**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ**

**КЫРГЫЗСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ имени И.РАЗЗАКОВА**

**КАФЕДРА «ПРОГРАММНОЕ ОБЕСПЕСЕНИЕ**

**КОМПЬЮТЕРНЫХ СИСТЕМ»**

**ВЫПУСКНАЯ**

**КВАЛИФИКАЦИОННАЯ РАБОТА**

**Разработка клиент-серверного приложения автошколы и обеспечение её информационной безопасности**

на академическую степень бакалавра

**по направлению: 590100 «Информационная безопасность»**

|  |  |
| --- | --- |
| **Выполнил**  **Группа** | **Абыл уулу Нурзамат**  **ИБ(б)-1-20** |
| **Руководитель** | **доцент Вагнер Андрей Арнович** |

**Бишкек 2024**

**КЫРГЫЗ РЕСПУБЛИКАСЫНЫН БИЛИМ БЕРҮҮ**

**ЖАНА ИЛИМ МИНИСТРЛИГИ**

**И.РАЗЗАКОВ атындагы КЫРГЫЗ МАМЛЕКЕТТИК ТЕХНИКАЛЫК**

**УНИВЕРСИТЕТИ**

**«КОМПЬЮТЕРДИК СИСТЕМАЛАРДЫ ПРОГРАММАЛЫК КАМСЫЗДОО»**

**кафедрасы**

**БҮТҮРҮҮЧҮ**

**КВАЛИФИКАЦИЯЛЫК ИШ**

**Автомектептин клиент-сервердик тиркемесин иштеп чыгуу жана анын маалыматтык коопсуздугун камсыздоо**

бакалавр академиялык даражасы

**590100 «Маалыматтык коопсуздук» багыты боюнча**

|  |  |
| --- | --- |
| **Аткарган**  **Топ** | **Абыл уулу Нурзамат**  **ИБ(б)-1-20** |
| **Жетекчи** | **доцент Вагнер Андрей Арнович** |

**Бишкек 2024**

**АННОТАЦИЯ**

В данной выпускной квалификационной работе представлены результаты разработки клиент-серверного приложения автошколы и обеспечение ее информационной безопасности.

Данная работа состоит из 5 основных глав: анализ и разработка требований, конструкторские работы, проектирование безопасности, разработка документации, экспериментальный раздел. А также введение, заключение, список литературы, глоссария и приложения.

Глава «Анализ и разработка требований» описывает процессы клиент-серверного приложения автошколы, также в этой главе представлена классификация информации, идентификация активов.

В главе «Конструкторские работы» представлены разработка концептуальной модели и модели потоков данных клиент-серверного приложения.

В главе «Проектирование безопасности» представлена перечень процессов системы защиты информации, направленных на снижение уровня риска до приемлемого.

В главе «Разработка документации» содержится описание программы, а также руководство для администратора, программиста и пользователя.

В главе «Экспериментальный раздел» приводится план тестирования и результаты проведенного тестирования.

В состав данной работы также входят приложения.

Выпускная квалификационная работа состоит из 61 страниц, содержит 28 рисунков, количество таблиц 8, используется 8 источников.

**АННОТАЦИЯ**

Бул бүтүрүүчүлөрдүн квалификациялык ишинде автомектептин клиент-сервердик тиркемесин иштеп чыгуунун жана коопсуздугун камсыз кылуунун натыйжалары келтирилген.

Бул бүтүрүүчү иши 5 негизги бөлүмдөн турат: талаптарды изилдөө жана иштеп чыгаруу, конструктордук иштер, коопсуздукту долбоорлоо, документтештирүү иштери, эксперименталдык бөлүк. Ошондой эле кириш сөз, корутунду, колдонулган адабияттар, глоссарий жана тиркемеден турат.

«Талаптарды изилдөө жана иштеп чыгаруу» автомектептин клиент-сервердик тиркемесинин процесстерин сүрөттөйт, жана дагы бул бөлүмдө маалыматтын классификациясы жана активдерди идентификациялоо сунушталат.

«Конструктордук иштер» бөлүмүндө концептуалдык моделин жана агымдардын берилиши моделин иштеп чыгуусу чагылдырылган.

«Коопсуздукту долбоорлоо» бөлүмү тобокелдиктин деңгээлин алгылыктуу деңгээлге чейин төмөндөтүү үчүн багытталган маалыматтык коопсуздук тутумунун процесстеринин тизмесин камтыйт.

«Документтештирүү иштери» бөлүмүндө программанын баяндамасын, ошондой эле администратордун, програмисттин жана пайдалануучунун жетектемесин камтыйт.

«Эксперименталдык бөлүк» бөлүгүндө тестирлөөнүн планы жана тестирлөөнүн натыйжалары келтирилген.

Бул иш ошондой эле тиркемелерди камтыйт.

Бүтүрүүчүлүк квалификациялык иш 61 барактан турат, 28 сүрөттү камтыйт, жадыбалдардын саны 8, 8 булак колдонулган.

ОГЛАВЛЕНИЕ

[ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 7](#_Toc169095166)

[ВВЕДЕНИЕ 9](#_Toc169095167)

[ЦЕЛЬ 11](#_Toc169095168)

[ЗАДАЧИ 11](#_Toc169095169)

[ГЛАВА 1. АНАЛИЗ И РАЗРАБОТКА ТРЕБОВАНИЙ 12](#_Toc169095170)

[**1.1** **Общая характеристика объекта защиты** 12](#_Toc169095171)

[**1.2** **Обоснование для разработки** 12](#_Toc169095172)

[**1.3** **Обзор системы автошколы** 12](#_Toc169095173)

[**1.4** **Описание процессов** 16](#_Toc169095174)

[**1.5** **Функциональные требования** 16](#_Toc169095175)

[**1.6** **Основные процессы и информационные потоки** 16](#_Toc169095176)

[**1.7** **Требования к составу и параметрам технических средств** 17](#_Toc169095177)

[**Требования к системе** 17](#_Toc169095178)

[**1.4** **Требования к безопасности** 17](#_Toc169095179)

[**1.5** **Требования к средствам и способам связи для информационного обмена между компонентами системы.** 19](#_Toc169095180)

[**1.6** **Требования по диагностированию системы** 19](#_Toc169095181)

[**1.7** **Требования к надежности комплекса.** 19](#_Toc169095182)

[ГЛАВА 2. КОНСТРУКТОРСКИЕ РАБОТЫ 20](#_Toc169095183)

[**2.1** **Декомпозиция концептуальной модели** 20](#_Toc169095184)

[**2.2** **Организация структуры данных** 22](#_Toc169095185)

[**2.3** **Архитектура разрабатываемой системы** 22](#_Toc169095186)

[ГЛАВА 3. ПРОЕКТИРОВАНИЕ БЕЗОПАСНОСТИ 25](#_Toc169095187)

[**3.1 Процессы организации** 25](#_Toc169095188)

[**3.2 Инфраструктура клиент-серверного приложения** 25](#_Toc169095189)

[**3.3 Идентификация активов** 25](#_Toc169095190)

[**3.4 Модель нарушителя** 26](#_Toc169095191)

[**3.5 Модель угроз** 27](#_Toc169095192)

[**3.6** **Способы защиты от вероятных атак** 31](#_Toc169095193)

[**3.6.1 Log4Qt - Логирование** 32](#_Toc169095194)

[**3.6.2 TinyWall - FireWall** 34](#_Toc169095195)

[**3.6.3 Модуль QT-Secret** 35](#_Toc169095196)

[**3.6.4 RBAC** 36](#_Toc169095197)

[ГЛАВА 4. РАЗРАБОТКА ДОКУМЕНТАЦИИ 38](#_Toc169095198)

[**4.1** **Описание программы** 38](#_Toc169095199)

[**4.2** **Руководство разработчика** 38](#_Toc169095200)

[ГЛАВА 5. ТЕСТИРОВАНИЕ 40](#_Toc169095201)

[**5.1** **Брутфорс (brute force)** 40](#_Toc169095202)

[**5.2** **HoneyBot** 41](#_Toc169095203)

[**5.3** **Dos/ddos** 44](#_Toc169095204)

[ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 46](#_Toc169095205)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ 47](#_Toc169095206)

[ЗАКЛЮЧЕНИЕ 48](#_Toc169095207)

[ПРИЛОЖЕНИЯ 49](#_Toc169095208)

[ПРИЛОЖЕНИЕ А 50](#_Toc169095209)

[ПРИЛОЖЕНИЕ Б 53](#_Toc169095210)

[ПРИЛОЖЕНИЕ В 58](#_Toc169095211)

**ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

В данной выпускной квалификационной работе применяются следующие термины с соответствующими определениями:

Актив – это все, что имеет ценность для организации.

Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут беспрепятственно их реализовывать.

Защита информации – защита конфиденциальности, целостности и доступности информации.

Информационная безопасность – состояние защищенности информации, при котором обеспечивается ее конфиденциальность, доступность и целостность.

Информация – сведения (сообщения, данные) независимо от формы их представления. Информация в зависимости от категории доступа к ней подразделяется на информацию общедоступную, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Инцидент информационной безопасности (инцидент ИБ): появление одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации бизнес-операций и указывающих на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ для активов организации.

Конфиденциальность – свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

Модель нарушителя ИБ – описание и классификация нарушителей безопасности информационной, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз безопасности информационной со стороны указанных нарушителей.

Модель угроз ИБ – описание источников угроз безопасности информационной; методов реализации угроз безопасности информационной; объектов, пригодных для реализации угроз безопасности информационной; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности активов информационных); масштабов потенциального ущерба.

Нарушитель информационной безопасности (нарушитель ИБ) – физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение безопасности информационной организации.

Политика ИБ – формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области безопасности информационной, которыми руководствуется организация в своей деятельности.

Риск – мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

Событие информационной безопасности (событие ИБ) – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики безопасности информационной или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Угроза – потенциальная причина инцидента, который может нанести ущерб системе или организации.

