Разработка клиент-серверного приложения автошколы и обеспечение её информационной безопасности

Подготовил студент группы ИБ-1-20:
Абыл уулу Нурзамат

Введение

В современном мире, где информационные технологии стали неотъемлемой частью многих сфер деятельности, включая образование, многие учебные организации прибегают к использованию клиент-серверных приложений. В частности, автошколы активно внедряют технологии для улучшения своей эффективности и качества обучения. Тем самым разработка и обеспечение безопасности клиент-серверного приложения автошколы становится критически значимым аспектом, требующим к себе особого внимания.

ЦЕЛЬ

Цель работы заключается в разработке и обеспечении информационной безопасности клиент-серверного приложения автошколы, включающая в себя состав:

- Управление базой данных курсантов;
- Работу сотрудников;
- Обеспечение безопасности системы и всех основных процессов, входящих в состав автошколы;

ЗАДАЧИ

1. Анализ предметной области.
2. Обзор системы организации.
3. Описание бизнес процессов.
4. Описание связи между бизнес процессами.
5. Разработка модели угроз.
6. Разработка модели нарушителя.

ОБОСНОВАНИЕ К РАЗРАБОТКЕ

- УЛУЧШЕНИЕ УПРАВЛЕНИЯ РАСПИСАНИЕМ
- ЦЕНТРАЛИЗОВАННОЕ ХРАНЕНИЕ ДАННЫХ
- ОБМЕН ИНФОРМАЦИЕЙ
- УЛУЧШЕНИЕ КАЧЕСТВА ОБУЧЕНИЯ
- АВТОМАТИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ
- ПОВЫШЕНИЕ БЕЗОПАСНОСТИ

ОБЗОР СИСТЕМЫ АВТОШКОЛЫ

- РЕГИСТРАЦИЯ / АВТОРИЗАЦИЯ
- ПРОСМОТР СПРАВОЧНИКА СОТРУДНИКОВ, КУРСАНТОВ
- СКАЧИВАНИЕ ОТЧЕТОВ
- ВВЕДЕНИЕ УСПЕВАЕМОСТИ КУРСАНТОВ
- ВВЕДЕНИЕ РАСПИСАНИЯ ЗАНЯТИЙ
- ДОБАВЛЕНИЕ, УДАЛЕНИЕ, ОБНОВЛЕНИЕ ГРУПП, КУРСАНТОВ, СОТРУДНИКОВ
- НАГРУЗКА ПРЕПОДАВАТЕЛЕЙ

ФУНКЦИИ ПРИЛОЖЕНИЯ

- Регистрация / Авторизация
- Просмотр справочника сотрудников, курсантов
- Введение расписания занятий
- Добавление, удаление, обновление групп, курсантов, сотрудников
- Нагрузка преподавателей

Идентификация активов

Бизнес-процесс	Активы	Среда обработки	ПСИБ	Уязвимости
Регистрация	Персональные данные (ИА-1)	QT V6 (ПА)	К,Ц,Д	CVE-2021-1636
	MS SQL Server 2017 CU31 (ПА)			CVE-2022-23298 CVE-2019 11137
Авторизация	Идентификационные данные (ИА-2)	QT V6 (ПА)	К,Ц,Д	CVE-2022-29143 CVE-2017-8516
	MS SQL Server 2019 CU31 (ПА)			CVE-2022-24454 CVE-2019-11137
Редактирование аккаунтов пользователей	База данных (ИА -3)	Microsoft SQL Server 2019 (RTM) 15.0.2000.5 Enterprise Edition	Д,Ц,К	CVE-2022-29143 CVE-2017-8516
		MS Office 2019 16.0	Д,Ц,К	CVE-2022-24454
	15.0.2000.5 Enterprise Edition (ПА) MS Office 2019 16.0 (ПА)	QT V6 (ПА)	Д,Ц,К	CVE-2019-11137
Обработка информации	База данных (ИА-3)	Microsoft SQL Server 2019 (RTM) 15.0.2000.5	Ц,Д,К	CVE-2022-34006
Нагрузка преподавателей	База данных (ИА-3)	Microsoft SQL Server 2019 (RTM) 15.0.2000.5 Enterprise Edition	Ц,Д,К	CVE-2022-34006
	Microsoft SQL Server 2019 (RTM)	MS Office 2019 16.0	Ц,Д,К	CVE-2022-3140
	Windows 10 Enterprise 21H2 (ПА)	QT V6 (ПА)	Ц,Д,К	CVE-2022-23298

Модель нарушителя

Тип нарушителя	Вид нарушителя	Описание уровня доступа	Мотивация нарушителя	Квалификация, знания и ресурсы нарушителя	Реализуемые угрозы	Способы реализации угроз
Антропогенный, Тип А (Сотрудник, не имеющий доступа)	Внутренний нарушитель	Физический доступ к системе	Корыстный умысел, месть, любопытство	Владение информацией об аппаратном и программном оснащении компьютера	НСД к персональному компьютеру	Копирование/перемещение информации, представляющей ценность для организации на внешний носитель
	Внутренний нарушитель					Заражение ОС троянской программой. Перебор пароля пользователя по словарю при удаленном подключении к компьютеру

