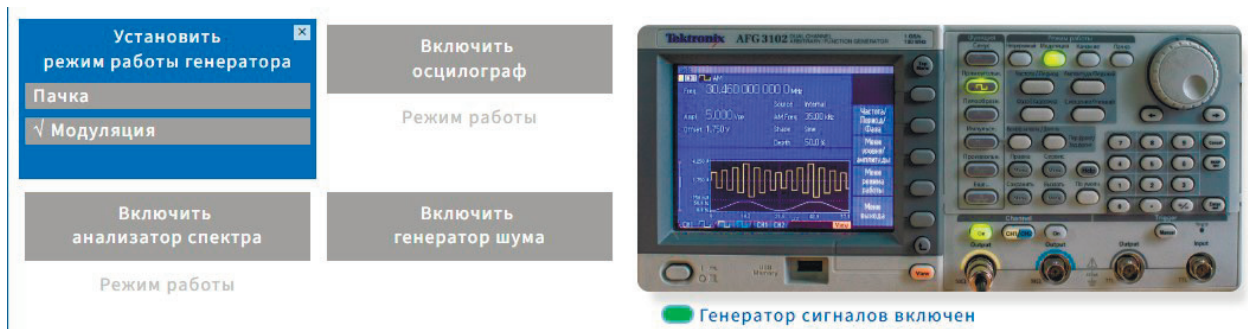


Рисунок 20 — Генератор сигналов в режиме «Модуляция»



Рисунок 21 — Генератор сигналов в режиме «Пачка»

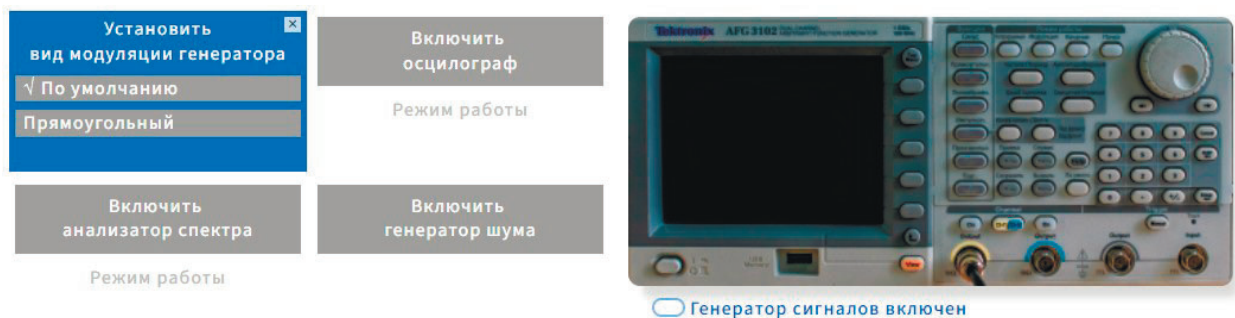


Рисунок 22 — Неверно настроенный генератор сигналов

В случае попытки настройки конфигурации генератора сигналов при его выключенном питании нарушитель увидит ошибку, представленную на рисунке 23.



Рисунок 23 — Ошибка при нарушении порядка настройки прибора

Была произведена проверка работы осциллографа. Прибор может функционировать при включенном в режиме «Модуляция» генераторе сигналов. Включенный осциллограф имеет зеленую индикацию. В случае неправильной настройки генератора индикация изменится на красную, и изображение вернется на исходное. Было проверено два режима осциллографа: «Форма сигнала» и «Спектр сигнала». Результат представлен на рисунках 24 — 26 соответственно.



Рисунок 24 — Форма сигнала

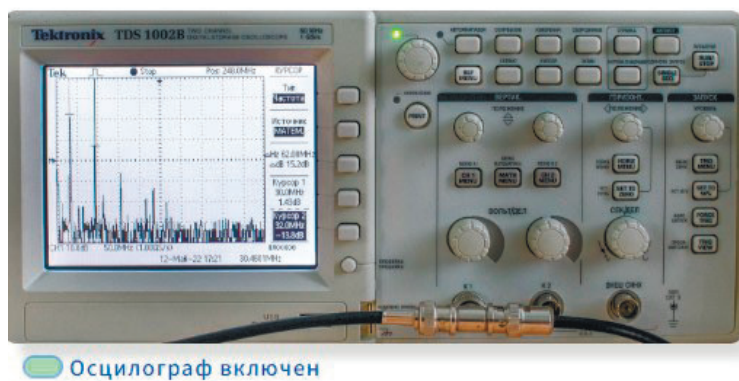


Рисунок 25 — Спектр сигнала



Рисунок 26 — Неверная настройка приборов

Была произведена проверка работы анализатора спектра. При проведении исследований дополнительно используется Генератор шума. Данный прибор представлен на стенде в виде кнопки и имеет два состояния: «Включен» и «Выключен». Анализатор спектра может функционировать в четырех режимах, каждый из которых работает при соблюдении определенных условий:

- «Тестовый сигнал + объектовый шум», работает при включенном в режиме «Модуляция» генераторе сигналов и отключенном генераторе шума;
- «Объектовый шум», работает при включенном в режиме «Пачка» генераторе сигналов и отключенном генераторе шума;
- «Тестовый сигнал + объектовый шум + зашумление», работает при включенном в режиме «Модуляция» генераторе сигналов и включенном генераторе шума;
- «Объектовый шум + зашумление», работает при включенном в режим «Пачка» генераторе сигналов и включенном генераторе шума.

Во включенном состоянии анализатор спектра имеет зеленую индикацию. В случае неверно настроенных приборов, от которых зависит работа анализатора, индикация становится красной. Результаты проверки представлена на рисунках 27 — 31.



Рисунок 27 — Тестовый сигнал + объективный шум



Рисунок 28 — Объективный шум



Рисунок 29 — Тестовый сигнал + объективный шум + зашумление



Рисунок 30 — Объективный шум + зашумление



Рисунок 31 — Неверная настройка приборов

Были проверены защитные меры, внедренные в рабочее пространство виртуального стенда. Если сессия не была завершена или студент бездействовал в течении 10 минут — система завершит сессию и попросит повторную аутентификацию. Результат представлен на рисунке 32.

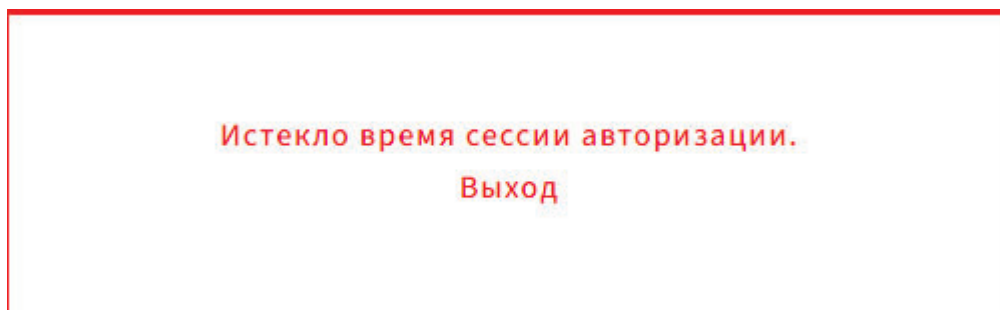


Рисунок 32 — Таймер активной сессии

Были произведены попытки открыть консоль разработчика и сохранить изображение прибора на компьютер. Поскольку защитные меры запрещают вызывать консоль разработчика с помощью клавиши «F12», сочетания клавиш «Ctrl+Shift+J», а так же запрещен вызов контекстного меню нажатием правой клавиши мыши — не удалось попасть в консоль разработчика или сохранить изображения.

Был открыт файл с методическими указаниями в новой вкладке и произведено завершение сессии. На вкладке, где были открыты методические указания, появилась ошибка, представленная на рисунке 33.

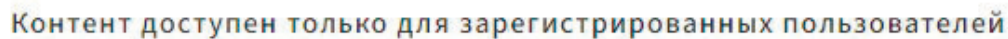


Рисунок 33 — Ограниченный доступ к методическим указаниям по лабораторной работе

Таким образом был проверен функционал панели администратора, рабочей среды виртуального стенда, а так внедренных защитных мер. В ходе тестирования недостатки не были выявлены. Ссылка на панель администратора и рабочее пространство виртуального стенда представлены ниже:

- Панель Администратора: <https://stend-tzi.ru/admin> ;
- Рабочее пространство виртуального стенда: <https://stend-tzi.ru> .

7 Вредные психофизические факторы, влияющие на органы зрения специалиста по информационной безопасности.