Угроза ИБ – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Уязвимость (информационной системы) – свойство системы информационной, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации.

Целостность информации – состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения.

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.

Учитывая конфиденциальные информации, такие как данные курсантов и инструкторов, необходимо предпринимать шаги для защиты от утечек и несанкционированного доступа. Это включает в себя шифрование данных, управление доступом, регулярное обновление системы безопасности и мониторинг активности для выявления подозрительных ситуаций.

Также одним из ключевых аспектов разработки такого приложения является создание интуитивно понятного интерфейса как для инструкторов, так и для курсантов. Удобство использования приложения включает в себя функциональность для записи на занятия, отслеживания прогресса, доступа к учебным материалам и другим аспектам обучения.

Кроме того, важно обеспечить стабильную работу приложения, чтобы избежать проблем в процессе обучения. Регулярные тестирования, обновления и поддержка приложения помогут устранить возможные сбои и повысить его надежность.

Таким образом, разработка и обеспечение безопасности клиент-серверного приложения автошколы требует комплексного подхода, включающего в себя удобство использования, защиту данных и стабильность работы.

АКТУАЛЬНОСТЬ РАБОТЫ

В ходе выполнения анализа автошколы, были выявлены следующие проблемы:

***1. Неэффективное управление рутинными задачами:***

* Ручное ведение журнала посещаемости, регистрации курсантов, планирования занятий,
* Длительное время обработки заявок на обучение.
* Ошибки в документации.
* Неоптимальное использование ресурсов.

***2. Низкое качество обучения:***

* Отсутствие доступа к обучающим материалам 24/7.
* Неперсонализированный подход к обучению.
* Неэффективные методы обучения.
* Недостаточная обратная связь.

***3. Снижение конкурентоспособности:***

* Отсутствие современных технологий.
* Неудовлетворенность клиентов.
* Ограниченный спектр услуг.

***4. Повышенные риски:***

* Ошибки, связанные с человеческим фактором.
* Несоответствие требованиям законодательства.

В связи с этими проблемами, было принято решение разработать и обеспечить безопасность клиент-серверного приложения для автошколы.

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.

**ГЛАВА 1. АНАЛИЗ И РАЗРАБОТКА ТРЕБОВАНИЙ**

* 1. **Общая характеристика объекта защиты**

Клиентское приложение разработано на фреймворке QT v6 языка С++. Хранение базы данных производится на СУБД SQL Server. Целью клиент-серверного приложения является оптимизация работы и улучшение взаимодействия преподавателей и курсантов. Внедрение является практической мерой по обеспечению эффективности производственного процесса. Для работы приложения используется сервер написанный также на фреймворке QT.

* 1. **Обоснование для разработки**

Разработанное клиент-серверное приложение для автошколы предназначено для внутри организационного пользования, с хранением и обработкой внутри себя персональных данных сотрудников и курсантов. Хранение персональных данных внутри приложения облегчает их доступность и конфиденциальность, а также исключает возможность потери или порчи в сравнении с хранением бумажных версий в архивах.

“Автолюкс” обеспечивает не только более удобный доступ к информации автошколы, но и обеспечивает ее безопасность и целостность, что играет ключевую роль в обеспечении качественного обучения и сохранении конфиденциальности данных курсантов и сотрудников.

* 1. **Обзор системы автошколы**

Для работы с нашей программой мы должны запустить сперва сервер Рис.1.1, при запуске сервера нас встречает окно с базой данных в котором мы должны прописать данные нашего сервера и базы данных.

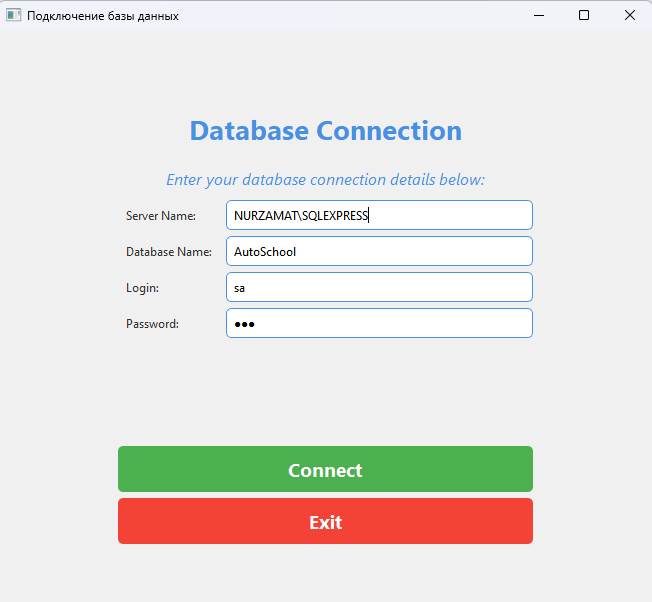


Рис. 1.1. Подключение к базе данных через пользователя “sa”

Далее запускаем клиент при открытии которого нас встречает нас встречает окно авторизации Рис.1.2, и если мы новый пользователь то переходим к окну регистрации, пишем логин и пароль и подключаемся к системе.

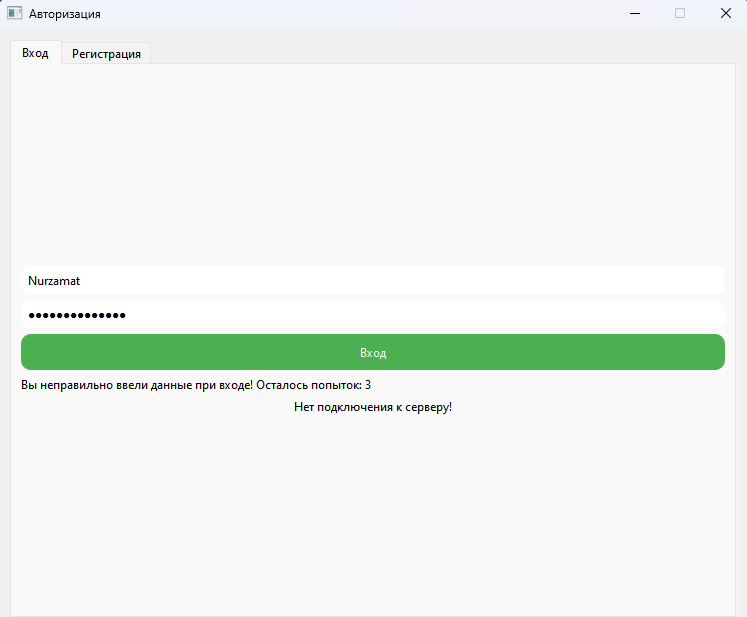


Рис. 1.2. Окно авторизации в систему

При входе в систему нас встречает окно с общедоступными данными (Расписание занятий, учебный материал) Рис.1.3.

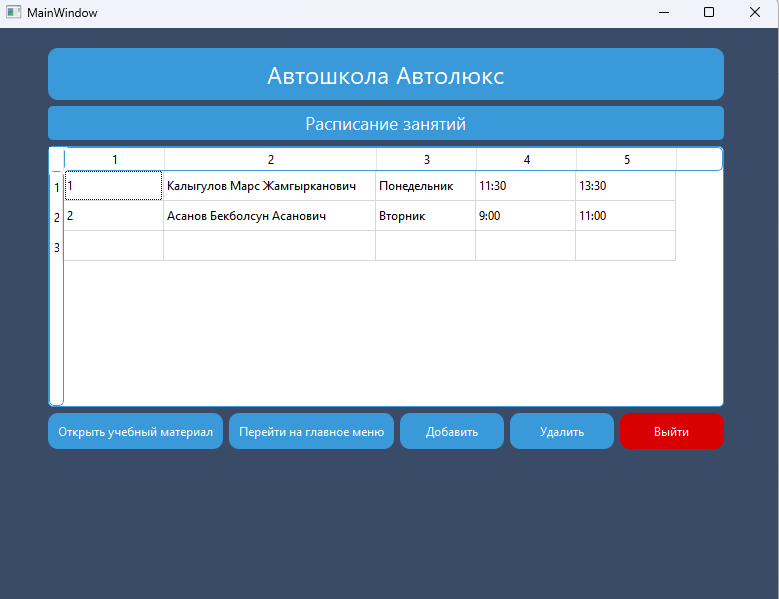


Рис. 1.3. Окно расписания занятий

Окно для просмотра и редактирования данными сотрудников автошколы Рис.1.4.

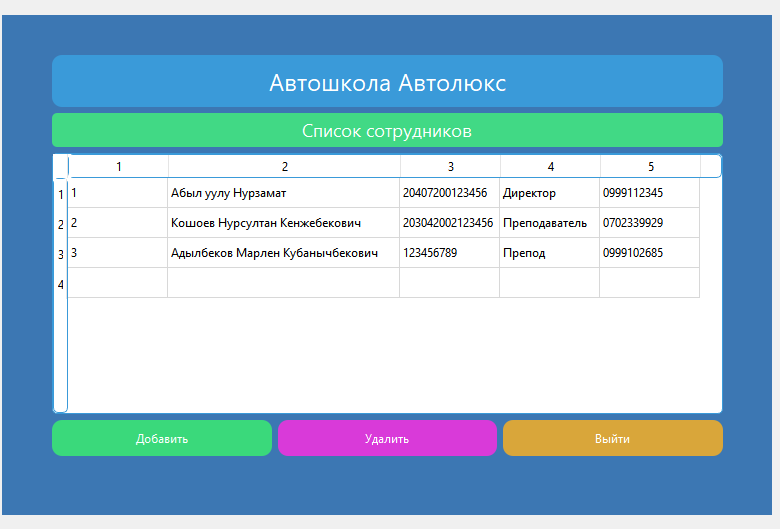


Рис. 1.4. Список сотрудников

На рисунке 1.5 форма заполнения данных сотрудников

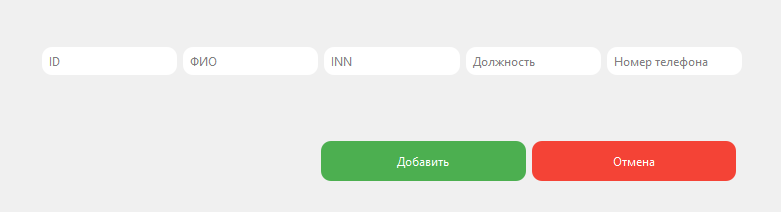


Рис. 1.5. Добавление нового сотрудника

* 1. **Описание процессов**

Таблица 1.1. Процессы

|  |  |  |
| --- | --- | --- |
| **Процесс** | **Актив** | **Среда обработки** |
| Авторизация пользователей | Персональные данные | ПК, Сервер |
| Регистрация пользователей | Персональные данные | ПК, Сервер |
| Добавить группу | Информация ограниченного доступа | ПК, Сервер |
| Добавить курсанта | Информация ограниченного доступа | ПК, Сервер |
| Добавить расписание | Открытый доступ | ПК, Сервер |
| Добавить успеваемости курсантов | Информация ограниченного доступа | ПК, Сервер |
| Справочник по сотрудникам, курсантам | Информация ограниченного доступа | ПК, Сервер |