Продолжение таблицы модель нарушителя

Антропогенный, Тип Б (Компьютерный злоумышленник)	Внешний	Доступ по протоколу IP к интернет-шлюзу со стороны интернет-сети	Корыстный умысел, месть, любопытство, вандализм	Знание стека сетевых протоколов TCP/IP, знание IP-адреса интернет-шлюза	Сбои, отказы, разрушения/повреждения программных и технических средств	DoS-атака
				Знание языка SQL, протоколов HTTP/HTTPS	SQL-инъекция	Внедрение вредоносного sql кода в формы или строку запроса
				Владение программными средствами перехвата пакетов в IP сетях, знание IP-адреса интернет-шлюза организации в сети «интернет»	Перехват аутентификационных данных	Компрометация интернет-шлюза (подбор идентификатора последовательности и номера порта-отправителя)

Продолжение таблицы модель нарушителя

	Внешний	Удаленный доступ к серверу системы, персональному компьютеру сотрудника	Корыстный умысел, месть, любопытство, вандализм	Наличие электронного почтового ящика. Навыки использования электронной почты. Знание стека протоколов TCP/IP	Сбой/отказ; Компрометация данных, передаваемых посредством интернета	Перебор пароля пользователя по словарю при удаленном подключении к компьютеру с вредоносным вложением;
Антропогенный, Тип В (Сотрудник организации, имеющий право работы с системой, а также имеющие к нему физический доступ)	Внутренний нарушитель	Физический и логический доступ к серверу системы, персональному компьютеру сотрудника	Корыстный умысел, месть, любопытство, халатное отношение	Владение информацией об аппаратном и программном оснащении компьютера	НСД к персональному компьютеру	Заражение ОС троянской программой.
	Внутренний нарушитель			Владение информацией об аппаратном и программном оснащении сервера	Удаление/модификация данных, хранящихся на сервере	Запуск исполняемого файла с цифровой подписью доверенного приложения

Модель угроз

Угроза ИБ	Источник угрозы ИБ	Актив				Метод реализации угрозы ИБ на среду обработки ИА	Последствия реализации угрозы ИБ
		Информационный актив	Значимые свойства ИБ в порядке приоритета	Среда обработки ИА	Уязвимость среды обработки ИА		
Сбои и отказы в обслуживании	Антропогенный тип Б	Информация открытого доступа	Доступность Целостность Конфиденциальность	QT framework v6	BDU:2021-02185, BDU:2020-02766	DDOS-атака. Посылание большого количества вредоносных запросов на сервер.	Остановка работы сервера и выдачи ошибки отказ в обслуживании
SQL-инъекции		Персональные данные и данные ограниченного доступа	Целостность Конфиденциальность Доступность	SQL Server 2019	BDU:2019-01225	Внедрение вредоносного SQL-кода в запросы к информационной системе	Нарушение целостности и конфиденциальности

Продолжение таблицы модель угроз

Повышение привилегий	Антропогенный Тип В	Данные ограниченного доступа	Конфиденциальность Целостность Доступность	QT framework v6	BDU:2021-02185, BDU:2020-02766	Повышение привилегий — эксплуатация уязвимостей в операционной системе или прикладном ПО	Нарушение конфиденциальности и целостности
Кража аутентификационных данных	Антропогенный Тип В	Персональные данные	Конфиденциальность Целостность Доступность	QT framework v6	BDU:2021-02185, BDU:2020-02766	Атака человек по середине	Нарушение конфиденциальности

Продолжение таблицы модель угроз

Обход контроля доступа	Антропогенный Тип Б	Данные ограниченного доступа, Персональные данные	Доступность Конфиденциальность Целостность	QT framework v6	BDU:2023-03689	SQL-атака, подмена, URL-адреса	Нарушение конфиденциальности и доступности
Выход из строя	Техногенный и/или Стихийный	Информация открытого доступа, Данные ограниченного доступа, Персональные данные	Доступность, Целостность, Конфиденциальность	Windows Server сеть организации	Возможные поломки системы, вызванные различными обстоятельствами		Нарушение целостности и/или доступности

Механизмы защиты

LOG4QT

Log4Qt - это порт C++ пакета Log4j Apache Software Foundation с использованием Qt Framework.

TINYWALL

Fire Wall для сетевого трафика

ВАЛИДАЦИЯ ДАННЫХ

Проверка вводимых данных на валидность

ЗАЩИТА ОТ SQL INJECTION

Защита от запросов с произвольного кода

QT SECRET

Модуль для шифрования данных

Диаграмма IDEF0

USED AT:	AUTHOR: Abyl uulu Nurzamat	DATE: 11.06.2000	WORKING	READER DATE	CONTEXT:
	PROJECT: AutoSchool	REV: 12.06.2024	DRAFT		TOP
			RECOMMENDED		
	NOTES: 1 2 3 4 5 6 7 8 9 10		PUBLICATION		

