**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ**

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

**КАФЕДРА «ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КОМПЬЮТЕРНЫХ СИСТЕМ»**

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

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

**По направлению 590100 «Информационная безопасность»**

**Выполнил:** Абыл уулу Нурзамат

**Группа:** ИБ(б)-1-20

**Руководитель:** доцент Вагнер Андрей Арнович

Бишкек 2024

**Содержание**

[**Введение** 3](#_Toc162345215)

[**Актуальность работы** 4](#_Toc162345216)

[**Цель** 5](#_Toc162345217)

[**Задачи** 5](#_Toc162345218)

[**ГЛАВА 1. Анализ и разработка требований** 6](#_Toc162345219)

[**1.1** **Общая характеристика объекта защиты** 6](#_Toc162345220)

[**1.2** **Обоснование для разработки** 6](#_Toc162345221)

[**1.3** **Описание процессов** 6](#_Toc162345222)

[**1.4** **Функциональные требования** 7](#_Toc162345223)

[**1.5** **Основные процессы и информационные потоки** 7](#_Toc162345224)

[**1.6** **Требования к составу и параметрам технических средств** 8](#_Toc162345225)

[**Требования к системе** 9](#_Toc162345226)

[**1.7** **Требования к безопасности** 9](#_Toc162345227)

[**1.8** **Требования к средствам и способам связи для информационного обмена между компонентами системы.** 10](#_Toc162345228)

[**1.9** **Требования по диагностированию системы** 10](#_Toc162345229)

[**1.10** **Требования к надежности комплекса.** 10](#_Toc162345230)

[**1.11** **Требования по стандартизации и унификации** 11](#_Toc162345231)

[**ГЛАВА 2. Конструкторские работы** 11](#_Toc162345232)

[**2.1** **Декомпозиция концептуальной модели** 11](#_Toc162345233)

[**2.2** **Организация структуры данных** 14](#_Toc162345234)

[**2.3** **Архитектура разрабатываемой системы** 15](#_Toc162345235)

[**ГЛАВА 3. Проектирование безопасности** 17](#_Toc162345236)

[**3.1 Процессы организации** 17](#_Toc162345237)

[**3.2 Инфраструктура клиент-серверного приложения** 17](#_Toc162345238)

[**3.3 Идентификация активов** 18](#_Toc162345239)

[**3.4 Модель нарушителя** 19](#_Toc162345240)

[**3.5 Модель угроз** 20](#_Toc162345241)

[**3.6** **Способы защиты от вероятных атак** 24](#_Toc162345242)

[**3.6.1 Log4Qt - Логирование** 25](#_Toc162345243)

[**3.6.2 TinyWall - FireWall** 26](#_Toc162345244)

[**3.6.3 Модуль QT-Secret** 26](#_Toc162345245)

[ПРИЛОЖЕНИЕ А 27](#_Toc162345246)

[**Идентификация активов** 28](#_Toc162345247)

[ПРИЛОЖЕНИЕ Б 29](#_Toc162345248)

[**Модель нарушителя** 30](#_Toc162345249)

[ПРИЛОЖЕНИЕ В 32](#_Toc162345250)

[**Модель угроз** 33](#_Toc162345251)

**Введение**

В современном мире информационных технологий клиент-серверные приложения стали неотъемлемой частью многих сфер деятельности, включая образование. В частности, автошколы активно внедряют технологии для улучшения своей эффективности и качества обучения. Разработка и обеспечение безопасности клиент-серверного приложения автошколы - это сложная задача, требующая внимания к различным аспектам, начиная от функциональности и удобства использования и заканчивая надежностью и защитой от потенциальных угроз.

Одним из ключевых аспектов разработки такого приложения является создание интуитивно понятного интерфейса как для инструкторов, так и для курсантов. Удобство использования приложения играет важную роль в его успешной реализации и принятии пользователями. Это включает в себя функциональность для записи на занятия, отслеживания прогресса, доступа к учебным материалам и другим аспектам обучения.

Следующим важным аспектом является обеспечение безопасности данных. 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.

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. Онлайн-платформы для автошкол могут значительно улучшить процесс обучения, предоставляя студентам и инструкторам эффективные инструменты для взаимодействия и обмена информацией.

Начало формы

# **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++, а серверная часть разработано на этом же фреймворке, только создается как консольное приложение без визуального интерфейса. Хранение базы данных производится на СУБД SQL Server.