* 1. **Функциональные требования**

Разрабатываемое клиент-серверное приложение должно выполнять следующие функции:

* Регистрация / Авторизация
* Просмотр справочника сотрудников, курсантов
* Скачивание отчетов
* Введение успеваемости курсантов
* Введение расписания занятий
* Добавление, удаление, обновление групп, курсантов, сотрудников
* Нагрузка преподавателей
  1. **Основные процессы и информационные потоки**

В процессе проведения анализа требований к разрабатываемой системе, была создана модель в виде диаграммы IDEF0 (рис. 1.6.). Данная диаграмма показывает процессы, которые протекают внутри автошколы в ходе выполнения работ, что позволяет более детально рассмотреть проблемы и определить уязвимые места системы.

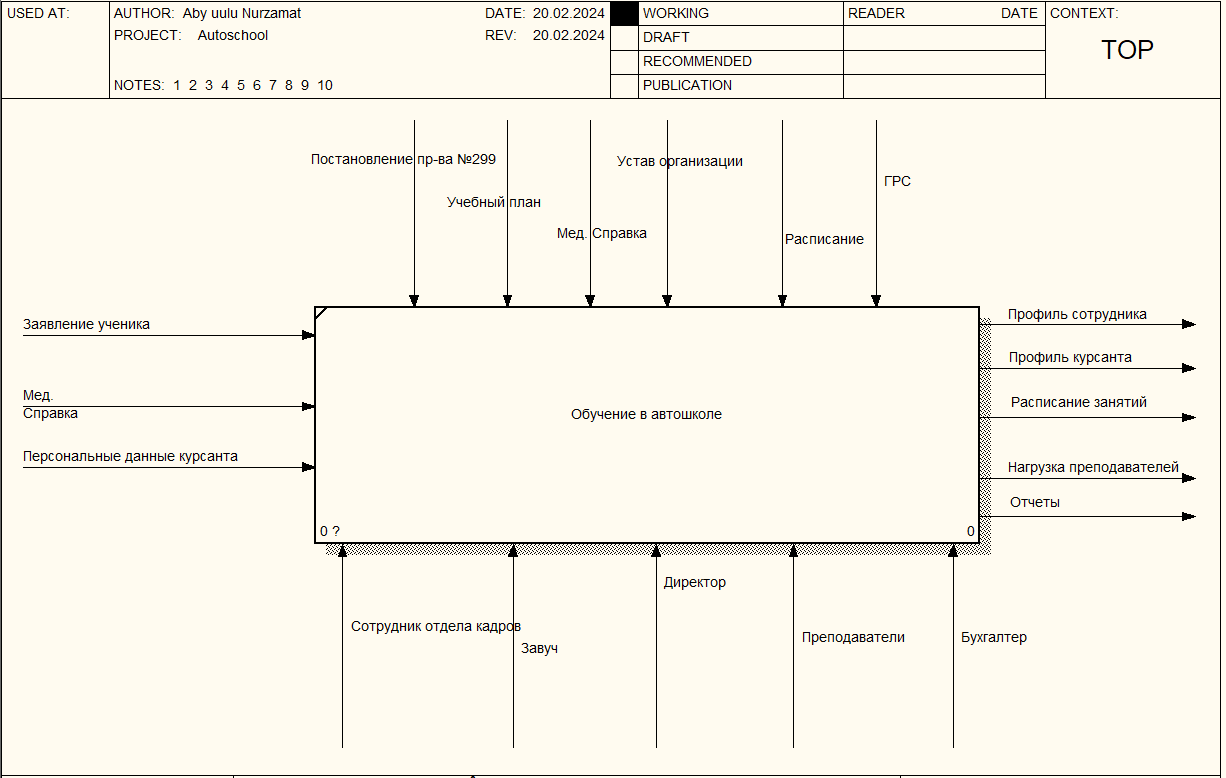
****

Рис. 1.6. Контекстная диаграмма основных процессов автошколы

* 1. **Требования к составу и параметрам технических средств**

Требования к аппаратному обеспечению:

• Тип процессора:

- Процессор x64: AMD Opteron, AMD Athlon 64, Intel Xeon с поддержкой Intel EM64T, Intel.

Pentium IV с поддержкой EM64T.

- Процессор x86: процессор, совместимый с Pentium III или выше.

• Быстродействие процессора: минимум 1,4 ГГц. Рекомендуется 2 ГГц и выше.

• ОЗУ: для обеспечения оптимальной производительности требуется не менее 4 ГБ с последующим увеличением по мере роста размера базы данных.

• Свободного дискового пространства для базы данных – 2 ГБ, так как со временем размер базы данных будет увеличиваться.

## **Требования к системе**

* 1. **Требования к безопасности**

**Подсистема (шифрование данных):**

**Надежность:** Алгоритм шифрования должен быть надежным и стойким к взлому.

**Соответствие стандартам:** Алгоритм шифрования должен соответствовать международным стандартам, таким как AES, ГОСТ 28147-89, RSA.

**Скорость:** Алгоритм шифрования должен работать достаточно быстро, чтобы не влиять на производительность системы.

**Длина ключа:** Длина ключа должна быть достаточно большой, чтобы обеспечить надежную защиту данных.

**Подсистема (идентификация, аутентификация, авторизация):**

**Соответствие стандартам:** Система идентификации должна соответствовать международным стандартам, таким как ISO/IEC 27001, NIST SP 800-63.

**Многофакторная аутентификация:** Должна быть предусмотрена возможность использования многофакторной аутентификации.

**Подсистема (управление доступом):**

**Соответствие стандартам:** Система управления доступом должна соответствовать международным стандартам, таким как ISO/IEC 27001, NIST SP 800-53.

**Гибкость:** Система управления доступом должна быть гибкой и способной адаптироваться к меняющимся потребностям вашей организации.

Обеспечение информационное безопасности Системы должно удовлетворять следующим требованиям:

• Защита Системы должна обеспечиваться комплексом программно-технических средств и поддерживающих их организационных мер.

• Защита Системы должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

• Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики Системы (надежность, быстродействие, возможность изменения конфигурации).

• Разграничение прав доступа пользователей и администраторов Системы должно строиться по принципу, что не разрешено, то запрещено и т.д.

• Система должна обеспечивать обработку конфиденциальной информации.

• Применяемые в системе средства и технологии защиты должны обеспечивать открытость архитектуры и обладать свойствами модульности, масштабируемости и возможности адаптации системы к различным организационным и техническим условиям.

• Система должна обеспечивать необходимую и достаточную защиту ресурсов от характерных угроз безопасности, определенных с учетом объективных факторов и анализа возможных моделей нарушителей.

• Средства защиты, входящие в состав системы, должны иметь развитые средства регистрации критических системных событий в электронных журналах и средства оперативного оповещения об этих событиях администраторов безопасности.

* 1. **Требования к средствам и способам связи для информационного обмена между компонентами системы.**

Для информационного обмена между компонентами системы должна быть организована глобальная сеть.

* Использование стандартных протоколов связи, таких как HTTP/HTTPS, SMTP, FTP/SFTP, LDAP, для обеспечения совместимости и безопасности.
  1. **Требования по диагностированию системы**

Диагностика и профилактика технических средств, проводится раз в месяц. Проверка целостности данных и нарушений проводится по мере необходимости. Проверка программного и аппаратного обеспечения проводится по мере необходимости.

* 1. **Требования к надежности комплекса.**

Надежность аппаратных и программных средств должно обеспечиваться за счет следующих организационных мероприятий:

* использованием в системе технических средств повышенной отказоустойчивости и их структурным резервированием
* защитой технических средств по электропитанию путем использования источников бесперебойного питания
* предварительного обучения пользователей и обслуживающего персонала
* своевременного выполнения процессов администрирования
* соблюдения правил эксплуатации и технического обслуживания программно-аппаратных средств
* своевременное выполнение процедур резервного копирования данных

Надежность программного обеспечения системы должна обеспечиваться за счет:

* проведением комплекса мероприятий отладки, поиска и исключения ошибок
* ведением журналов системных сообщений и ошибок для последующего анализа и изменения конфигурации.

# **ГЛАВА 2. КОНСТРУКТОРСКИЕ РАБОТЫ**

## **Декомпозиция концептуальной модели**

На рисунке 2.1 и 2.2 представлены декомпозиции контекстной диаграммы.

