# **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

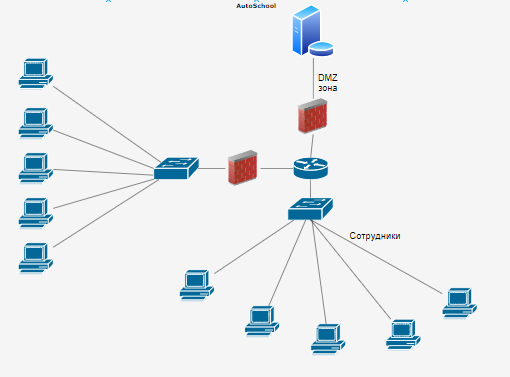


Рис.3.1. Архитектура сети приложения

## **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**

Модель нарушителя описывает возможности потенциального нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

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.

Составление модели угроз является необходимым при решении следующих задач:

* Выбор методов и способов защиты информации, хранящейся в серверах автошколы 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 клиент-серверного приложения, формирование перечня мероприятий, направленных на предотвращение несанкционированного доступа к ресурсам клиент-серверного 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 разные угрозы, которые определяются особенностями каждой информационной системы и её объектов.

Под уровнем защищенности ИС понимается показатель, который зависит от технических и эксплуатационных характеристик ИС. Также 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 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, из набора технических средств и характеристик эксплуатаций. Коэффициент Y2 определяется посредством экспертной т.е. субъектной 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**

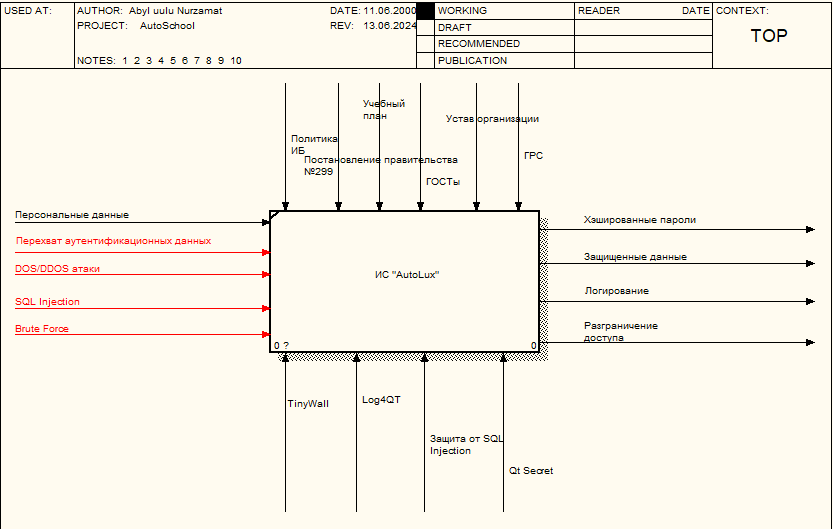


Рис. 3.2 Диаграмма IDEF0

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

- Защита от SQL Injection

Выходные данные:

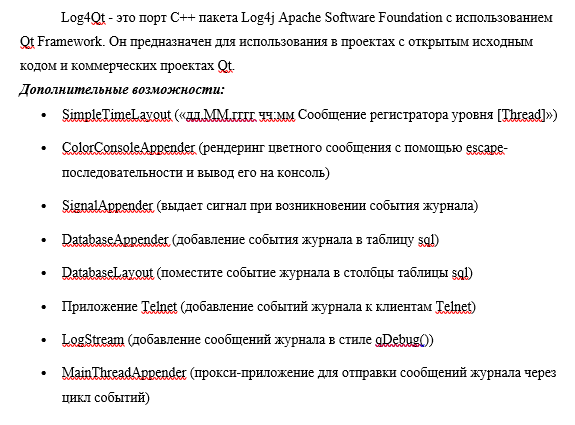
- Хэшированные пароли

- Защищенные данные

- Разграничение доступа

- Логирование

### **3.6.1 Log4Qt - Логирование**



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

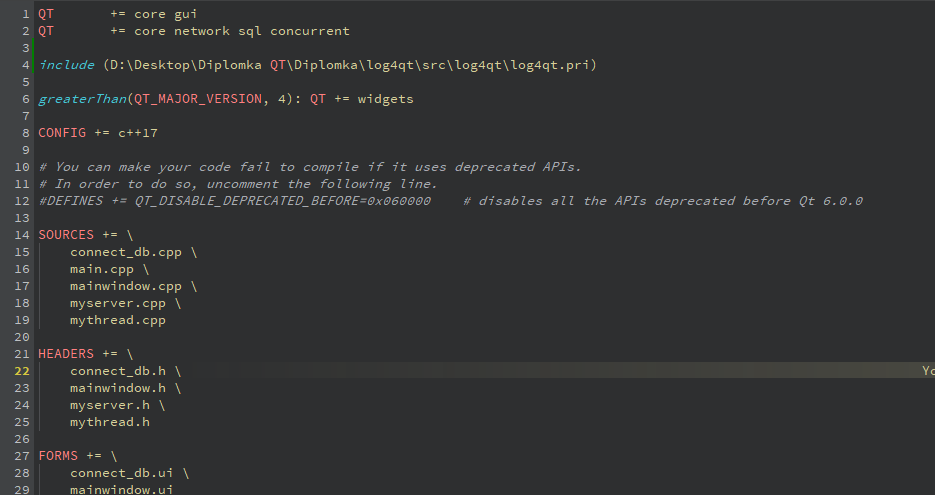


Рис.3.3 Подключение log4qt

Далее подключаем следующие классы:

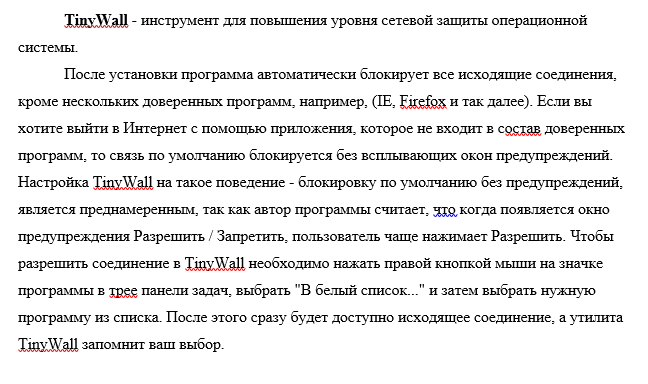
1. include "log4qt/consoleappender.h"
2. include "log4qt/logger.h"
3. include "log4qt/ttcclayout.h"