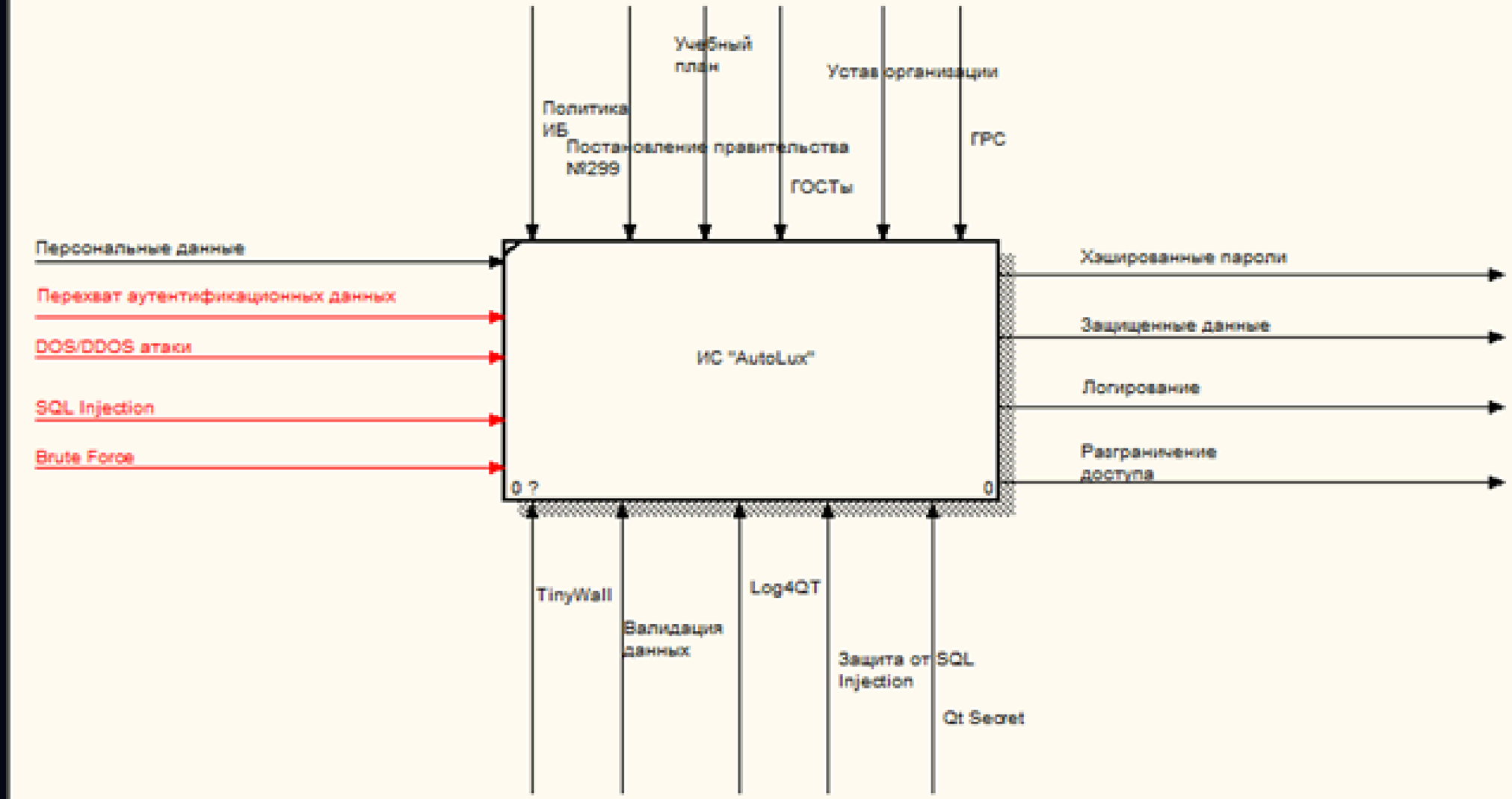
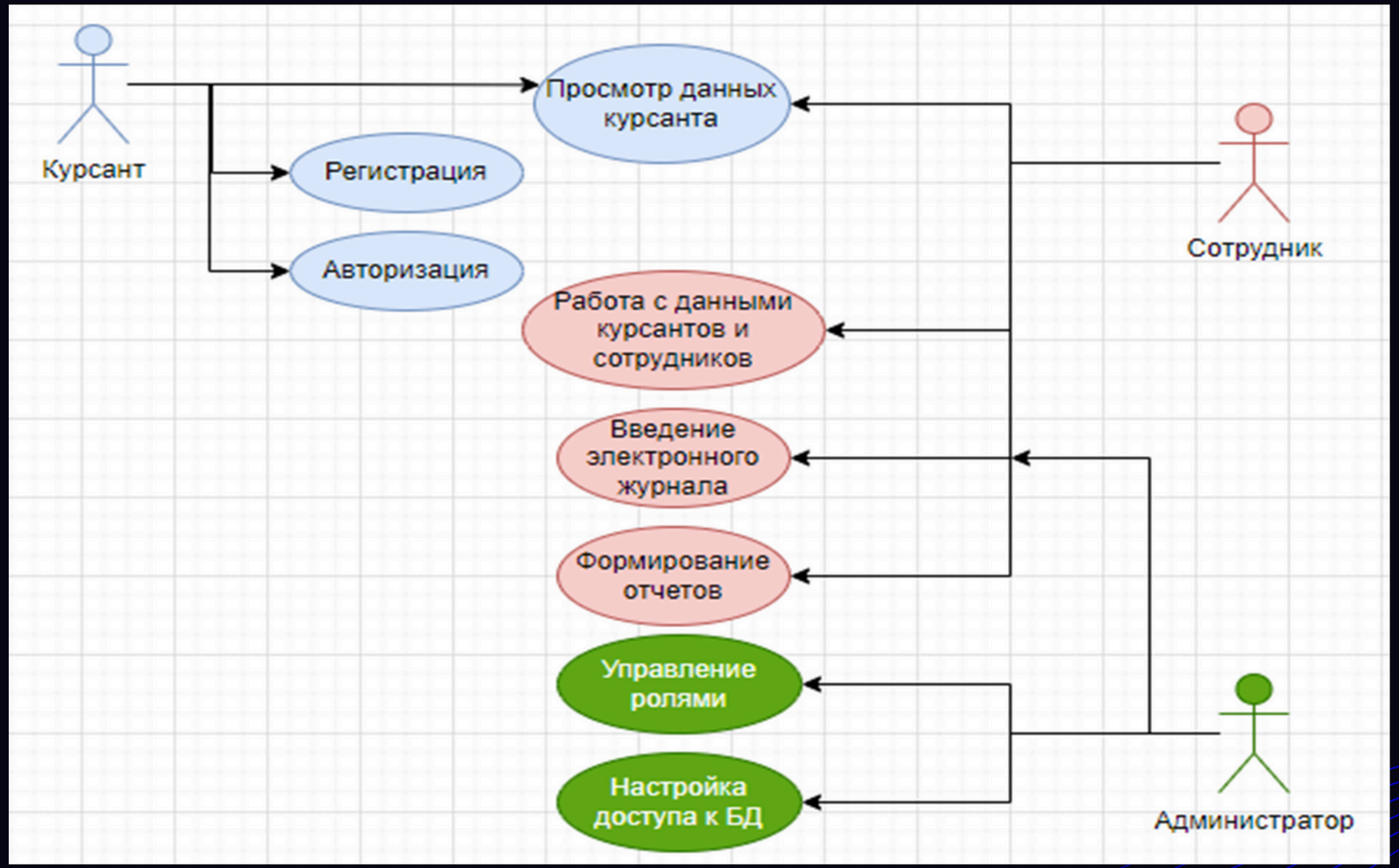