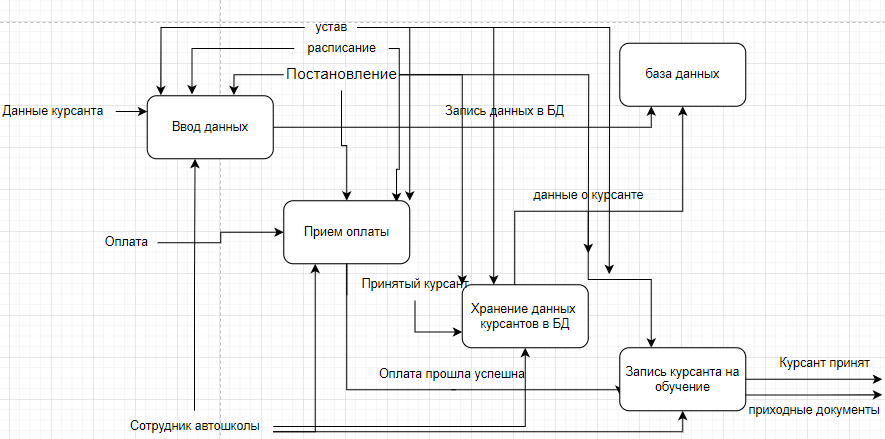


Рис.2.1. Диаграмма: прием новых курсантов



Рис.2.2 Диаграмма: процесс обучения

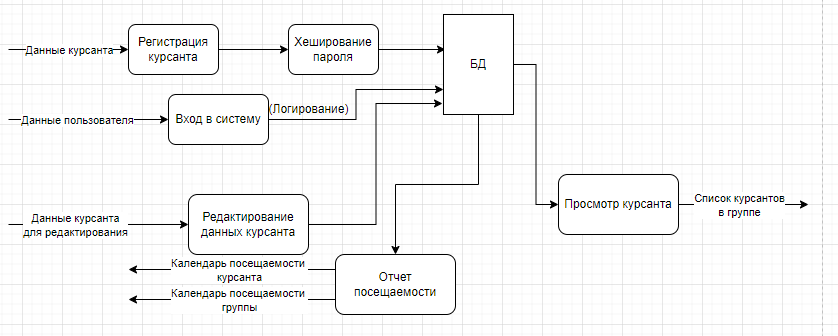


Рис. 2.3. Диаграмма: Регистрация курсанта

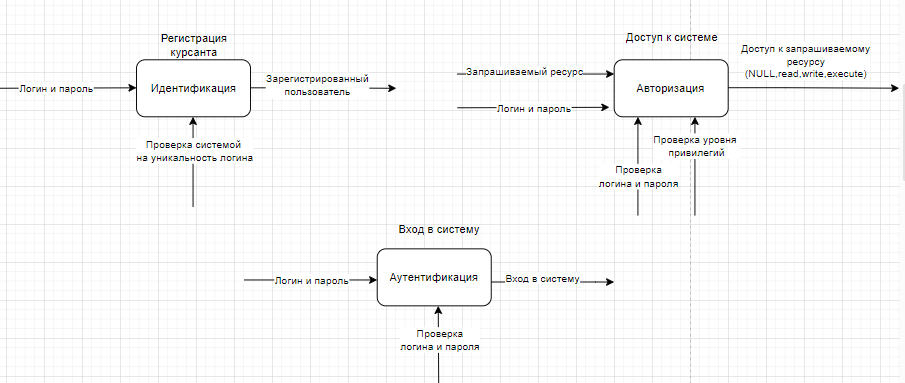


Рис. 2.4. Диаграмма: Идентификации, авторизации и аутентификации в системе

**Описание вариантов использования системы**

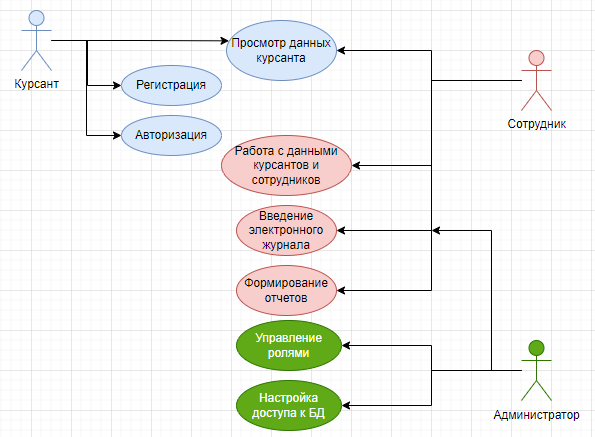


Рис. 2.5. Диаграмма Use Case

## **Организация структуры данных**

Схема «сущность-связь» представляет собой блок-схему, которая иллюстрирует, каким образом различные «сущности» взаимодействуют друг с другом в рамках системы.

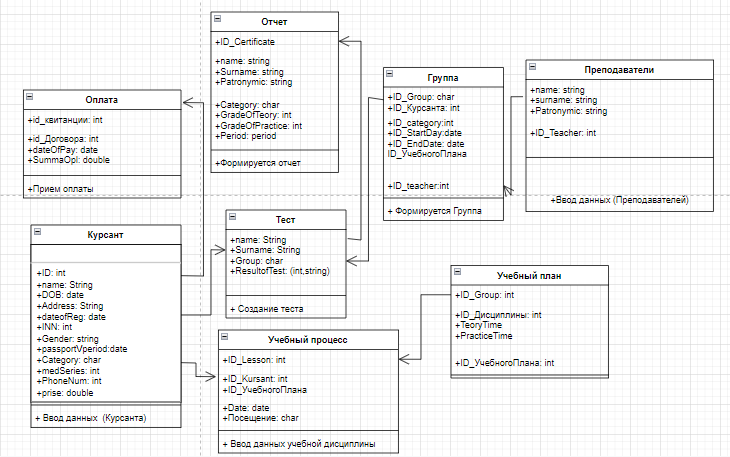


Рис. 2.5. ER - Диаграмма

## **Архитектура разрабатываемой системы**

Архитектура разрабатываемой мною системы основывается на клиент-сервере.

Клиент-серверная архитектура представляет модель взаимодействия между двумя сущностями: клиентом и сервером. Клиент запрашивает ресурсы или услуги, а сервер предоставляет их. Этот подход широко используется в сетевых и веб-приложениях.

**Основные компоненты**

1. **Клиент**:
   * **Описание**: Программное обеспечение или устройство, запрашивающее сервис или ресурсы у сервера.
   * **Примеры**: Веб-браузеры, мобильные приложения, настольные приложения.
   * **Функции**: Посылает запросы серверу и обрабатывает ответы (рендеринг веб-страниц, отображение данных, выполнение вычислений).
2. **Сервер**:
   * **Описание**: Программное обеспечение или устройство, предоставляющее запрашиваемые ресурсы или услуги.
   * **Примеры**: Веб-серверы (Apache, Nginx), серверы баз данных (MySQL, PostgreSQL), файлообменные серверы.
   * **Функции**: Обрабатывает запросы от клиентов, выполняет необходимые вычисления или операции, и возвращает результат клиенту.

**Принцип работы**

1. **Запрос клиента**: Клиент отправляет запрос серверу через сеть. Запрос может быть HTTP-запросом для веб-сервера или SQL-запросом для сервера баз данных.
2. **Обработка сервером**: Сервер принимает запрос, выполняет необходимые действия (например, доступ к базе данных, вычисления, генерация HTML) и формирует ответ.
3. **Ответ сервера**: Сервер отправляет ответ обратно клиенту. Ответ может содержать данные, подтверждение выполнения операции, или страницу HTML.

**Преимущества архитектуры клиент-сервер**

1. **Централизованное управление**:
   * Легко администрировать и обновлять серверное программное обеспечение, так как оно размещено на одном сервере или группе серверов.
2. **Масштабируемость**:
   * Легко масштабировать серверную часть для обработки большего количества запросов, добавляя новые серверы или улучшая существующие.
3. **Безопасность**:
   * Серверы могут централизованно управлять доступом к данным и услугам, обеспечивая безопасность и защиту данных.
4. **Разделение ответственности**:
   * Клиент занимается интерфейсом пользователя и отображением данных, а сервер — обработкой данных и логикой приложения.

**Типы клиент-серверных архитектур**

1. **Одноуровневая**:
   * Клиент напрямую взаимодействует с сервером, который выполняет все задачи.
2. **Многоуровневая (N-tier)**:
   * Логика приложения разделена на несколько уровней (например, презентационный, бизнес-логика и данные). Это улучшает масштабируемость и управляемость.
   * Примеры: Трехуровневая архитектура (клиент, сервер приложений, сервер баз данных).

**Протоколы и технологии**

1. **HTTP/HTTPS**:
   * Применяются для взаимодействия между веб-клиентами и серверами.
2. **RESTful API**:
   * API, использующие стандартные HTTP-методы (GET, POST, PUT, DELETE) для взаимодействия между клиентом и сервером.
3. **WebSocket**:
   * Протокол для двусторонней связи между клиентом и сервером в режиме реального времени.
4. **SOAP**:
   * Протокол для обмена структурированными сообщениями между клиентом и сервером через HTTP.
5. **SQL**:
   * Язык запросов для взаимодействия с сервером базы данных.

**Примеры использования**

1. **Веб-приложения**:
   * Клиент (веб-браузер) отправляет запросы веб-серверу, который возвращает веб-страницы или данные.
2. **Мобильные приложения**:
   * Мобильное приложение (клиент) взаимодействует с сервером для получения и отправки данных.
3. **Desktop приложения:**
   * Настольные приложения или другие клиенты взаимодействуют с серверами баз данных и приложений.

# **ГЛАВА 3. ПРОЕКТИРОВАНИЕ БЕЗОПАСНОСТИ**

## **3.1 Процессы организации**

Основным процессом организации автошколы является автоматизация документооборота, создание единой базы данных. Этот процесс состоит из следующих под-процессов:

* Регистрация
* Авторизация
* Выгрузка расписания занятий
* Распределение нагрузок преподавателей
* Выгрузка отчетов
* Редактирование данных курсантов
* Редактирование данных сотрудников

## **3.2 Инфраструктура клиент-серверного приложения**

Инфраструктура клиент-серверного приложения организации описана в виде функциональной схемы на рисунке 3.1

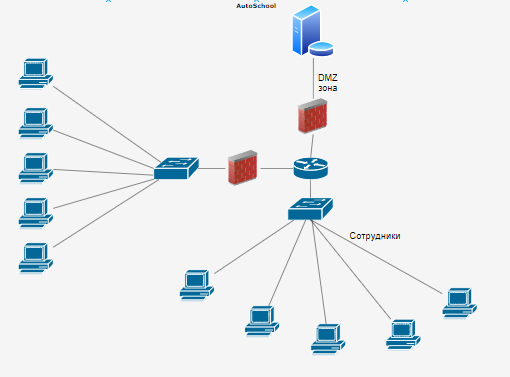


Рис.3.1. Архитектура сети приложения

## **3.3 Идентификация активов**

Согласно ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»

Актив это – все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении.