* 1. **Обоснование для разработки**

Разработанное клиент-серверное приложение для автошколы призвано 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.

* 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. 1.1.). Данная диаграмма показывает процессы, которые протекают внутри автошколы в ходе выполнения работ, что позволяет более детально рассмотреть проблемы и определить уязвимые места системы.

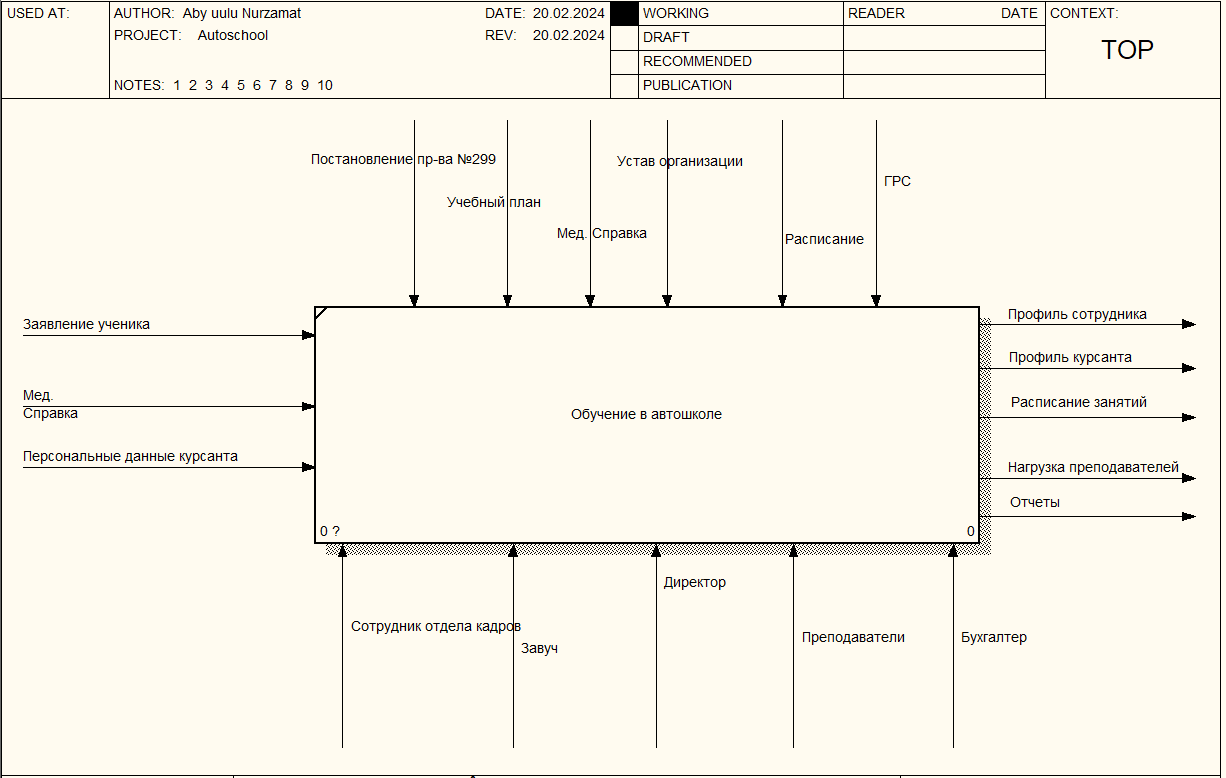
****

Рис. 1.1. 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.
  1. **Требования по стандартизации и унификации**

В требования к стандартизации и унификации включают: показатели, устанавливающие требуемую степень использования стандартных, унифицированных методов реализации функций (задач) системы, поставляемых программных средств, типовых математических методов и моделей, типовых проектных решений, унифицированных форм управленческих документов, установленных ГОСТ 6.10.1, общесоюзных классификаторов технико-экономической информации и классификаторов других категорий в соответствии с областью их применения, требования к использованию типовых автоматизированных рабочих мест, компонентов и комплексов.

# **ГЛАВА 2. Конструкторские работы**

## **Декомпозиция концептуальной модели**

На рисунке 2.1 и 2.2 представлены декомпозиции контекстной диаграммы.

