**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ**

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

**КАФЕДРА «ПРОГРАММНОЕ ОБЕСПЕСЕНИЕ**

**КОМПЬЮТЕРНЫХ СИСТЕМ»**

**ВЫПУСКНАЯ**

**КВАЛИФИКАЦИОННАЯ РАБОТА**

**Разработка и обеспечение безопасности**

**веб-приложения школы**

бакалавр академиялык даражасы

**590100 «Маалыматтык коопсуздук» багыты боюнча**

|  |  |
| --- | --- |
| **Выполнил**  **Группа** | **Ашырбек уулу Анвар**  **ИБ(б)-1-19** |
| **Руководитель** | **доцент Стамкулова Гулдана Кубанычбековна** |

**Бишкек 2023**

**КЫРГЫЗ РЕСПУБЛИКАСЫНЫН БИЛИМ БЕРҮҮ**

**ЖАНА ИЛИМ МИНИСТРЛИГИ**

**И.РАЗЗАКОВ атындагы КЫРГЫЗ МАМЛЕКЕТТИК ТЕХНИКАЛЫК**

**УНИВЕРСИТЕТИ**

**«КОМПЬЮТЕРДИК СИСТЕМАЛАРДЫ ПРОГРАММАЛЫК КАМСЫЗДОО»**

**кафедрасы**

**БҮТҮРҮҮЧҮ**

**КВАЛИФИКАЦИЯЛЫК ИШ**

**Мектептин веб-тиркемесин иштеп чыгуу жана маалыматтык коопсуздугун камсыздоо**

бакалавр академиялык даражасы

**590100 «Маалыматтык коопсуздук» багыты боюнча**

|  |  |
| --- | --- |
| **Аткарган**  **Топ** | **Ашырбек уулу Анвар**  **ИБ(б)-1-19** |
| **Жетекчи** | **доцент Стамкулова Гулдана Кубанычбековна** |

**Бишкек 2023**

**АННОТАЦИЯ**

В данной пояснительной записке представлены результаты разработки и обеспечения безопасности веб-приложения школы.

Пояснительная записка состоит из введения, пяти основных глав, заключения, списка литературы, глоссария и приложения.

В главе «Описание веб-приложения школы» приведено описание веб-приложения разработанной для школы, представлена классификация информации, идентификация активов.

В главе «Оценка угроз информационной безопасности веб-приложения» включены этапы анализ и описание актуальных угроз ИБ.

В главе «Процессы и меры защиты информации веб-приложения» определяется перечень процессов системы защиты информации и реализующих их мер защиты информации для снижения уровня риска до приемлемого.

В главе «Построение системы обеспечения информационной безопасности» представлены оценка защищенности, разработка требований к безопасности ОС Windows Pro, управления парольной политикой, управления предоставлением удаленного доступа.

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

В состав данной работы также входят приложения.

Пояснительная записка состоит из 73 страниц, содержит 25 рисунков, 6 таблиц, используется 9 источников.

**АННОТАЦИЯ**

Бул түшүнүк катта мектептин веб-тиркемесин иштеп чыгуунун жана коопсуздугун камсыз кылуунун натыйжалары келтирилген.

Түшүндүрмө кат кириш сөздөн, беш негизги бөлүмдөн, корутундудан, пайдаланылган адабияттардын тизмесинен, глоссарийден жана тиркемеден турат.

«Веб-тиркеменин сүрөттөлүшү» мектептин автоматташкан веб-тиркемеси сүрөттөлөт, процесстин модели, маалыматтын классификациясы жана активдерди идентификациялоо сунушталат.

«Веб-тиркеменин маалыматтык коопсуздугуна болгон коркунучтарды баалоо» бөлүмүндө МК коркунучтарын талдоо жана сыпаттоо этаптарын камтыйт.

«Веб-тиркеменин маалыматын коргоо процесстери жана чаралары» бөлүмү маалыматтык коопсуздук тутумунун процесстеринин тизмесин жана тобокелдиктин деңгээлин алгылыктуу деңгээлге чейин төмөндөтүү үчүн аларды ишке ашыруучу маалыматтык коопсуздук чараларын аныктайт.

«Маалыматтык коопсуздук системасын түзүү» бөлүмүндө коопсуздукту баалоо, маалыматтар базасын коргоо, сырсөз саясатын башкаруу берилген.