Информационный актив – знания или данные, которые имеют значение для организации.

К активам организации могут относиться:

* Информационные активы, в том числе различные виды информации, циркулирующие в информационной системе (служебная, управляющая, аналитическая, деловая и т.д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение);
* Ресурсы (финансовые, людские, вычислительные, информационные, телекоммуникационные и прочие);
* Процессы (технологические, информационные и т.д.);

Выделены следующие активы, связанные с автошколой:

1. Информационный актив:
   1. Персональные данные
   2. Данные ограниченного доступа (отчеты, планы, группы, журналы и т.д.)
   3. Данные открытого доступа (учебные материалы и др.)
   4. Аутентификационные данные (логин/пароль)
2. Ресурсы:
   1. Программные:
      1. Операционные системы
      2. Программные обеспечения и файлы
   2. Аппаратные:
      1. Серверы
      2. Персональные компьютеры
      3. Сетевые устройства
   3. Помещения

## **3.4 Модель нарушителя**

Под моделью нарушителя понимаются предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности. Модель нарушителя является важной частью информационной безопасности организации.

Все источники угроз безопасности информации можно разделить на три основные группы:

* Антропогенные источники угроз.
* Техногенные источники угроз.
* Стихийные источники угроз.

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления.

К техногенным источникам угроз относятся угрозы, которые вышли из-под контроля человека и существуют самостоятельно.

К стихийным источникам угроз относятся стихийные бедствия, которые невозможно предусмотреть и предотвратить.

Нарушитель типа «А»

К это й категории нарушителей относятся внутренние сотрудники организации, имеющие право работы с системой, а также имеющие к ней доступ. К ним можно отнести работников учреждения, которые в корыстных целях могут скомпрометировать персональные данные, хранящиеся в базе данных.

Нарушитель типа «Б»

Нарушителями типа «Б», являются компьютерными злоумышленниками (так же хакеры), которые пытаются удаленно получить доступ к системе с целью получения персональных данных от системы, используемых сотрудниками.

Нарушитель типа «В»

К нарушителям типа «В» могут относиться сотрудники организации, имеющие к нему как физический, так и логический доступ. К ним относятся системные администраторы, имеющие право и возможность настраивать параметры передачи данных с помощью системы, модифицировать параметры портов для считывания поступающей информации, имеющие возможность физического извлечения/замены элементов рабочего компьютера сотрудника.

## **3.5 Модель угроз**

Модель угроз ИБ – это описание существующих угроз ИБ, их актуальности, возможности реализации и последствий.

[ГОСТ Р 53114-2008](https://www.wikisec.ru/index.php?title=%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_53114-2008): модель угроз (безопасности информации): Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Модели угроз информационной безопасности позволяют выявить существующие угрозы, разработать эффективные контрмеры, повысив тем самым уровень ИБ, и оптимизировать затраты на защиту (сфокусировав её на актуальных угрозах).

Составление модели угроз является необходимым при решении следующих задач:

* Выбор методов и способов защиты информации, хранящейся в серверах университета и передаваемой по сети;
* Формирование перечня мероприятий, направленных на предотвращение несанкционированного доступа (далее - НСД) к ресурсам внутренних серверов и (или) передачи данных, обрабатываемых в конечных узлах, лицам, не имеющим права доступа к такой информации;
* Предупреждение и предотвращение воздействия на физические компоненты, в результате которого может быть нарушено функционирование;
* Контроль над обеспечением уровня защищенности активов.
* Определение уровня защищенности веб-приложения, формирование перечня мероприятий, направленных на предотвращение несанкционированного доступа к ресурсам веб-приложения

Разработка Модели произведена на основании анализа исходных данных объекта исследования, нормативных и правовых документов органов исполнительной власти с учетом требований по безопасности, предъявляемым к информационным системам.

В модели должны учитываться все актуальные угрозы на всех стадиях их жизненного цикла. У различных информационных систем, а также объектов одной информационной системы может быть разный спектр угроз, определяемый особенностями конкретной информационной системы и её объектов и характером возможных действий источника угрозы.

Под уровнем исходной защищенности ИС понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС. Исходная степень защищенности определяется экспертным путем, а именно:

* 0 – для высокой степени исходной защищенности;
* 5 – для средней степени исходной защищенности;
* 10 – для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показателя, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПД для данной ИС в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

* **маловероятно** – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);
* **низкая вероятность** – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);
* **средняя вероятность** – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПД недостаточны;
* **высокая вероятность** – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПД не приняты.

При составлении перечня актуальных угроз безопасности ПД каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y2, а именно:

* 0 – для маловероятной угрозы;
* 2 – для низкой вероятности угрозы;
* 5 – для средней вероятности угрозы;
* 10 – для высокой вероятности угрозы;

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением:

Y = (Y1 +Y2)/ 20 (Ф-1)

Y1 – числовой коэффициент, определяющий исходную степень защищенности;  
Y2 – числовой коэффициент, определяющий вероятность возникновения угрозы;  
20 – нормирующий коэффициент.

Коэффициент Y1 определяется, исходя из набора технических и эксплуатационных характеристик, общих для всех ИСПД. Коэффициент Y2 определяется на основе экспертной (субъективной) оценки вероятности возникновения угрозы.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

* если 0 <= Y <= 0,3, то возможность реализации угрозы признается низкой;
* если 0,3 <Y <= 0,6, то возможность реализации угрозы признается средней;
* если 0,6 <Y <= 0,8, то возможность реализации угрозы признается высокой;
* если Y> 0,8, то возможность реализации угрозы признается очень высокой;

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИС, в соответствии с правилами, приведенными в таблице 3.1

Таблица 3.1. Правила отнесения угрозы безопасности ПД к актуальной

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность  реализации  угрозы | Показатель опасности угрозы | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | неактуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | Актуальная | актуальная | актуальная |
| Очень высокая | Актуальная | актуальная | актуальная |

Таблица 3.2. Определение актуальных угроз безопасности

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Угроза** | **Уровень защищенности (Y1)** | **Вероятность реализации угрозы (Y2)** | **Коэффициент реализуемости угрозы (Y)** | **Актуальность** |
| Повреждения программных и технических средств | 0 | 2 | 0,1 | неактуальная |
| Получение уровень доступа админа | 0 | 2 | 0,1 | неактуальная |
| Сбои и отказы в обслуживании | 5 | 10 | 0,75 | актуальная |
| SQL-инъекции | 10 | 10 | 1 | актуальная |
| Перехват аутентификационных данных | 10 | 5 | 0,75 | актуальная |
| Обход контроля доступа | 5 | 5 | 0,5 | актуальная |
| Повышение  привилегий | 5 | 10 | 0,75 | актуальная |

**3.6 Способы защиты от вероятных атак**

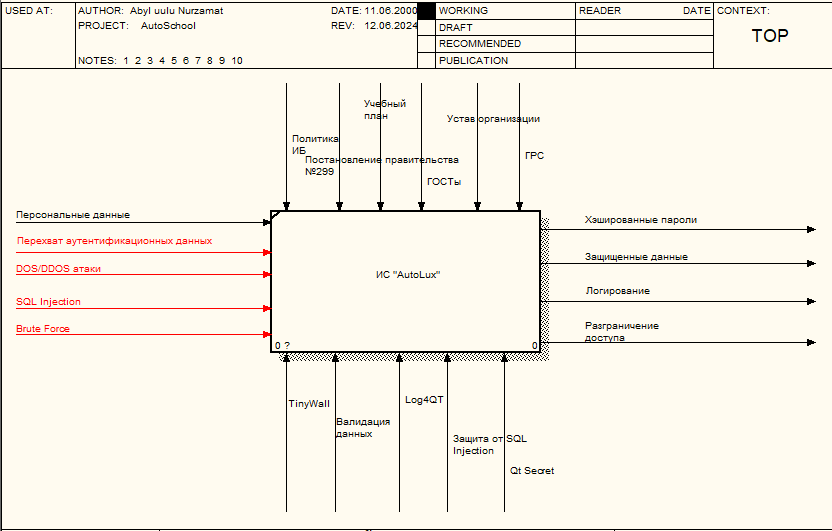


Рис. 3.2 Диаграмма IDEF0

Входные данные:

- Персональные данные

- Угрозы

Управление:

- Политика ИБ

- Модель угроз

- Модель нарушителя

- ГОСТ ИСО/МЭК 27001

- ГОСТ Р 53114-2008

Механизмы:

- Log4Qt

- TinyWall

- модуль QT-Secret

Выходные данные:

- Хэшированные пароли

- Защищенные данные

- Разграничение доступа

- Логирование

### **3.6.1 Log4Qt - Логирование**

Log4Qt - это порт C++ пакета Log4j Apache Software Foundation с использованием Qt Framework. Он предназначен для использования в проектах с открытым исходным кодом и коммерческих проектах Qt.