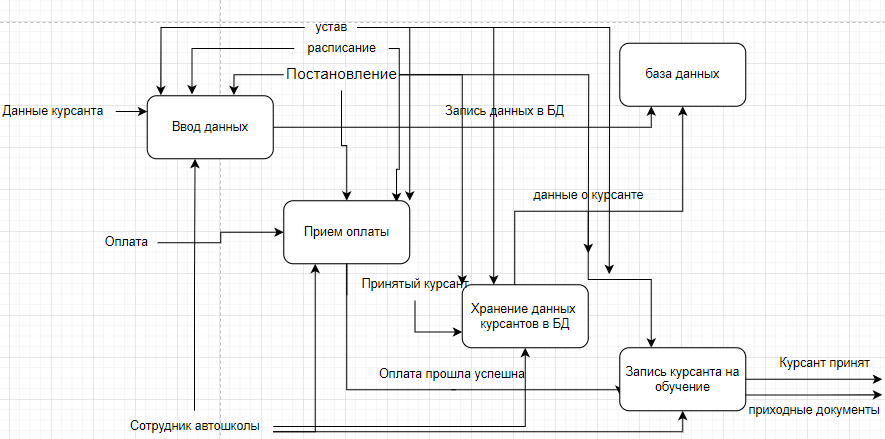


Рис.2.1. Диаграмма: прием новых курсантов



Рис.2.2 Диаграмма: процесс обучения

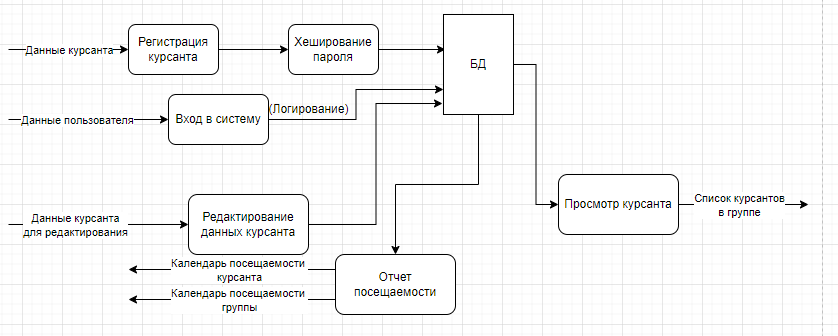


Рис. 2.3. Диаграмма: Регистрация курсанта

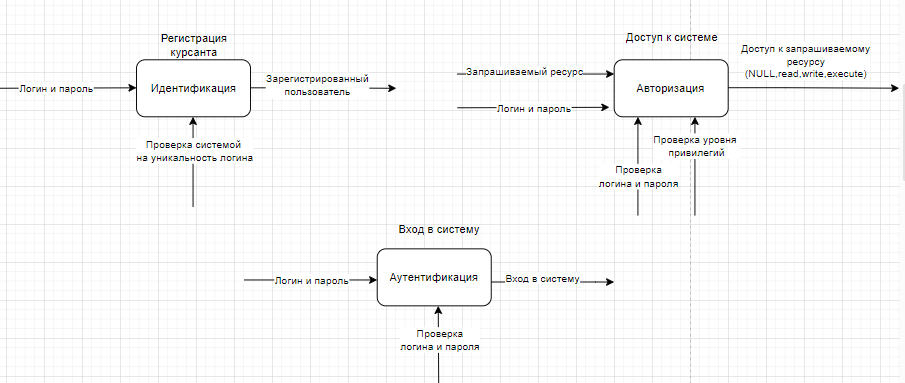


Рис. 2.4. Диаграмма: Идентификации, авторизации и аутентификации в системе

**Описание вариантов использования системы**

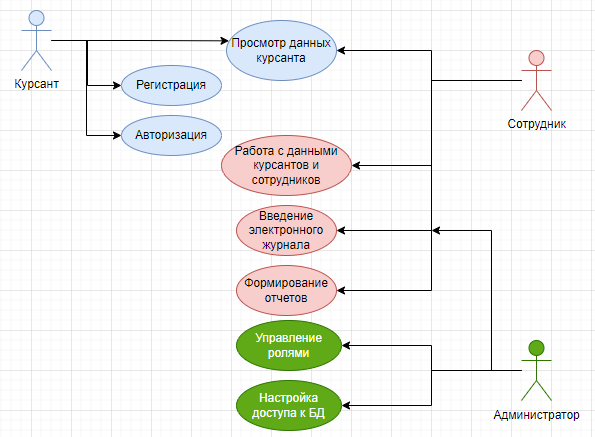


Рис. 2.5. Диаграмма Use Case

## **Организация структуры данных**

Схема «сущность-связь» (также ERD или ER-диаграмма) — это разновидность блок- схемы, где показано, как разные «сущности» (люди, объекты, концепции и так далее) связаны между собой внутри системы. ER-диаграммы чаще всего применяются для проектирования и отладки реляционных баз данных в сфере образования, исследования и разработки программного обеспечения и информационных систем. ER- диаграммы (или ER-модели) полагаются на стандартный набор символов, включая прямоугольники, ромбы, овалы и соединительные линии, для отображения сущностей, их атрибутов и связей. Эти диаграммы устроены по тому же принципу, что и грамматические структуры: сущности выполняют роль существительных, а связи — глаголов.

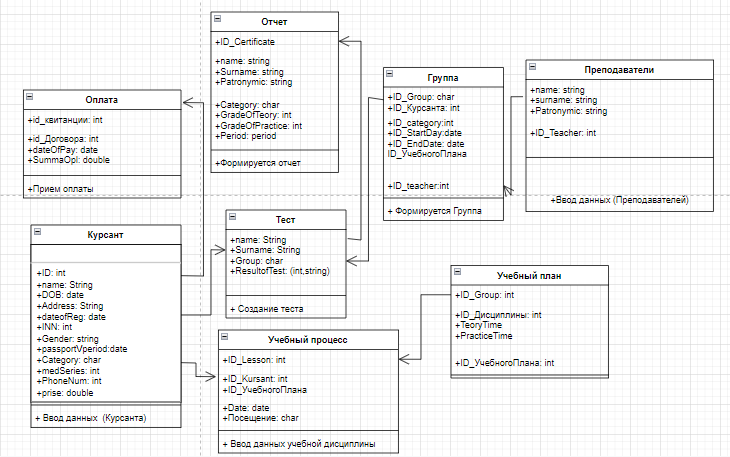


Рис. 2.5. ER - Диаграмма

## **Архитектура разрабатываемой системы**

Архитектура разрабатываемой системы основывается на монолитной.

Выражение «монолитная архитектура» сразу ассоциируется со словом «монолит». А монолитом еще с давних пор называют большой единый блок из камня или бетона. Монолит — это что-то большое и единое, имеющее общую и мощную структуру.

В программировании «монолитная архитектура» также подразумевает наличие общей и единой платформы, где сконцентрированы все компоненты одной программы. Сколько бы ни насчитывалось подобных компонентов, все они унифицированы и при этом управляются из одного места. В этом и определяется сила «монолитных» приложений.