«Маалыматтык коопсуздук системасын түзүү» бөлүмүндө «Эксперименталдык бөлүм» бөлүмүндө тестирлөөнүн планы жана тестирлөөнүн натыйжалары келтирилген.

Бул иш ошондой эле тиркемелерди камтыйт.

Түшүндүрмө кат 73 барактан турат, 25 сүрөттөн, 6 таблицадан турат, 9 булак колдонулган.

**ОГЛАВЛЕНИЕ**

[ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 15](#_Toc137639682)

[ВВЕДЕНИЕ 18](#_Toc137639683)

[АКТУАЛЬНОСТЬ РАБОТЫ 19](#_Toc137639685)

[ЦЕЛЬ 20](#_Toc137639686)

[ЗАДАЧИ 20](#_Toc137639687)

[ГЛАВА 1. АНАЛИЗ И РАЗРАБОТКА ТРЕБОВАНИЙ 21](#_Toc137639688)

[1.1 Общая характеристика объекта защиты 21](#_Toc137639689)

[1.2 Обоснование для разработки 21](#_Toc137639690)

[1.3 Обзор системы школы 21](#_Toc137639691)

[1.4 Описание процессов 23](#_Toc137639692)

[1.5 Функциональные требования 24](#_Toc137639693)

[1.6. Основные процессы и информационные потоки 24](#_Toc137639694)

[1.7 Требования к составу и параметрам технических средств 25](#_Toc137639695)

[ГЛАВА 2. КОНСТРУКТОРСКИЕ РАБОТЫ 26](#_Toc137639696)

[2.1 Декомпозиция концептуальной работы 26](#_Toc137639697)

[2.2 Организация структуры данных 26](#_Toc137639698)

[2.3 Архитектура разрабатываемой системы 28](#_Toc137639699)

[2.4 Уязвимости в процессах системы 30](#_Toc137639700)

[ГЛАВА 3. ПРОЕКТИРОВАНИЕ БЕЗОПАСНОСТИ 32](#_Toc137639701)

[3.1 Процессы организации 32](#_Toc137639702)

[3.2 Инфраструктура веб-приложения 32](#_Toc137639703)

[3.3 Идентификация активов 33](#_Toc137639704)

[3.4 Модель нарушителя 35](#_Toc137639705)

[3.5 Модель угроз 36](#_Toc137639706)

[3.6 Способы защиты от вероятных атак 40](#_Toc137639707)

[ГЛАВА 4. РАЗРАБОТКА ДОКУМЕНТАЦИИ 48](#_Toc137639713)

[4.1 Описание программы 48](#_Toc137639714)

[4.2 Руководство разработчика 48](#_Toc137639715)

[ГЛАВА 5. ТЕСТИРОВАНИЕ 50](#_Toc137639716)

[5.1 DoS атака 50](#_Toc137639717)

[5.2 SQL инъекция 51](#_Toc137639718)

[ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 53](#_Toc137639719)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ 2](#_Toc137639720)

[ЗАКЛЮЧЕНИЕ 55](#_Toc137639721)

[ПРИЛОЖЕНИЯ 56](#_Toc137639722)

[ПРИЛОЖЕНИЕ А 57](#_Toc137639723)

[ПРИЛОЖЕНИЕ Б 63](#_Toc137639724)

[ПРИЛОЖЕНИЕ В 68](#_Toc137639725)

[ПРИЛОЖЕНИЕ Г 72](#_Toc137639726)

# **ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

В настоящем отчете применяются следующие термины с соответствующими определениями:

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

Действия в ЧС (англ. Emergency Response): оперативное реагирование (ответные меры) на событие (эвакуация персонала и оборудования, вызов аварийных служб и т.п.) и аварийное восстановление, включая первоначальный контроль ЧС, действия аварийно- спасательных служб с целью сохранения человеческой жизни и стабилизация ситуации, обеспечение охраны, первоначальная оценка ущерба и, если возможно, ограничение размера этого ущерба.

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.

Компетентность(competence): способность применять знания и умения для достижения намеченных результатов.

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

Максимально приемлемый период нарушения (maximum tolerable period of disruption): Период времени, по истечении которого существует угроза окончательной потери жизнеспособности организации в том случае, если поставка продукции и/или предоставление услуг не будут возобновлены.

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.

Несоответствие (nonconformity): невыполнение требования.

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.

Соответствие (conformity): выполнение требования.