***Дополнительные возможности:***

* SimpleTimeLayout («дд.ММ.гггг чч:мм Сообщение регистратора уровня [Thread]»)
* ColorConsoleAppender (рендеринг цветного сообщения с помощью escape-последовательности и вывод его на консоль)
* SignalAppender (выдает сигнал при возникновении события журнала)
* DatabaseAppender (добавление события журнала в таблицу sql)
* DatabaseLayout (поместите событие журнала в столбцы таблицы sql)
* Приложение Telnet (добавление событий журнала к клиентам Telnet)
* LogStream (добавление сообщений журнала в стиле qDebug())
* MainThreadAppender (прокси-приложение для отправки сообщений журнала через цикл событий)

Для подключения логгера Log4QT нам нужно сперва добавить заголовочный файл log4qt.pri в наш проект Рис.3.2

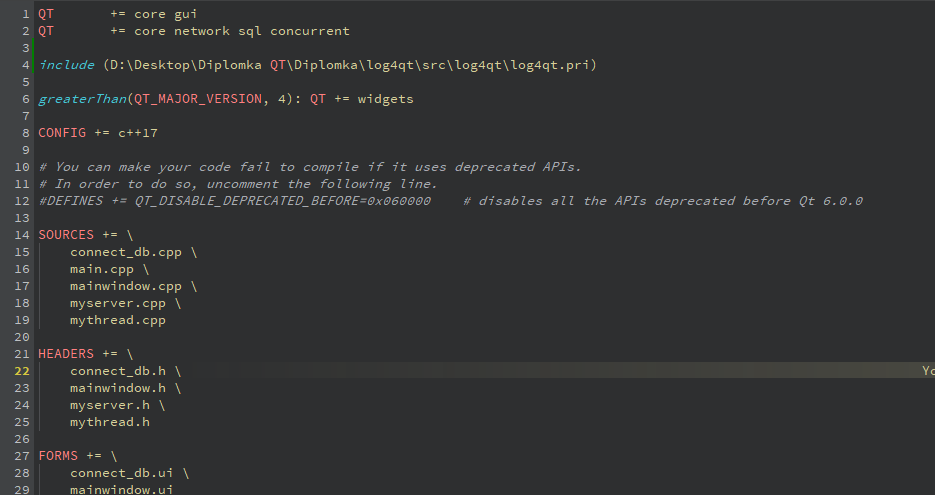


Рис.3.3 Подключение log4qt

Далее подключаем следующие классы:

1. include "log4qt/consoleappender.h"
2. include "log4qt/logger.h"
3. include "log4qt/ttcclayout.h"

Настраиваем регистратор для генерации выходных данных Рис. 3.3



Рис.3.4 Настройка корневого регистратора для примера

### **3.6.2 TinyWall - FireWall**

**TinyWall** - инструмент для повышения уровня сетевой защиты операционной системы.

После установки программа автоматически блокирует все исходящие соединения, кроме нескольких доверенных программ, например, (IE, Firefox и так далее). Если вы хотите выйти в Интернет с помощью приложения, которое не входит в доверенный перечень программ, то связь по умолчанию блокируется без всплывающих окон предупреждений.

Настройка TinyWall на такое поведение - блокировку по умолчанию без предупреждений, является преднамеренным, так как автор программы считает, что когда появляется окно предупреждения Разрешить / Запретить, пользователь чаще нажимает Разрешить. Чтобы разрешить соединение в TinyWall необходимо нажать правой кнопкой мыши на значке программы в трее панели задач, выбрать "В белый список..." и затем выбрать нужную программу из списка. После этого сразу будет доступно исходящее соединение, а утилита TinyWall запомнит ваш выбор.

Для настройки tinywall включаем ее в настройках, добавляем нашу программу в моем случае это сервер и указываем по какому порту она работает.

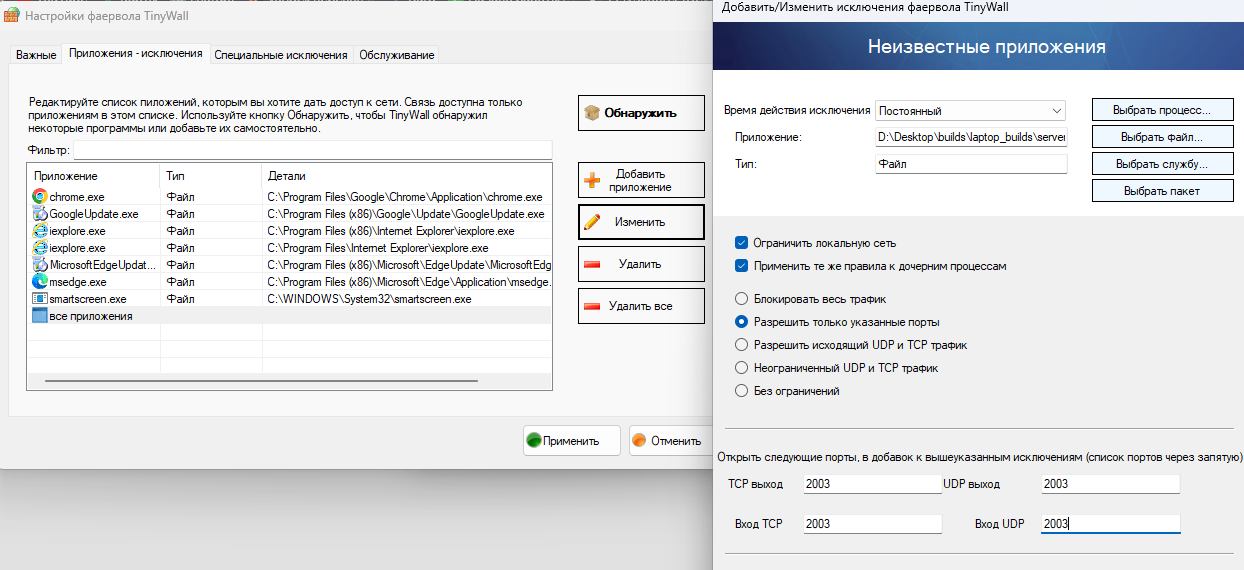


Рис. 3.5 Настройка fire wall

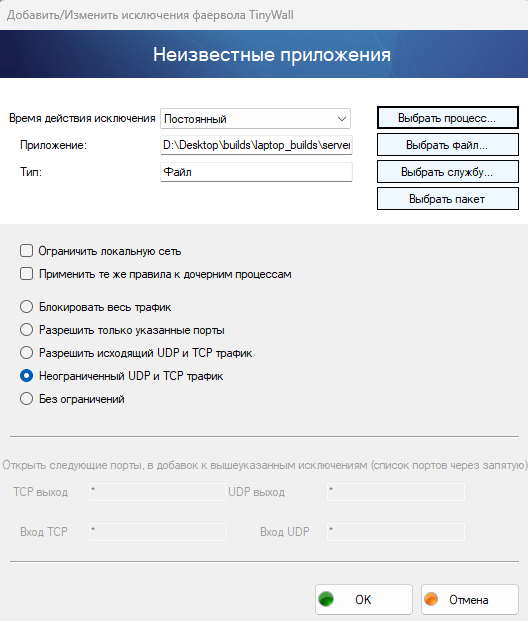


Рис.3.6. Настройка firewall

### **3.6.3 Модуль QT-Secret**

[Qt-Secret](https://github.com/QuasarApp/Qt-Secret)— это библиотека целью которой является обеспечение основных возможностей шифрования, у которых нет в родном Qt. Это алгиритмы RSA и AES.

Ключевая особенность:

* Генерирует пары ключей RSA64 и RSA128 ( а также предполагается поддержка количества номеров до RSA2048)
* Шифрование и дешифрование RSA.
* Подпись и аутентификация сообщения.
* Генерация ключей AES (AES64, AES128, AES256)
* Шифрование и дешифрование AES

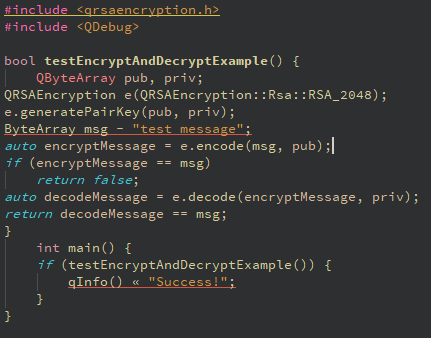
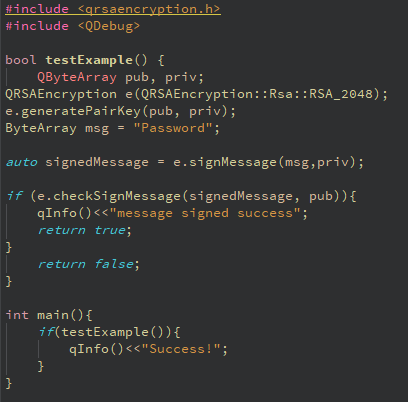
** **

Рис. 3.7 код процесса шифрования

### **3.6.4 RBAC**

Разграничение доступа — это процесс установления и управления уровнями доступа к определённым данным, информации или функциям в системе. Эта мера направлена на защиту данных и предотвращение несанкционированного доступа к конфиденциальной информации или чувствительным данным.

В процессе разграничения доступа обычно назначаются различные уровни привилегий или ролей для пользователей или групп пользователей. Каждый уровень доступа предоставляет определённые права и привилегии, которые определяют, какие действия или операции пользователь может выполнять в системе.

Модель управления доступом на основе ролей (Role-Based Access Control, RBAC) — это подход к управлению доступом, в котором права пользователей определяются их ролями в системе. В RBAC каждому пользователю назначается определённая роль, которая определяет набор разрешений и привилегий, доступных для этой роли. Пользователи получают доступ к ресурсам и функциональности системы в соответствии с назначенной им ролью.

Таблица 3.3. Модель разграничения доступа.

|  |  |  |  |
| --- | --- | --- | --- |
| Субъекты/Объекты | Администратор | Преподаватель | Курсант |
| Пользователи | r, w, e | r | r |
| Форма сотрудников | r, w, e | r, w | r |
| Форма курсантов | r, w, e | r, w | r |
| Учебный материал | r, w, e | r, w | r |
| Расписание | r, w, e | r, w | r |

Обозначения:

* R(read) – чтение объекта
* W(write) – запись объекта
* E(execute) – запись объекта на выполнение

**ГЛАВА 4. РАЗРАБОТКА ДОКУМЕНТАЦИИ**

## **4.1 Описание программы**

Данное разрабатываемое клиент-серверное приложение предназначено для автоматизации процессов автошколы.