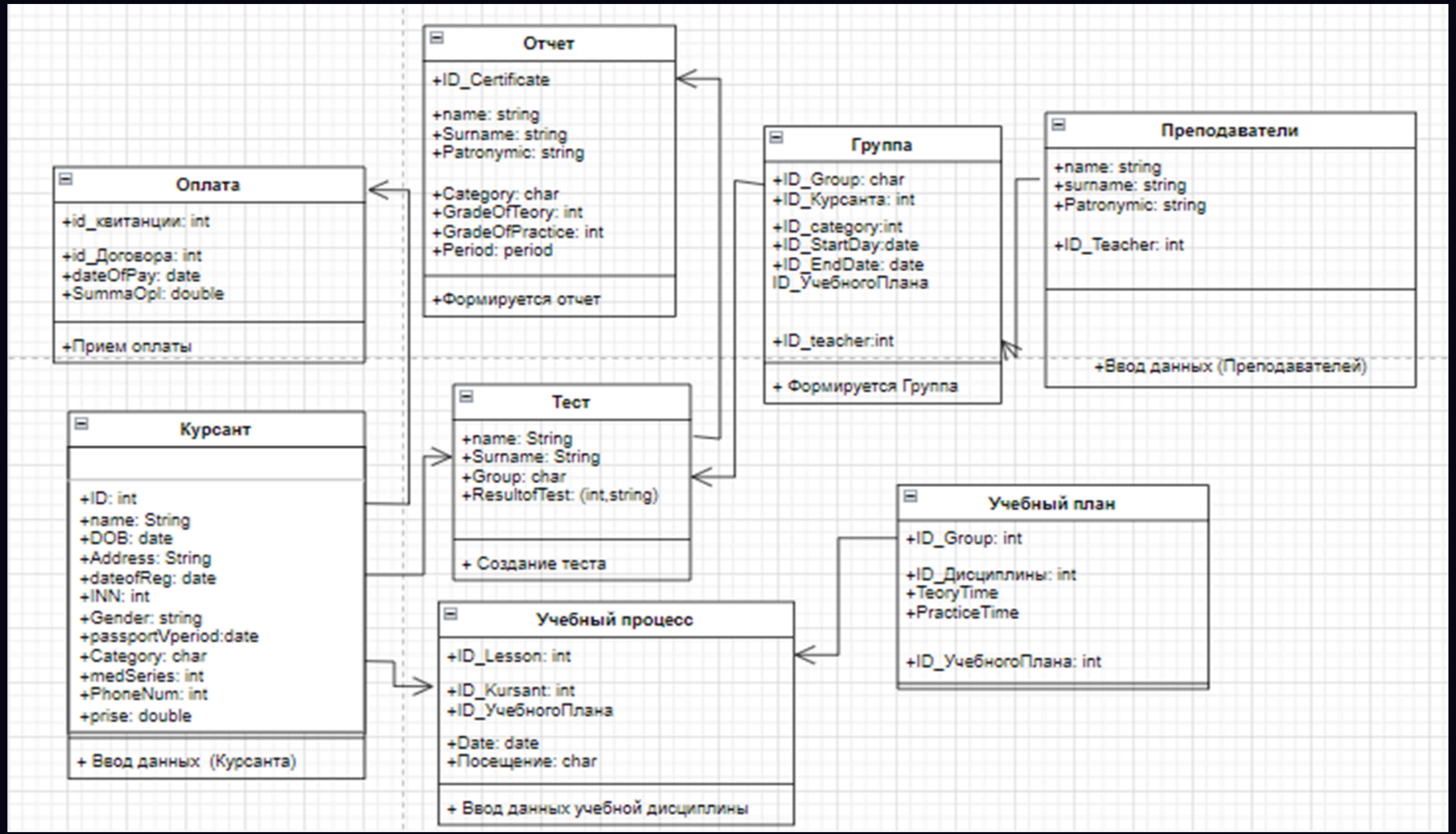