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**

# Современные школы всё больше прибегают к использованию веб-приложений для улучшения организационных процессов и обеспечения качественного образования. Однако, с ростом цифровизации и увеличением объёма передаваемой информации, безопасность таких веб-приложений становится критически важным аспектом, требующим специального внимания. В данной выпускной квалификационной работе (ВКР) исследуется разработка и обеспечение безопасности веб-приложения школы, с учетом современных технологий и угроз информационной безопасности.

Необходимость обеспечения безопасности персональных данных в настоящее время стала объективной реальностью. Эта необходимость вызвана быстрым развитием современных информационных технологий, средств электронной коммерции и электронного информационного обмена между пользователями, свободного доступа к средствам массовых коммуникаций, возможностью копирования и распространения информации.

Потеря персональных данных приводит к тому, что, используя данные сотрудника, злоумышленники могут продать их на специальных форумах, украсть его личность, оформить кредит с большими процентами.

**АКТУАЛЬНОСТЬ РАБОТЫ**

В школе работают более 100 человек персонала, и из них преподавательский состав 60 человек. Количество учащихся превышает 1500 человек. Для эффективного обучения школьников и для быстрого получения отчетности, преподаватели сталкиваются со множеством количеством проблем. В ходе анализа, были выявлены следующие проблемы:

* Заполнение поурочных/годовых планов. Это занимает огромное количество времени для заполнения документов.
* Вывод отчетности. Каждый четверть преподаватели вручную составляют таблицу по успеваемости учеников. Также, завучи вручную заполняют Excel файл для предоставления отчетности к вышестоящим органам.
* Отсутствие единого базы данных для хранения и обработки данных. Недостаточность места хранения архивных данных.
* Трата на ресурсы. Каждый преподаватель в день используют 6-7 белых бумаг формата А4, и в месяц один раз меняют картридж.
* Трата времени. Для заполнения документов, каждый преподаватель в день минимум тратит по 2-3 часа.

В связи с этими проблемами, было принято решение разработать и обеспечить безопасность веб-приложения для школы.

# **ЦЕЛЬ**

Цель работы заключается в разработке и обеспечении информационной безопасности веб-приложения школы, включающая в свой состав:

* Управление базой данных учащихся;
* Сотрудники;
* Обеспечение безопасности системы и всех основных процессов, входящих в состав школы;

# **ЗАДАЧИ**

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

По средствам защиты:

* Разработка модели угроз.
* Разработка нарушителя.
* Разработка Проекта Политики ИБ.
* Настройка межсетевого экрана.
* Защита от скриптовых атак и перебора паролей.
* Защита от SQL-инъекции.
* Шифрование данных.

**ГЛАВА 1. АНАЛИЗ И РАЗРАБОТКА ТРЕБОВАНИЙ**

**1.1 Общая характеристика объекта защиты**

Веб приложение разработано на языке программирования Java v11, а хранение данных производится на СУБД MySQL . Целью создания веб приложения является оптимизация работы и улучшение взаимодействия преподавателей и отчетов. Внедрение является практической мерой по обеспечению эффективности производственного процесса. Для работы веб приложения используется Ubuntu Server v21.04 и Apache2.

**1.2 Обоснование для разработки**

Разработанное веб приложение для школы призвано для внутри организационного пользования, с хранением и обработкой внутри себя персональных данных сотрудников, учеников и родителей. 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.