Многие современные стартапы выбирают именно монолитную архитектуру приложения, потому что она комфортна при работе небольшими группами разработчиков. При ее использовании все компоненты программы взаимосвязываются и взаимозаменяются — это помогает развивать программу автономной и самодостаточной. Монолитная архитектура считается традиционной и проверенной при разработке приложений.

Монолитная архитектура хоть и «старая» по своему происхождению, но до сих пор актуальна и используется многими компаниями, так как идеально подходит для небольших стартапов и разработок, а также удовлетворяет следующим задачам:

* когда нужно быстро развернуть небольшое приложение;
* если в команде разработчиков небольшое количество людей (2-5), которые смогут работать совместно, а также смогут вместе поддерживать приложение в дальнейшем;
* когда создается непроверенный продукт и нужно его быстро создать, чтобы протестировать;
* когда просто нет опыта работы с микросервисами;
* если изначально известно, что приложение не будет разрастаться до колоссальных масштабов;
* если в приоритете разработки программного обеспечения находятся именно скорость его работы и производительность.

Поэтому перед использованием монолитной архитектуры нужно все тщательно взвесить. Иногда продумывают такой ход: запуск приложения осуществляют при использовании монолитной архитектуры, а чуть позже, если оно «зашло» пользователю, то его можно быстро раздробить на микросервисы для удобного масштабирования, тем самым меняя его архитектуру. Достоинства монолитной архитектуры являются простая разработка и запуск программы. Благодаря чему, вся разработка сконцентрирована в одном месте, легче дается интегрировать инструменты для облегченной разработки, а также при необходимости изменить элементы программы не нужно вносить изменения по отдельности в разных местах — все делается в одном месте.