Настраиваем регистратор для генерации выходных данных Рис. 3.3



Рис.3.4 Настройка корневого регистратора для примера

### **3.6.2 TinyWall - FireWall**

****

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

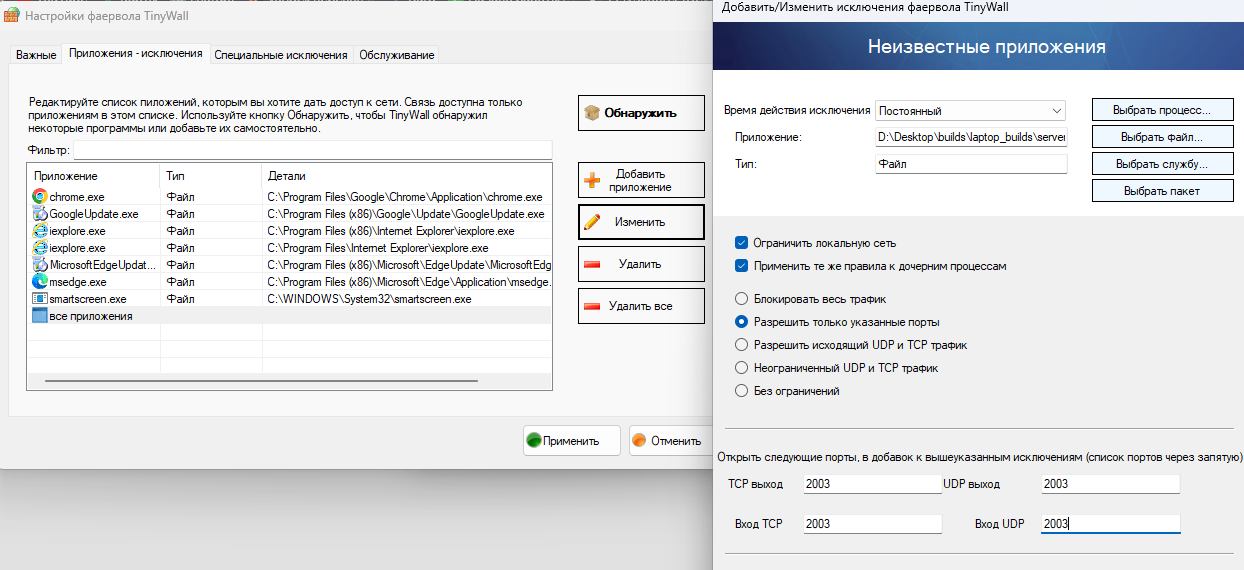


Рис. 3.5 Настройка fire wall

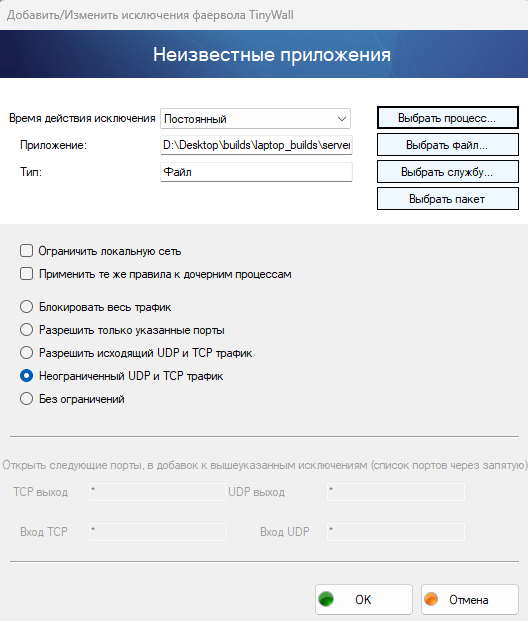


Рис.3.6. Настройка firewall

### **3.6.3 Модуль QT-Secret**

[Qt-Secret](https://github.com/QuasarApp/Qt-Secret)— это библиотека с помощью которой я шифрую данные с алгоритмами, у которых нет в родном Qt. Это алгиритмы RSA и AES.

Ключевая особенность QT-Secret:

* Генерирует пары ключей RSA64 и RSA128
* Шифрование и дешифрование RSA.
* Подпись и аутентификация сообщения.
* Генерация ключей AES (AES64, AES128, AES256)
* Шифрование и дешифрование AES

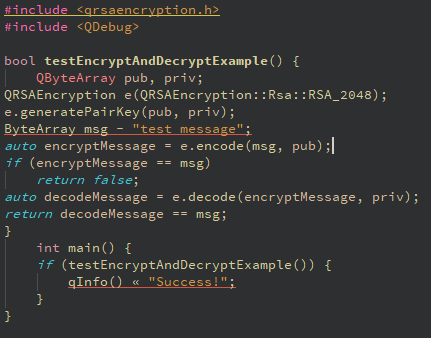
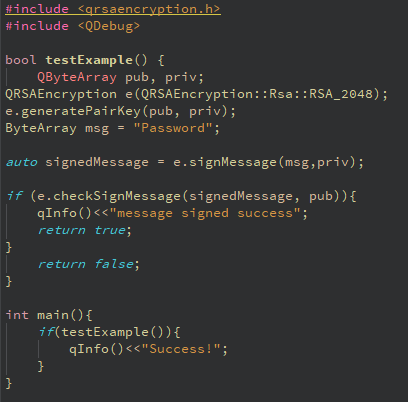
** **

Рис. 3.7 код процесса шифрования

### **3.6.4 RBAC**

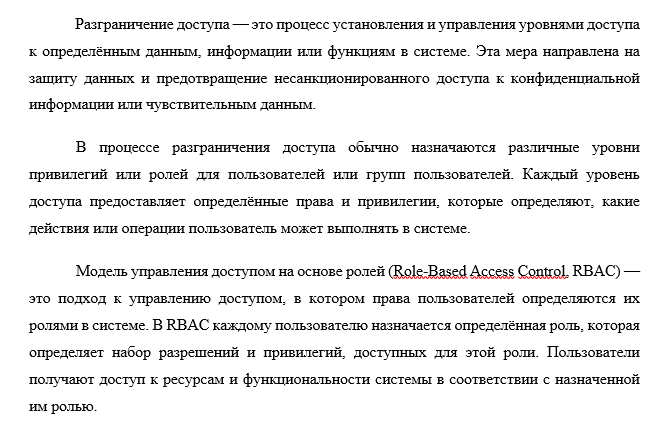


Таблица 3.3. Модель разграничения доступа.

|  |  |  |  |
| --- | --- | --- | --- |
| 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