В этой системе есть три вида пользователей, это – администратор, преподаватель и сам курсант. Администратор имеет полный доступ к системе

Преподаватель имеет привилегированный доступ к системе, может: создавать группы, редактировать данные сотрудников и курсантов, загрузить расписание занятий, выгрузить отчеты и так далее.

Курсант имеет право только на просмотр расписания занятий и учебных материалов.

## **4.2 Руководство разработчика**

**4.2.1 Назначение и условия применения**

Данное клиент-серверное приложение предназначено для оптимазации работы сотрудников автошколы.

Требования к составу и параметрам технических средств:

* операционная система: Windows, MacOS, Linux;
* процессор: Тактовая частота от 2300 МГц и выше;
* ОЗУ: 8 и выше;
* свободное место на диске: не менее 256 Гб.

**4.2.2 Средства реализации**

В качестве средств реализации клиент-серверного приложения были использованы следующие технологии:

* язык программирования C++;
* фреймворк для создания клиент-серверного приложения QT v6;
* сборщик приложения qmake;
* система управления базами данных: SQL Server Management Studio 20;

**4.2.3 Входные и выходные данные**

Система получает на вход следующие данные:

* данные регистрации;
* запросы на регистрацию;
* данные авторизации;
* запросы на редактирование персональных данных;
* данные сотрудников;
* данные курсантов;
* редактированные персональные данные.

А в качестве выходных:

* список групп;
* список курсантов;
* расписание занятий;
* список пользователей;
* учебный материал;
* список неподтвержденных пользователей на регистрацию;
* список неподтвержденных пользователей на изменение данных;
* информационные сообщения об ошибках.

**ГЛАВА 5. ТЕСТИРОВАНИЕ**

Тестирование информационной системы – это процесс исследования, испытания программного обеспечения для проверки на соответствие между реальным и ожидаемым поведением на конечном наборе тестов.

И в процессе тестирования на отказоустойчивость системы необходимо проделать действия, которые помогут проверить информационную систему в различных сценариях использования, и как следствие установить, степень работоспособности приложения.

## **Брутфорс (brute force)**

Брутфорс (англ. brute force) — это метод атаки на информационную систему, основанный на переборе всех возможных комбинаций паролей или ключей для достижения желаемого результата. Основная идея брутфорса заключается в том, чтобы просто проверять все возможные варианты, пока не будет найден правильный.

В нашем случае при попытке входа в систему перебором паролей, после каждых 3 попыток окно авторизации становится не активной и злоумышленнику придется ждать определенное количество времени, что делает brute force атаку не актуальной.

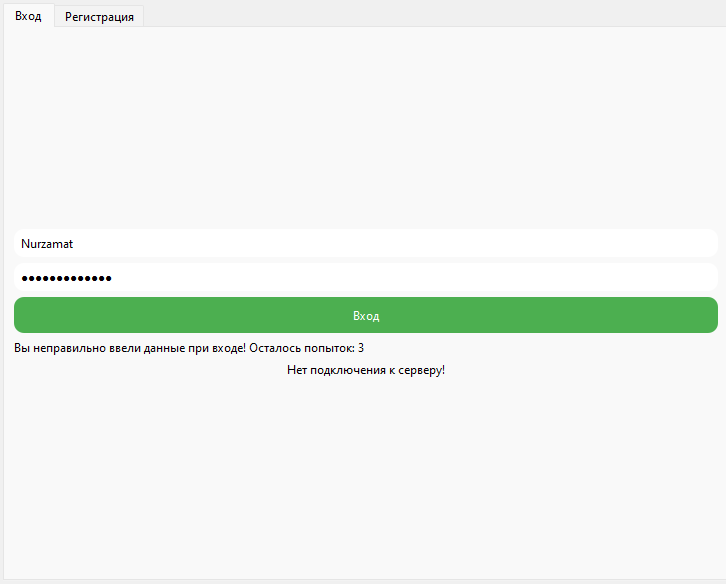


Рис. 5.1 Окно авторизации в систему

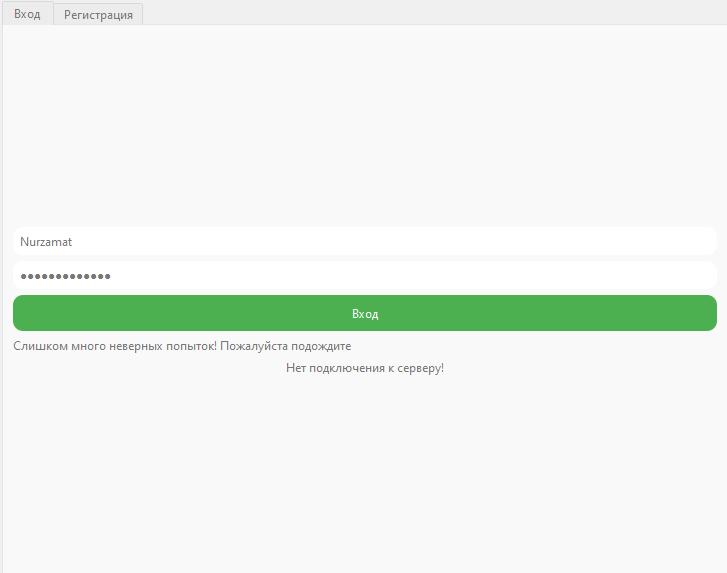


Рис.5.2. Окно авторизации в систему

## **HoneyBot**

Для запуска программы необходимо нажать на панели управления на кнопку старт:

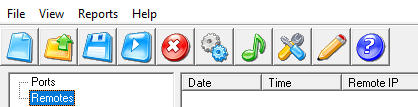


Рис.5.3 Запуск программы

После чего откроется окошко, где нужно будет выбрать IP-адрес хоста:

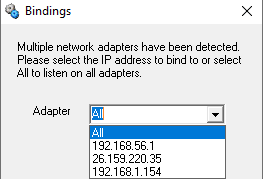


Рис.5.4 Выбор IP-адреса в HoneyBot

В данном случае это 192.168.1.154. В качестве злоумышленника выберем Kali и попробуем просканировать жертву командой Nmap:

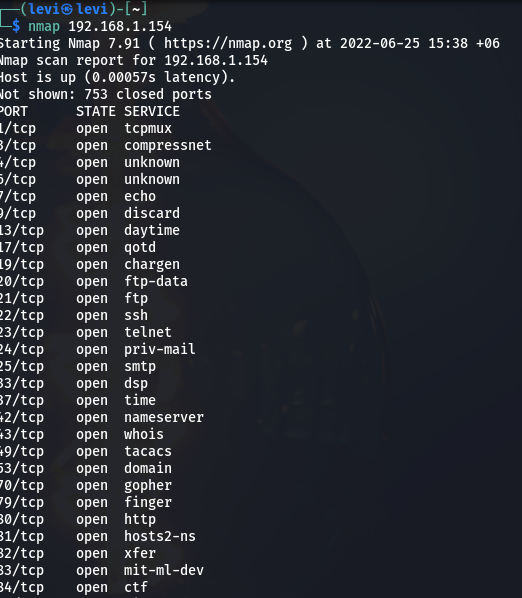


Рис.5.5 Вывод утилиты Nmap

Как можно заметить, на экран злоумышленника вывелось огромное количество различных открытых портов. Их открыл HoneyBot, чтобы запутать атакующего. И это же можно увидеть в программе жертвы:

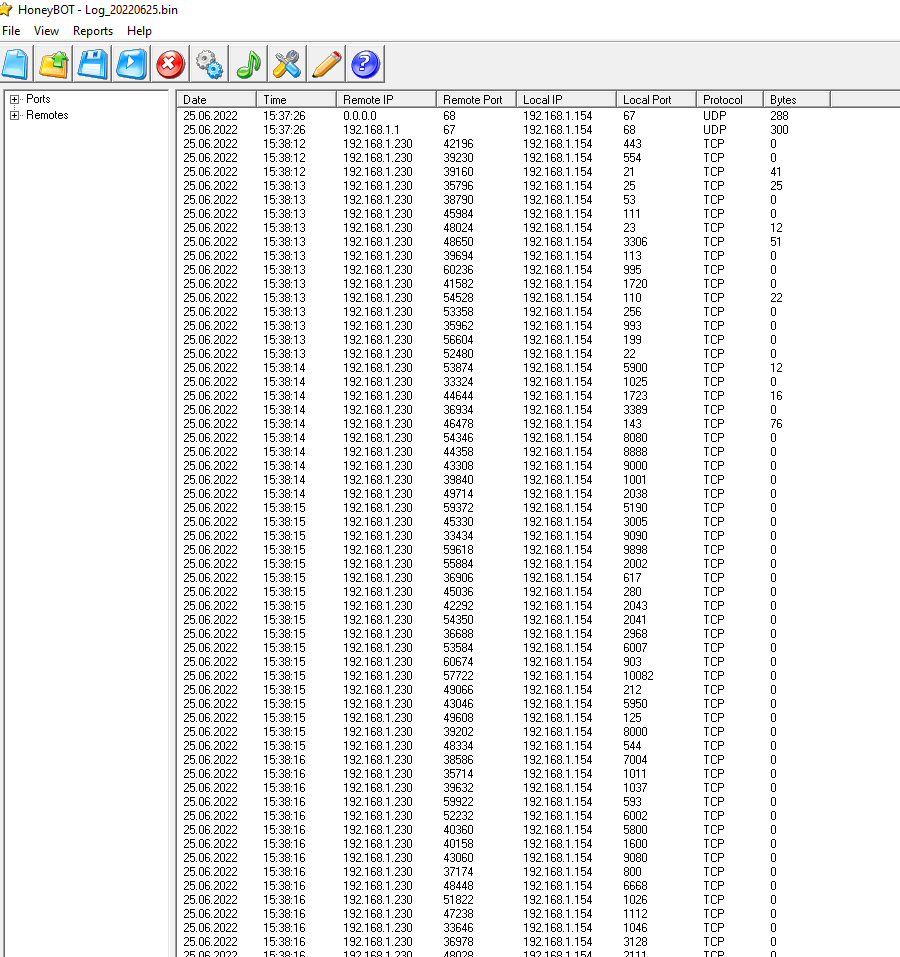


Рис.5.6 Работа программы HoneyBot

Попробуем теперь подключиться по SSH через программу putty:

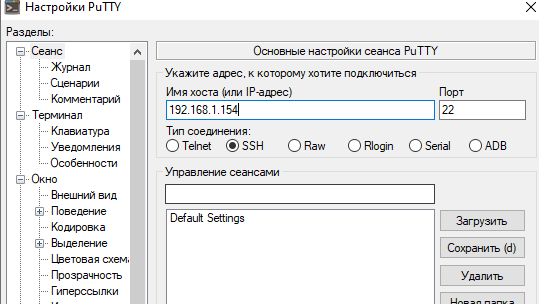


Рис.5.7 SSH подключение через putty

И вот, что выдаст программа:

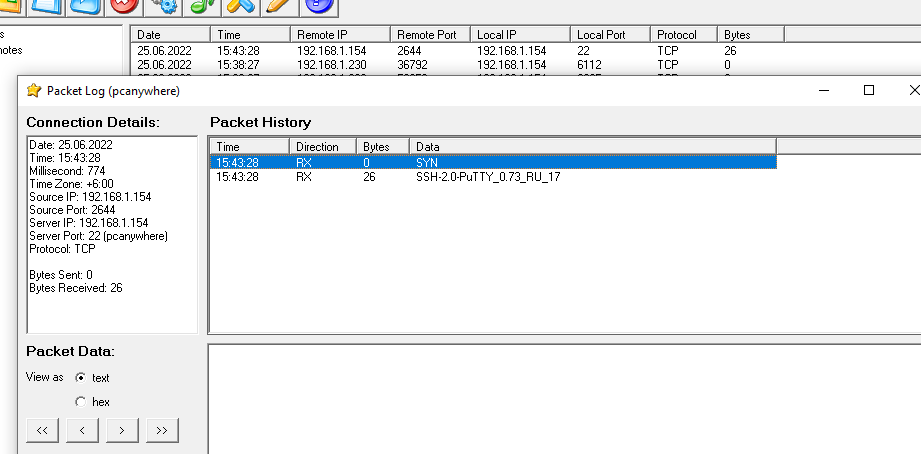


Рис. 5.8 Детали SSH подключения в HoneyBot

## **Dos/ddos**

DoS (Denial of Service) и DDoS (Distributed Denial of Service) атаки — это типы кибератак, направленные на вывод из строя компьютеров, сетевых устройств или целых сетевых инфраструктур, делая их недоступными для законных пользователей. Различие между ними заключается в масштабе и методах атаки.

DoS атака — это атака, в которой один злоумышленник использует один компьютер и одно интернет-соединение для отправки большого количества запросов на сервер, цель которого — исчерпать ресурсы системы и сделать её недоступной для законных пользователей.

DDoS атака — это более сложная форма DoS атаки, в которой множество скомпрометированных компьютеров (ботнет) участвуют в атаке одновременно. Эти компьютеры могут находиться по всему миру и управляются центральным контроллером, называемым бот-мастером.

**hping3** — это мощный инструмент для генерации и анализа TCP/IP пакетов, который может использоваться для тестирования сети

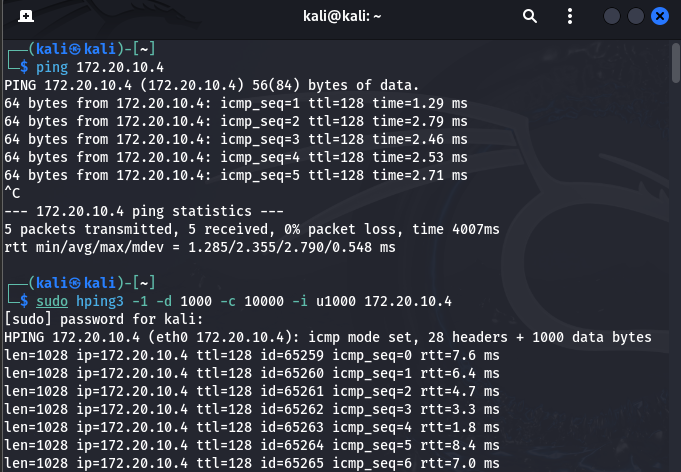


Рис. 5.9 Команда для отправки пакета, отправленные пакеты

-1 указывает использование ICMP (ping).

-d задает размер пакета.

-c указывает количество пакетов.

-i задает интервал между пакетами.

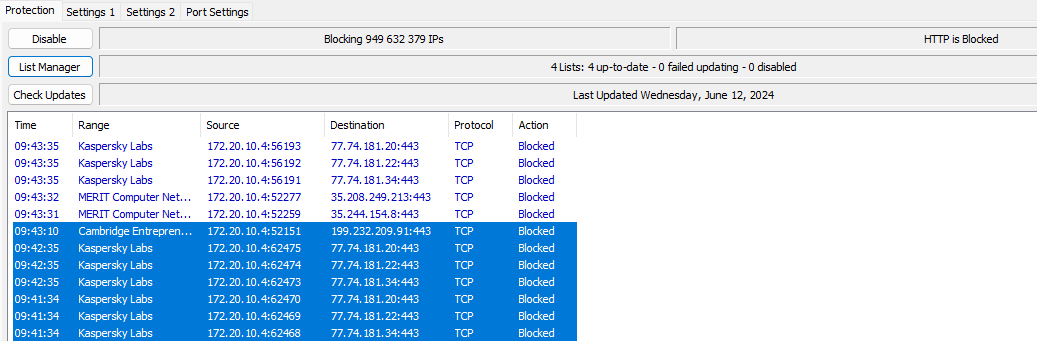


Рис. 5.10 Блокирование пакетов

**ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

БД База данных  
ИА Информационный актив

ПА Программный актив  
ИБ Информационная безопасность  
ИС Информационная система  
ИТ Информационные технологии  
НСД Несанкционированный доступ  
ОЗУ Оперативное запоминающее устройство  
ОС Операционная система  
ПК ПК  
ПО Программное обеспечение  
ПДн Персональные данные  
СВР угроз ИБ СЗПДн Степень возможности реализации угроз ИБ

СЗПД Система защиты персональных данных

СКЗ Средство криптографической защиты информации

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ**

1. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – Москва: Стандартинформ, 2008. - 20 с.

2. ГОСТ Р 53131–2008. Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения. – Москва: Стандартинформ, 2008. - 53 с.

3. ГОСТ Р ИСО/МЭК 17999–2005. Информационная технология. Практические правила управления информационной безопасностью. – Стандартинформ, 2006. - 62 с.

4. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – Москва: Стандартинформ, 2009. – 50 с.

5. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. – Москва: Стандартинформ, 2007. – 22 с.

6. ГОСТ Р 52863-2007. Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования. – Стандартинформ, 2020. – 40 с.

7. <https://www.qt.io/>

8. <https://www.kaspersky.ru/resource-center/threats/what-is-a-honeypot>

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.

Одной из ключевых задач, решаемых в данном проекте, было обеспечение информационной безопасности системы. В рамках проекта были реализованы следующие меры защиты:

1. **Аутентификация и авторизация пользователей**: внедрена система разграничения доступа на основе ролей (RBAC), что позволяет предоставлять различные уровни доступа к функциям и данным системы в зависимости от роли пользователя.
2. **Шифрование данных**: использованы современные алгоритмы шифрования для защиты данных, передаваемых между клиентом и сервером, что позволяет предотвратить их перехват и несанкционированное использование.
3. **Безопасное хранение данных**: внедрены механизмы защиты данных, хранимых в базе данных, включая шифрование критически важных данных.
4. **Защита от угроз**: реализованы меры по предотвращению атак типа SQL-инъекций, что значительно повышает общую безопасность системы.

Разработанное клиент-серверное приложение соответствует современным требованиям к информационной безопасности и предоставляет удобные инструменты для управления процессами автошколы. Данный проект демонстрирует возможность создания эффективных и безопасных систем, которые могут быть успешно интегрированы в деятельность учебных учреждений. Внедрение такой системы позволит автошколам улучшить качество обучения, обеспечить надежную защиту данных и повысить общую эффективность работы.

# **ПРИЛОЖЕНИЯ**

ПРИЛОЖЕНИЕ А

**Идентификация активов**

Таблица 1. П-А. 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 (ПA)  MS Office 2019 16.0 (ПA) | QT V6 (ПА) | Д,Ц,К | CVE-2019-11137 |
| Обработка информации | База данных (ИА-3) | Microsoft SQL Server 2019 (RTM) 15.0.2000.5 Enterprise Edition | Ц,Д,К | CVE-2022-34006 |

Продолжение таблицы 1. П-А. Идентификация активов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 (ПA) | QT V6 (ПА) | Ц,Д,К | CVE-2022-23298 |
| Отчет | 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 (ПA) | QT V6 (ПА) | Ц,Д,К | CVE-2022-23298 |

ПРИЛОЖЕНИЕ Б

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Таблица 2.П-Б. 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 2. П-Б. 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 2. П-Б. 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 |
| Антропогенный,  Тип В  (Уволенные сотрудники) | Внутренний нарушитель | Доступ по  протоколу IP к  интернет-шлюзу  со стороны  интернет-сети | Корыстный умысел, месть, вандализм | Владение  информацией об  аппаратном и  программном  оснащении  компьютера | Компрометация  данных,  передаваемых  посредством  интернета | Копирование/перемещение информации,  представляющей  ценность для  организации на  внешний носитель |

ПРИЛОЖЕНИЕ В

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Таблица 3.П-В. 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 |

Таблица 3.П-В. 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 3.П-В. 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 |