Методы и средства физической культуры, снижающие их воздействие

Зрения является одним из самых важнейших органов чувств. С его помощью мы получаем огромный поток информации. Зрение отвечает за нашу безопасность, контакты с окружающими и эмоциональное состояние. Невозможно встретить человека, которого не волнует состояние его глаз. По статистике, проблемы со зрением есть у каждого второго специалиста по информационной безопасности.

Сегодня на человека воздействует множество неблагоприятных факторов, как через его собственный неправильный образ жизни, так и извне. Например, длительное нахождение в закрытых помещениях негативно влияет на остроту зрения. Ученые подтвердили, что люди, которые проводят больше времени на открытом воздухе, гораздо меньше склонны к ухудшению зрения, чем домоседы.

Избыточный вес является ещё одним фактором, который может привести к потере зрения. Конечно, напрямую он не влияет, но может вызвать болезни, такие как диабет, которые приводят к ухудшению или вовсе потере зрения. Курение также связывают со скоростной потерей зрения. Исследования подтвердили, что у курильщиков есть повышенный риск развития катаракты, а так же дистрофия сетчатки.

Даже если специалист по информационной безопасности много проводит времени на свежем воздухе и ведет здоровый образ жизни — он всё равно подвержен риску. Непрерывная работа за компьютером вызывает сухость глаз, что может привести к дискомфорту, а в плохом случае — к инфекции. Во избежание этого следует делать короткие перерывы во время работы, чтобы дать глазам отдохнуть. Стоит отметить, что правильно подобранное освещение рабочего места является залогом здоровья зрения.

Освещение должно быть достаточным для работы за равномерно освещенным столом, и не должно быть чрезмерным, при котором свет бьет по глазам.

Чтобы избежать ухудшение зрения рекомендуется совершать ежедневные прогулки на свежем воздухе, во время прогулок взгляд расслабляется, ведь ему не нужно концентрировать взгляд на одной точке. Необходимо также заботиться о поступлении витаминов А, Е, С в организм. Они могут содержаться в таких продуктах как черника, морковь, смородина.

При использовании смартфона или компьютера в темное время суток рекомендуется снижать яркость, чтобы не было резкого контраста яркости, который создаёт нагрузку на глаза [13].

Для профилактики и улучшения зрения рекомендуется регулярно делать упражнения для глаз. Ниже представлены несколько видов упражнений, которые помогают предотвратить падение зрения.

- «Поочередное мигание». В течении двух минут необходимо быстро и часто моргать. Данное упражнение способствует ускорению кровообращению в тканях;

- «Глаза совы». Необходимо сесть на стул и держать спину прямо. Суть упражнения состоит в крепком зажмуривании глаз на 5 секунд и широком открытии век. Упражнение рекомендовано повторять до 10 раз. Этот метод укрепляет мышцы глазного яблока.

- «Массаж». Необходимо тремя пальцами коснуться век на обоих глазах. Касание должно длиться 1-2 секунды, а нажатие не должно быть сильным. Упражнение рекомендовано делать до 5 раз. Это упражнение ускоряет циркуляцию жидкостей в тканях зрительного аппарата и помогает бороться с отечностью.

- «Жмурки». Чтобы расслабить глазные мышцы и снизить напряжение с глаз, нужно сильно зажмуриться на пять секунд, а затем

открыть глаза на такой же период времени. Повторять метод нужно от пяти до семи раз.

Выполняя данные упражнения, совершая частые прогулки на свежем воздухе, а так же выполняя рекомендации по освещению рабочего места и отказ от вредных привычек гарантирует сохранение остроты зрения на более продолжительное время даже при долгой работе за компьютером [14].

Заключение

В ходе выполнения дипломного проекта была выполнена основная его цель — разработка защищенного виртуального стенда для дистанционного выполнения лабораторных работ.

На первом этапе были проанализированы используемые технологии виртуализации, описана ее предыстория, выделены основные принципы виртуализации, выбрана и обоснована технология, на основе которой будет разработан защищенный виртуальный стенд.

На втором этапе была разработана структура защищенного виртуального стенда.

На третьем этапе было разработано дерево событий защищенного виртуального стенда.

На четвертом этапе был разработан защищенный виртуальный стенд.

На пятом этапе были внедрены защитные меры, были выявлены угрозы информационной безопасности для защищенного виртуального стенда, и разработаны защитные меры.