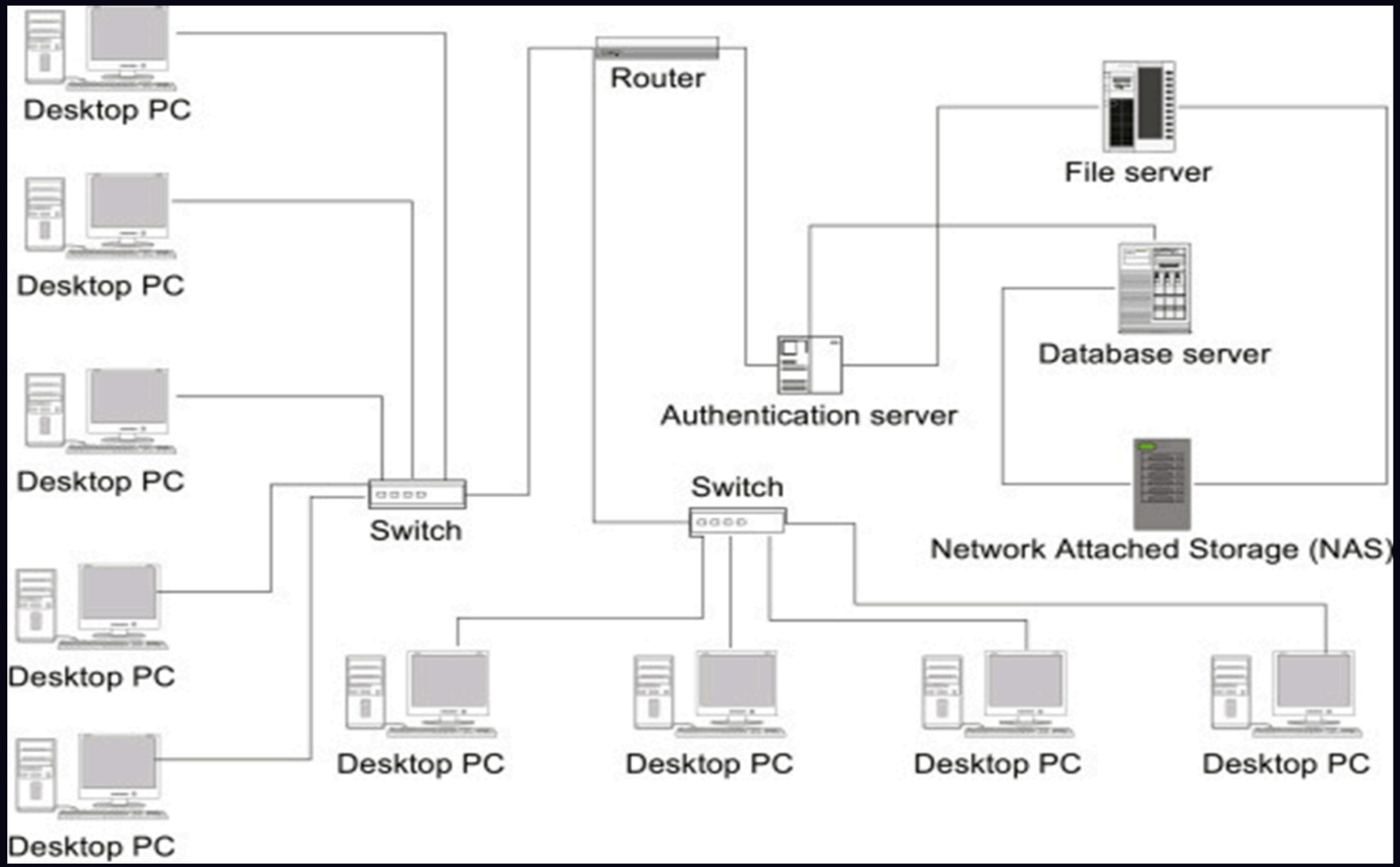
ДИАГРАММА USE - CASE



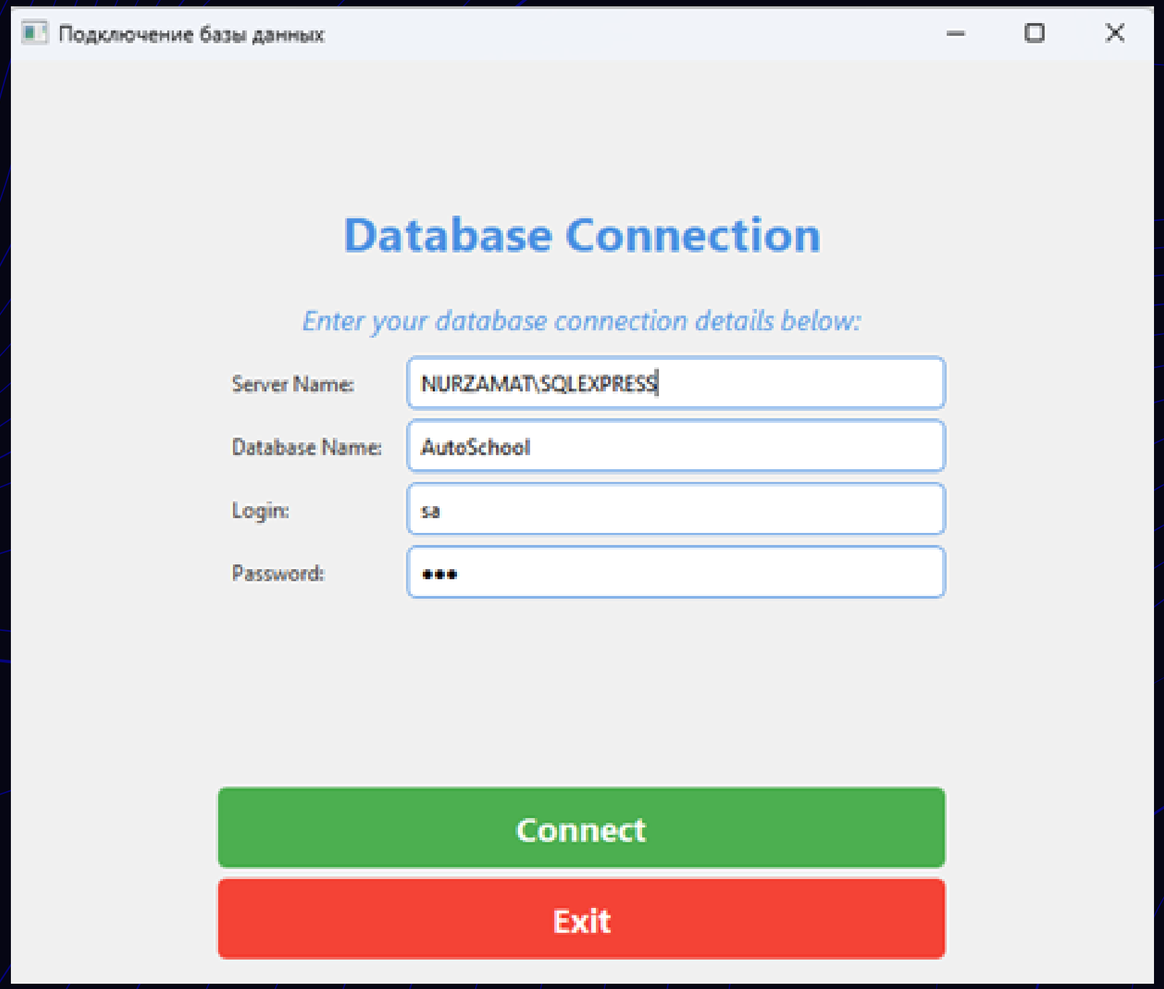
ER - ДИАГРАММА

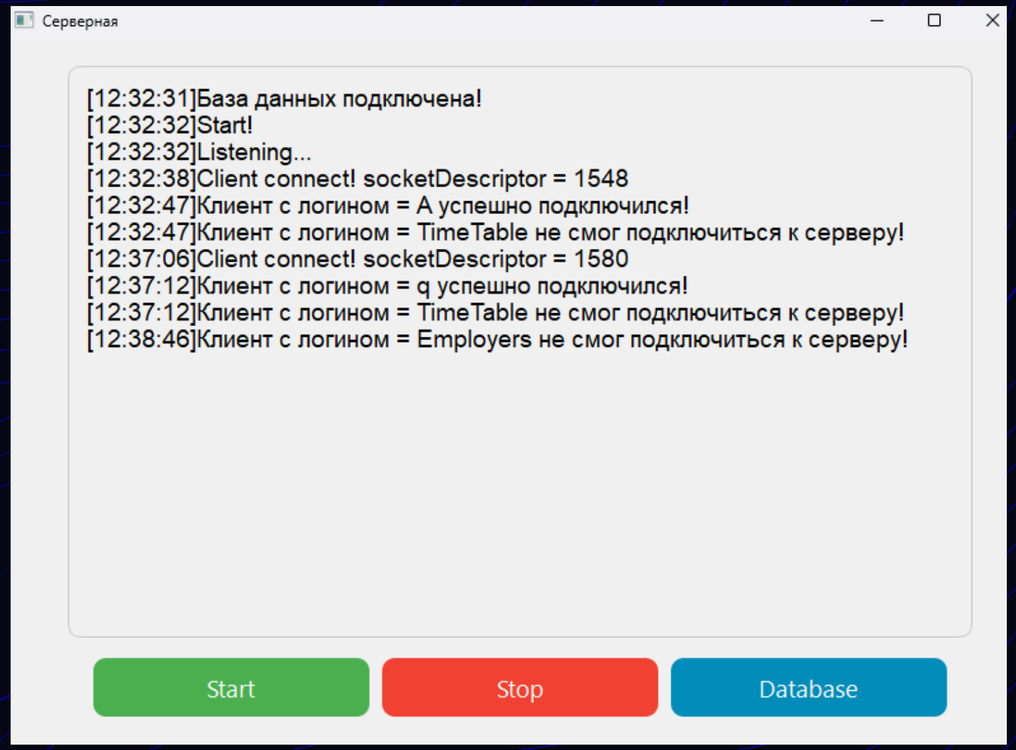


АРХИТЕКТУРА СЕТИ



ОБЗОР СИСТЕМЫ

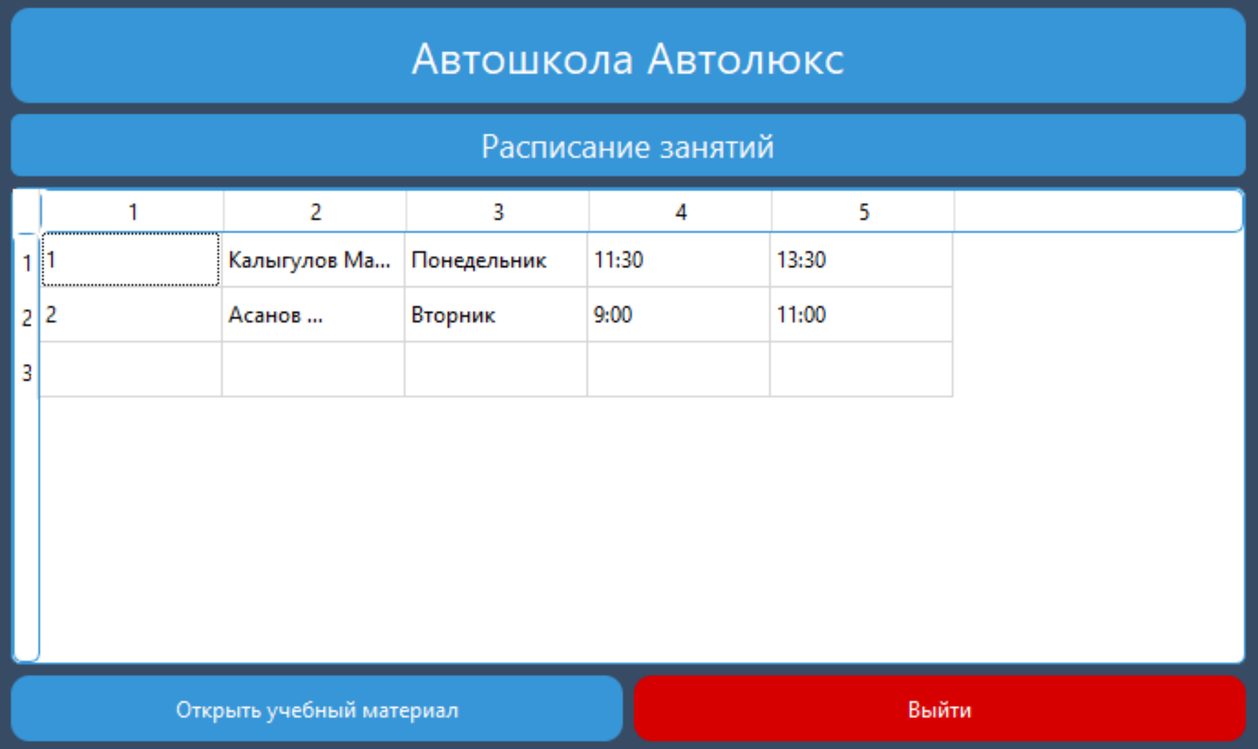