Проблемы у монолитной архитектуры практически отсутствуют, так как большое количество приложений имеют зависимость от задач, которые совершаются между компонентами программы: логи, ограничения скорости, контрольные журналы и т. д. При монолитной архитектуре эти проблемы практически отсутствуют, так как все сконцентрировано в одном коде и все работает в одном приложении.

# **ГЛАВА 3. Проектирование безопасности**

## **3.1 Процессы организации**

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

* Регистрация
* Авторизация
* Выгрузка успеваемости курсанта
* Выгрузка расписания занятий
* Распределение нагрузок преподавателей
* Выгрузка отчетов

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

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

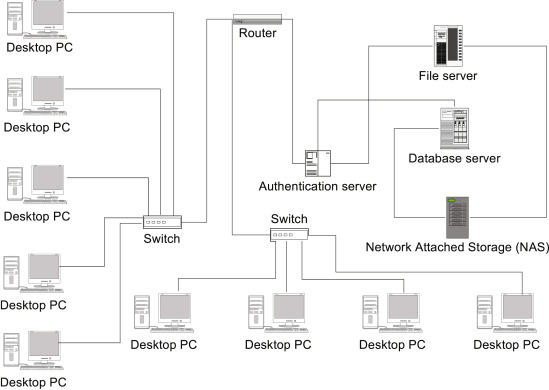


Рис.3.1. Архитектура сети приложения

## **3.3 Идентификация активов**

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

Актив – 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** | **Уязвимость** | **Вероятность CNA (Y2)** | **Актуальность** |
| Несанкционированный доступ к целевому компьютеру | CVE-2016-0702 | 5.1 | (Y1 + Y2)/20 = 0,51  Средняя возможность реализации угрозы  ***Актуальная*** |
| Повреждения программных и технических средств | CVE-2019-7632 | 8.8 | (Y1 + Y2)/20 = 0,69  Высокая возможность реализации угрозы  **Актуальная** |
| Перехват данных с сетевых устройств  (Исполнение произвольного кода  ) | CVE-2020-14524 | 9.8 | (Y1 + Y2)/20 = 0,74  Высокая возможность реализации угрозы  ***Актуальная*** |
| Сбои, отказ в обслуживании | CVE-2020-14522 | 7.5 | (Y1 + Y2)/20 = 0,625  Высокая возможность реализации угрозы  ***Актуальная*** |
| Изменение логов | CVE-2022-22476  CVE-2022-22475 | 5.0 | (Y1 + Y2)/20 = 0,5  Средняя возможность реализации угрозы  ***Актуальная*** |