На шестом этапе была произведена проверка работоспособности защищенного виртуального стенда и действие его защитных средств.

На седьмом этапе были рассмотрены вредные психофизические факторы, влияющие на органы зрения специалиста по информационной безопасности. Были выявлены меры и средства физической культуры, снижающие их воздействие.

Техническое задание на выпускную квалификационную работу выполнено в полном объеме.

Список используемых источников

- 1 Светлана Соболева (Блог компании ИТ Интегратора «СТЭК») // Что такое виртуализация? [Электронный ресурс] URL: <https://stekspb.ru/blog/virtualizaciya/> (дата обращения 11.06.2022);
- 2 Блог компании хостинга облачных серверов «Маклауд» (Сообщество IT-специалистов «ХАБР») // Виртуалка-камуфляж: вредоносный подход к виртуализации. [Электронный ресурс] URL: <https://habr.com/ru/company/maccloud/blog/559730/> (дата обращения 11.06.2022);
- 3 Блог компании облачных решений для бизнеса 1cloud.ru (Сообщество IT-специалистов «ХАБР») // Виртуализация: история и тренды развития. [Электронный ресурс] URL: <https://habr.com/ru/company/1cloud/blog/237005/> (дата обращения 11.06.2022);
- 4 Александр Косивченко (Сообщество IT-специалистов «ХАБР») // Зачем же нужна виртуализация? [Электронный ресурс] URL: <https://habr.com/ru/post/91503/> (дата обращения 12.06.2022);
- 5 Национальный открытый университет «ИНТУИТ» // Технологии виртуализации [Электронный ресурс] URL: <https://intuit.ru/studies/courses/3508/750/lecture/27408?page=2> (дата обращения 12.06.2022);
- 6 Алёна Терентьева (Блог компании AZOFT) // Стек технологий для разработки веб-приложений: что важно знать. [Электронный ресурс] URL: <https://www.azoft.ru/blog/web-development-stack/> (дата обращения 12.06.2022);
- 7 Сообщество IT-специалистов «ХАБР» // Вадим Сырцев — Использование диаграммы вариантов использования UML. [Электронный ресурс] URL: <https://habr.com/ru/post/566218/> (дата обращения 12.06.2022);

8 The Creately Blog // Учебное пособие по диаграмма последовательностей: полное руководство с примерами. [Электронный ресурс] URL: <https://creately.com/blog/ru/диаграмма/учебное-пособие-по-последовательной/> (дата обращения 12.06.2022);

9 Сергей Давиденко (Интернет-блог «Планёрка») // Диаграмма коммуникации UML. [Электронный ресурс] URL: <https://planerka.info/item/diagrammy-kommunikacij-uml/> (дата обращения 13.06.2022);

10 Сайт студентов кафедры МОСИТ // Диаграмма компонентов. [Электронный ресурс] URL: http://imlearning.ru/netcat_files/file/FSIS/ФСИС_семинар-9_Диаграмма-компонентов.pdf (дата обращения 20.05.2022);

11 Свободная энциклопедия Wikipedia // Блок схема [Электронный ресурс] URL: <https://ru.wikipedia.org/wiki/Блок-схема> (дата обращения 13.06.2022);

12 Федеральная служба по техническому и экспортному контролю (ФАУ «ГНИИИ ПТЗИ ФСТЭК России») // Банк данных угроз безопасности [Электронный ресурс] URL: <https://bdu.fstec.ru/threat> (дата обращения 14.06.2022);

13 Блог компании ООО «Ядран» // Из-за чего портится зрение? [Электронный ресурс] URL: <https://optinol.ru/poleznaya-informatsiya/iz-za-chego-portitsya-zreniye> (дата обращения 14.06.2022);

14 Керимов Эрвин (Элит Плюс клиника) // Упражнения для глаз для улучшения зрения. [Электронный ресурс] URL: <https://elitplus-clinic.ru/stati/uprazhneniya-dlya-glaz.html> (дата обращения 14.06.2022);

15 Справочник языка php.ru (Сообщество РНР-программистов) // Управляющие конструкции [Электронный ресурс]

URL: <https://php.ru/manual/language.control-structures.html> (дата обращения 11.05.2022);

16 Руководство по PHP (The PHP Group) // Ошибки [Электронный ресурс] URL: <https://www.php.net/manual/ru/language.errors.php>(дата обращения 11.05.2022).