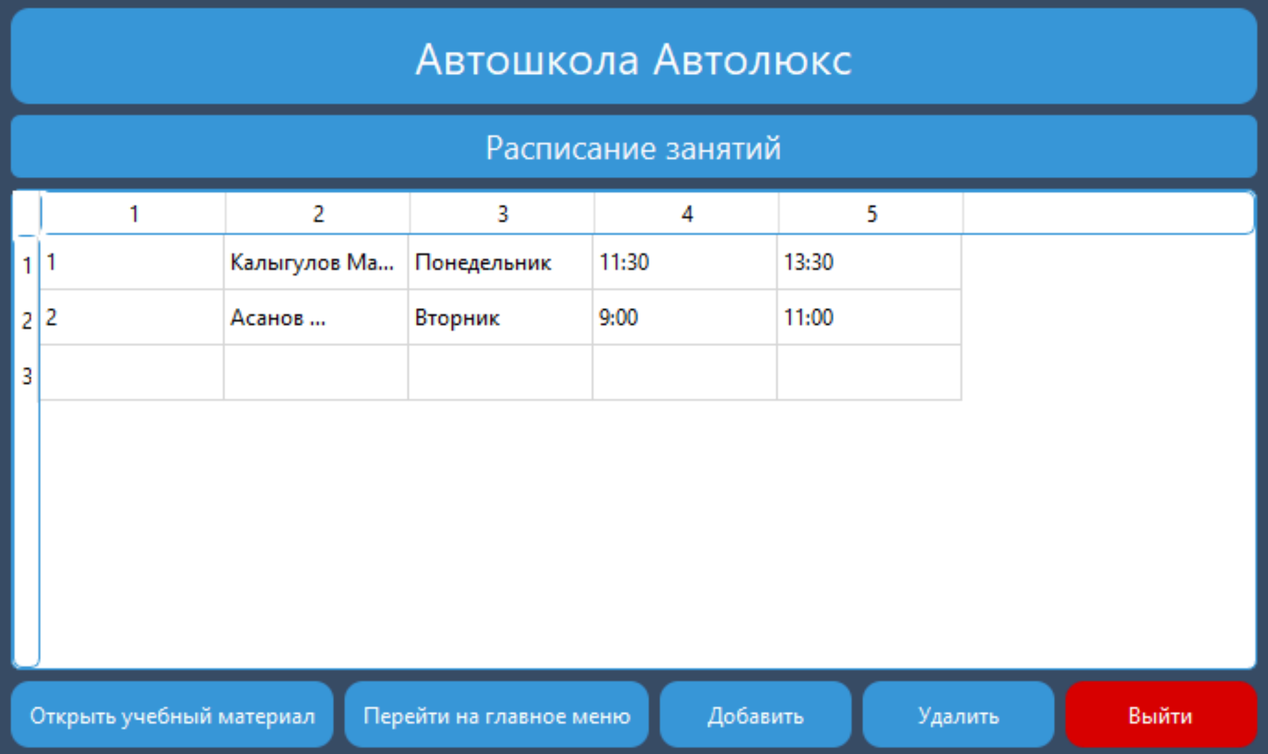


СЕРВЕРНАЯ ЧАСТЬ

Клиентская часть

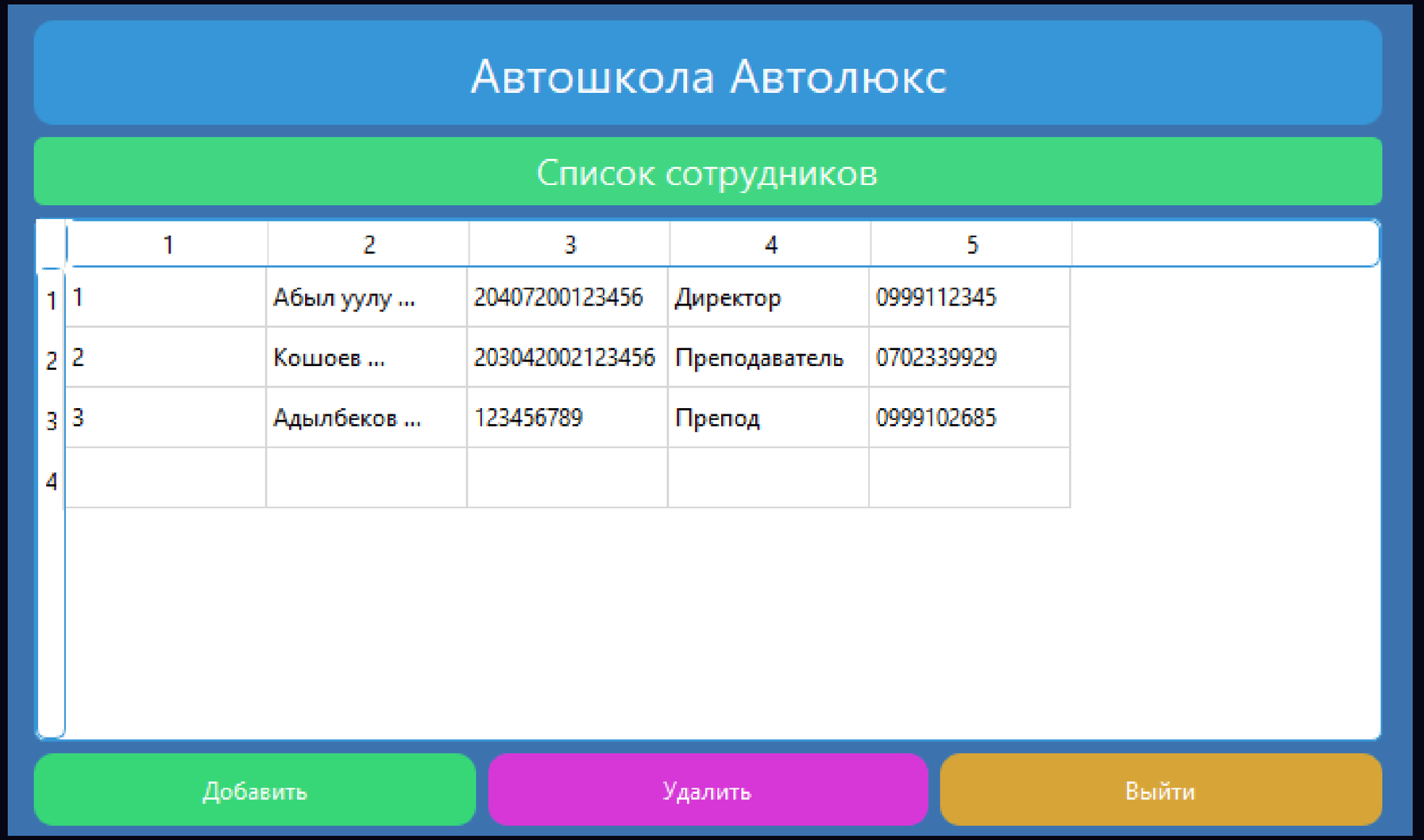
Если заходит курсант то у него будет доступ только к просмотру расписания занятий и учебных материалов.





Главное меню системы

Форма сотрудников



Заключение

В ходе выполнения дипломного проекта была разработана клиент-серверная система для автошколы, обеспечивающая удобное управление учебным процессом, а также взаимодействие между администрацией, инструкторами и учащимися. Проект включал в себя создание и управления расписанием, редактирование с данными курсантов и преподавателей, что позволяет значительно повысить эффективность работы автошколы.

Спасибо за внимание!