**3.6 Способы защиты от вероятных атак**

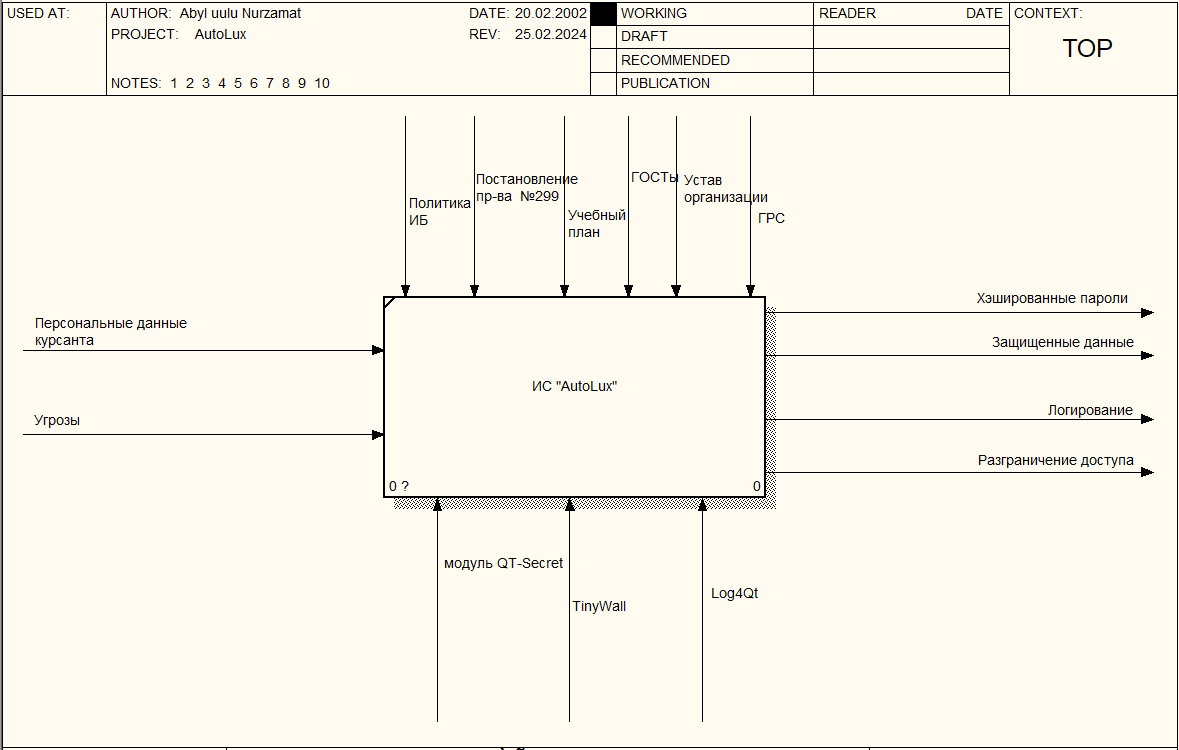


Рис. 3.1 Диаграмма IDEF0

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)
* XMLLayout для поддержки бензопилы Apache
* DailyFileAppender, который генерирует файл журнала за каждый день (добавьте текущую дату в формате имени файла)
* Двоичный регистратор
* Приложение консоли отладки Windows

### **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.

### **3.6.3 Модуль QT-Secret**

[Qt-Secret](https://github.com/QuasarApp/Qt-Secret)— это библиотека, созданная [группой QuasarApp](https://github.com/QuasarApp)на Qt/qmake, цель — для обеспечения основных возможностей шифрования, которых нет в родном Qt. А именно: алгоритмы RSA и AES.

Ключевая особенность:

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

# ПРИЛОЖЕНИЕ А

ИДЕНТИФИКАЦИЯ АКТИВОВ

## **Идентификация активов**

Таблица 3.1 Идентификация активов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Бизнес-процесс** | **Активы** | **Среда обработки** | **ПСИБ** | **Уязвимости** |
| Регистрация | Персональные данные (ИА-1) | Браузер (Chrome, Mozilla Firefox, Opera) | К,Ц,Д | CVE-2021-1636 |
| MS SQL Server 2017 CU31 (ПА) | CVE-2022-23298 |
| Windows 10 Enterprise 21H2 (ПА) | CVE-2019 11137 |
| Авторизация | Идентификационные данные (ИА-2) | Браузер (Chrome, Mozilla Firefox, Opera) | Д,Ц,К | CVE-2022-29143  CVE-2017-8516 |
| MS SQL Server 2017 CU31 (ПА) | CVE-2022-24454 |
| Windows 10 Enterprise 21H2 (ПA) | 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 |
| Microsoft SQL Server 2019 (RTM) | MS Office 2019 16.0 | Д,Ц,К | CVE-2022-24454 |
| 15.0.2000.5 Enterprise Edition (ПA)  MS Office 2019 16.0 (ПA) | Windows 10 Pro 21H2 | К,Ц,Д | 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 |
| Microsoft SQL Server 2019 (RTM) | MS Office 2019 16.0 | Ц,Д,К | CVE-2022-3140 |
| Windows 10 Enterprise 21H2 (ПA) | Windows 10 Pro 21H2 | К,Ц,Д | CVE-2022-23298 |

# ПРИЛОЖЕНИЕ Б

МОДЕЛЬ НАРУШИТЕЛЯ

## **Модель нарушителя**

Таблица 3.2 - Модель Нарушителя

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Угроза ИБ** | **Источник угроз** | **Категория нарушителя** | **Мощность Тех средств** | **Доступ к интернету, тип каналов** | **Финансовые возможности** | **Уровень знаний в области IT** | **Используемые Технологии** | **Знания о построении системы защиты объекта** | **Цели** | **Характер действий** | **Глубина проникновения** |
| Выход из строя(сервер)/ Изменение логов/  Повреждение проводки | Сотрудник фирмы | Внутренний | Компьютер /ноутбук, технические спец средства | Добавляется доступ к корпоративной сети | Могут быть слабо ограничены | Варьируется от должности(инженер, системный администратор, офисный рабочий, офицер ИБ) | Добавляется знание и владение корпоративным софтом | Варьируются от должности и допуска субъекта(вплоть до максимального) | Финансовая выгода | Кража данных, порча активов | В теории максимальная |
| Несанкционированный доступ к целевому компьютеру/  Изменение логов/  Перехват данных с сетевых устройств  (Исполнение произвольного кода и отказ в обслуживании  ) | Хакер-одиночка | Внешний | Компьютер /ноутбук | Обычный доступ к сети, теоретическое имение доступа к закрытым спец каналам в телеграмм и дип вэб | Ограничены заработком и мотивацией субъекта | Варьируется от базового знания утилит и протоколов до специфических умений в ИБ и хакинге | Открытые утилиты  (платные и бесплатные) | Минимальные(открытые данные, слухи) | Самоутверждение и/или финансовая выгода | Взлом системы, использование уязвимостей | Зависит от мощностей и используемых уязвимостей |
| Несанкционированный доступ к целевому компьютеру/ | Представители силовых структур. | Внешний | Не ограничено | Сбор информации | Не ограничено | На уровне офицера ИБ и выше | Не ограничено | Не ограничено | Контроль, Сбор информации | Взлом системы, использование уязвимостей, кибер - разведка | Максимальная |

# ПРИЛОЖЕНИЕ В

МОДЕЛЬ УГРОЗ

## **Модель угроз**

Таблица 3.3 - Модель Угроз

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Угроза ИБ** | **Источник угрозы ИБ** | **Тип актива** | **Значимые свойства ИБ** | **Среда обработки ИА** | **Уязвимость среды обработки ИА** | **Метод Реализации угрозы ИБ на среду обработки** | **Последствия**  **реализации угрозы ИБ**  **Для ИА** |
| Повреждения программных и технических средств | Антропогенный  [I.A.2]  [I.A.6] | Персональные данные  (ИА) | Д, Ц, К | ОЗУ(, DDR4 4GB PC-19200 (2400MHz) TEAM ELITE,) | CVE-2019-7632 | Устройства LifeSize Team, Room, Passport и Networker 220 допускают Аутентифицированное внедрение команд удаленной ОС | Нарушение целостности и/или доступности системы |
| Перехват данных с сетевых устройств  (Исполнение произвольного кода и отказ в обслуживании) | Антропогенный  [I.A.2]  [I.B.4] | Данные с узлов ком сетей  (ИА) | Ц, К, Д | Сетевые устройства (маршрутизаторы, хабы, т.д.) | CVE-2020-14524  CVE-2020-14522 | Исполнение произвольного кода и отказ в обслуживании  https://ics-cert.kaspersky.ru/publications/news/2021/03/04/more-critical-vulnerabilities-identified-in-opc-protocol-implementations/ | Нарушение конфиденциальности и/или доступности |
| Сбои, отказы, разрушения повреждения программных и технических средств | Антропогенный  [I.A.2] | Персональные данные  (ИА) | Д, Ц, К | Microsoft Windows Server 2012 | CVE-2013-0075 CVE-2012-0156 CVE-2012- 0152рее CVE-2011-1965 | DoS-атака | Нарушение доступности системы |
| Изменение логов | Антропогенный  [I.A.2] | Логи  (ИА) | Ц, К, Д | Сеть компании  (IBM WebSphere Application Server и подобные) | CVE-2022-22476  CVE-2022-22475 | IBM WebSphere Application Server Liberty версий с 17.0.0.3 по 22.0.0.7 и Open Liberty уязвимы для подмены идентификационных данных аутентифицированным пользователем с использованием специально созданного запроса. | Нарушение целостности  и/или конфиденциальности |
| Выход из строя | Техногенный и/или Стихийный  [II.B.1] [II.B.2]  [III.A.1]  [III.A.2] | SIEM  (ПА) | К, Ц, Д | SIEM (требования расписаны выше) | Возможные поломки системы, вызванные различными обстоятельствами | | Нарушение целостности и/или доступности |
| Выход из строя | Техногенный и/или Стихийный  [II.B.1] [II.B.2]  [III.A.1]  [III.A.2] | Сервер компании  (ПА) | К, Ц, Д | Сервер (требования расписаны выше) | Возможные поломки системы, вызванные различными обстоятельствами | | Нарушение целостности и/или доступности |
| Повреждение проводки | Антропогенный/  Стихийный  [I.B.4]  [III.A.] | Проводка Сети (ПА) | Ц, Д, К | Проводка Сети | Возможные повреждения проводки, вызванные различными обстоятельствами | | Нарушение целостности и/или доступности |