**1.3 Обзор системы школы**

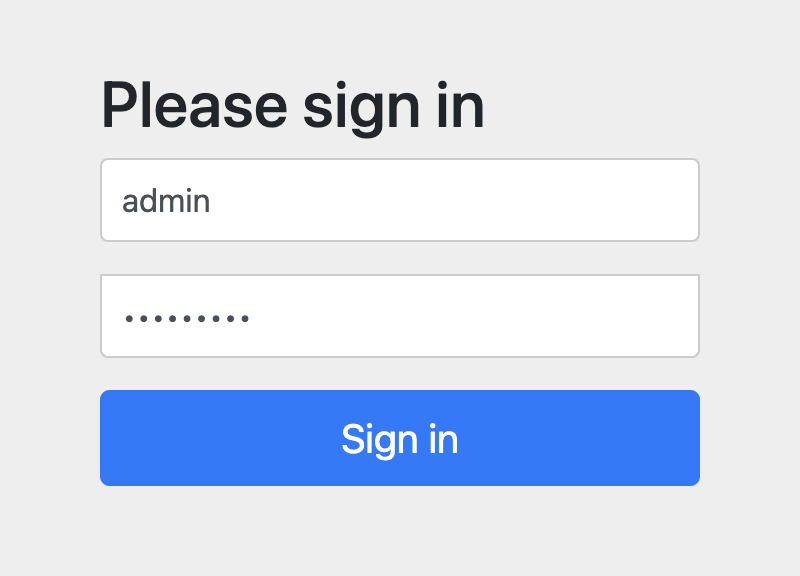


Рис.1.1. Форма для входа в систему

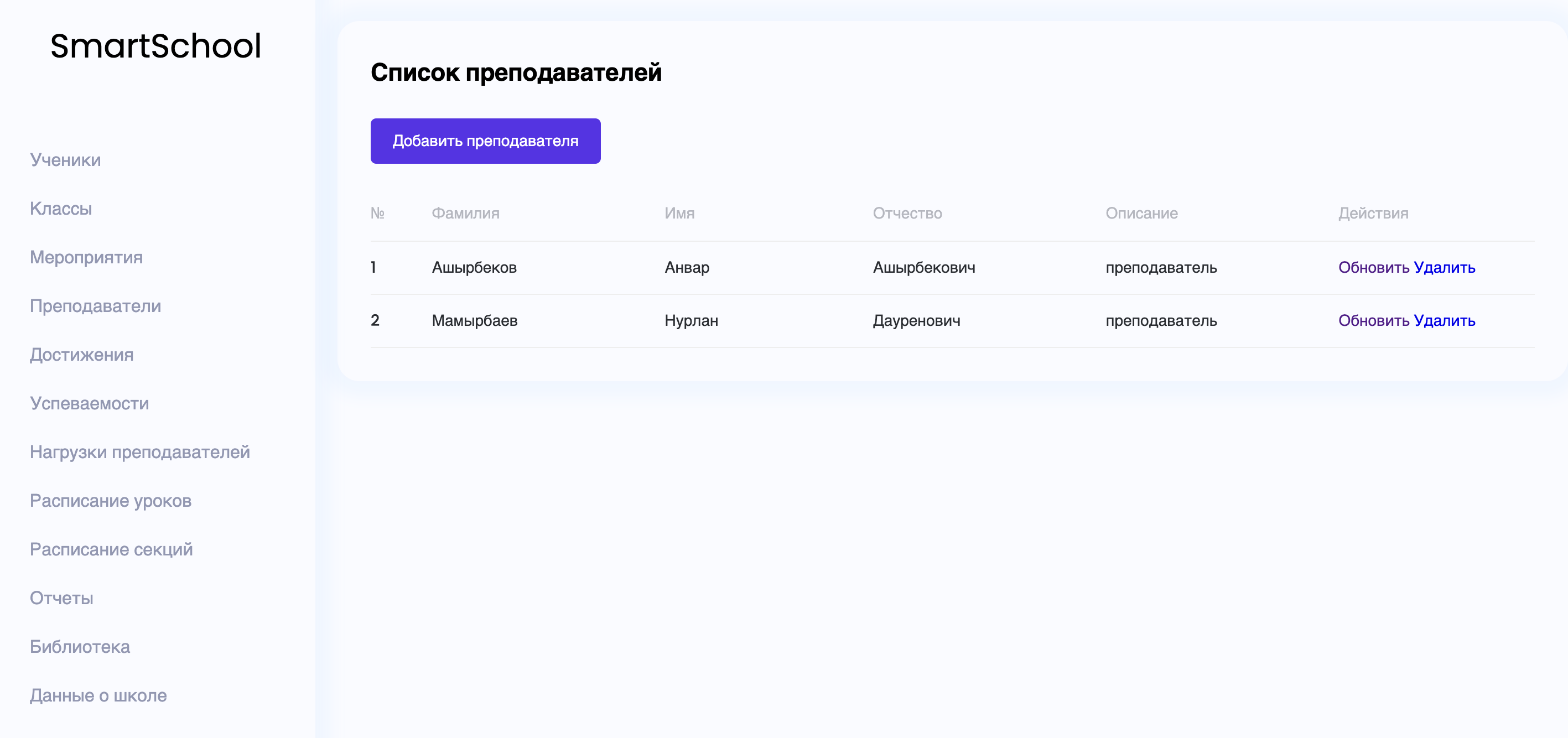


Рис.1.2. Страница для просмотра данных

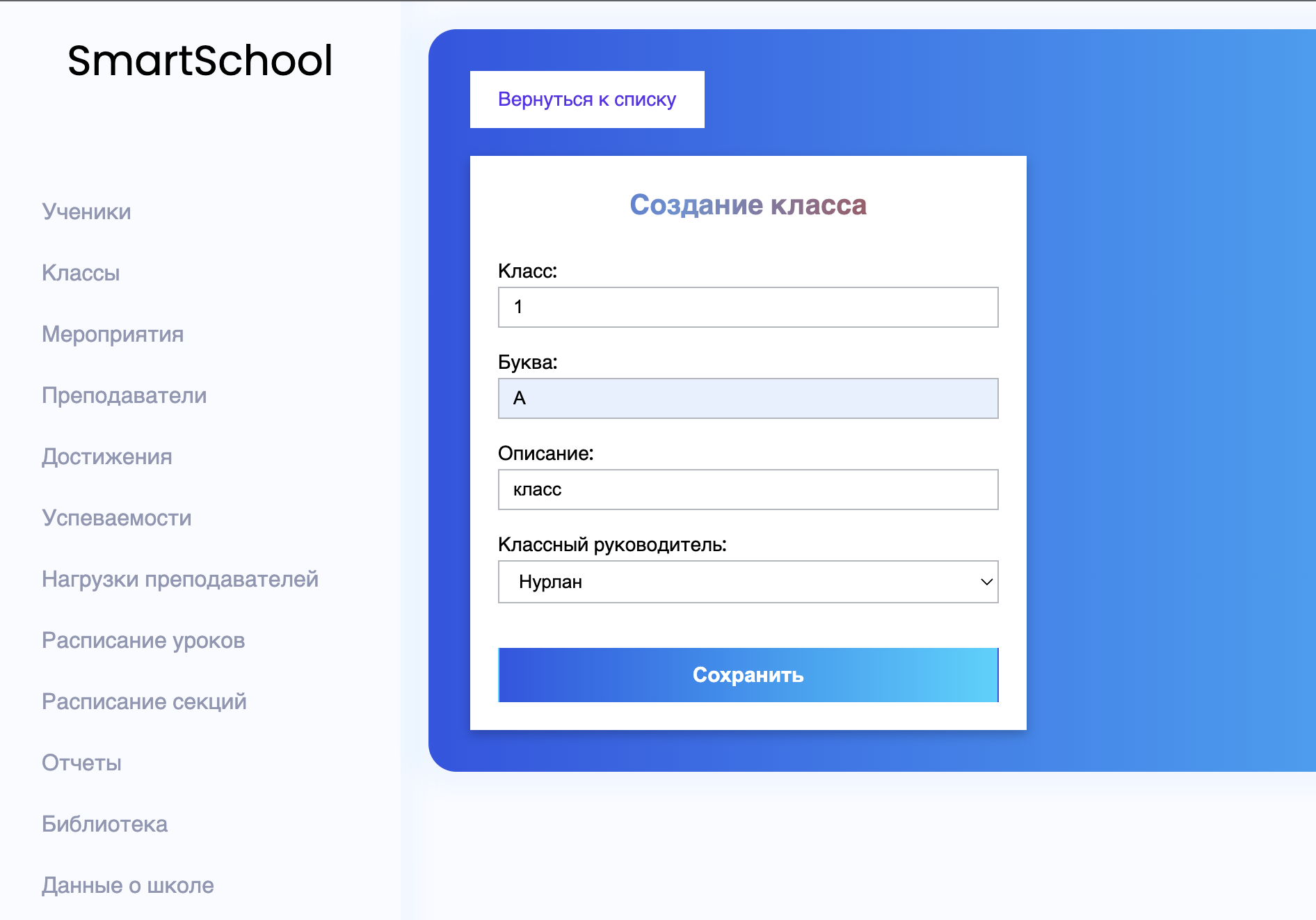


Рис.1.3. Страница для добавления данных

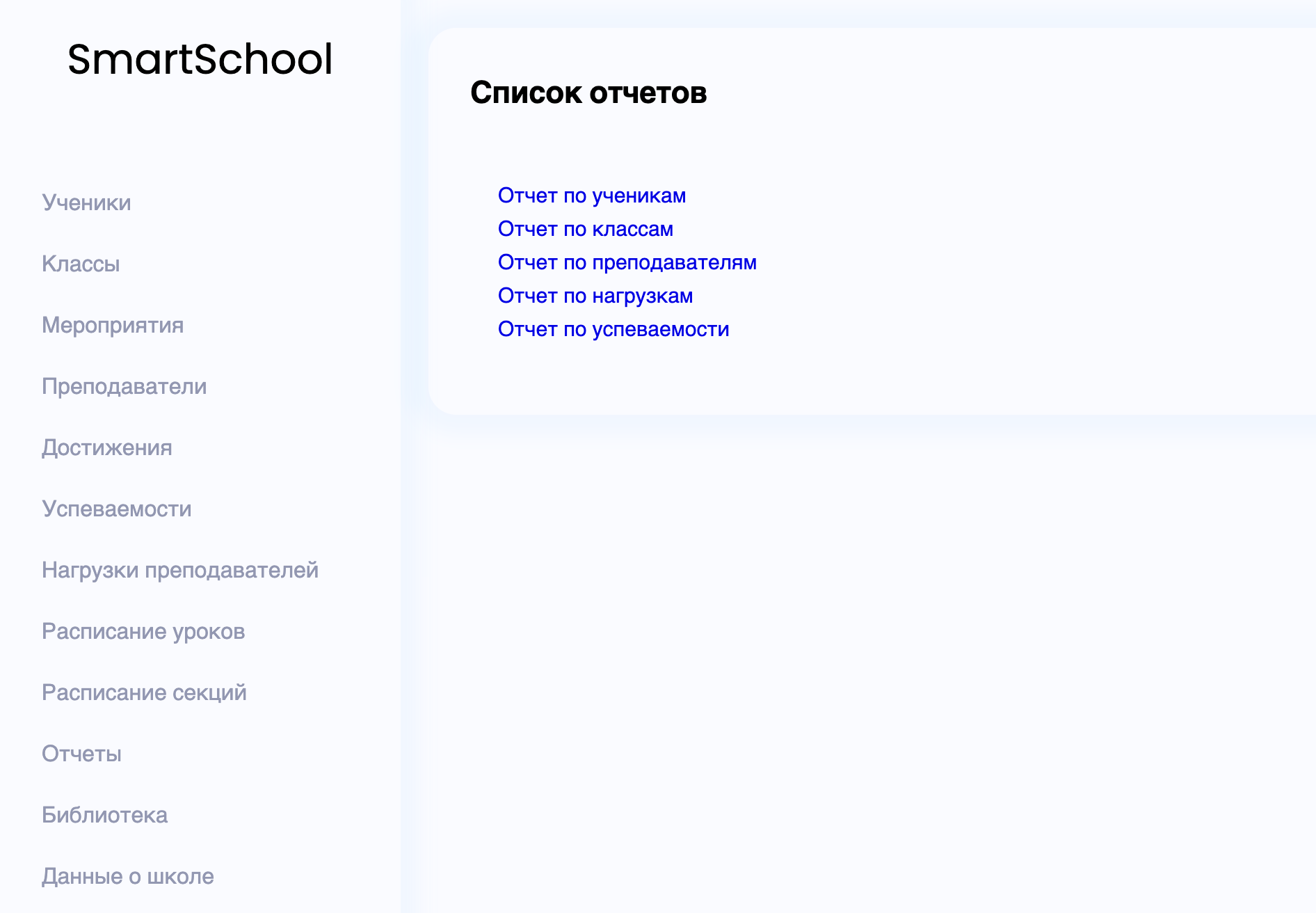


Рис.1.4. Страница для скачивания отчетов

**1.4 Описание процессов**

Таблица 1.1. Процессы

|  |  |  |
| --- | --- | --- |
| **Процесс** | **Актив** | **Среда обработки** |
| Авторизация сотрудников | Персональные данные | ПК, Сервер |
| Регистрация сотрудников | Персональные данные | ПК, Сервер |
| Добавить класс | Информация ограниченного доступа | ПК, Сервер |
| Добавить ученика | Информация ограниченного доступа | ПК, Сервер |
| Добавить мероприятия | Открытый доступ | ПК, Сервер |
| Добавить новости | Открытый доступ | ПК, Сервер |
| Добавить успеваемости учеников | Информация ограниченного доступа | ПК, Сервер |
| Справочник по сотрудникам, ученикам | Информация ограниченного доступа | ПК, Сервер |

**1.5 Функциональные требования**

Разрабатываемое веб-приложение должно выполнять следующие функции:

* Регистрация / Авторизация
* Просмотр справочника сотрудников, учеников
* Скачивание отчетов
* Введение успеваемости учащихся по четвертям
* Мероприятия / достижения
* Добавление, удаление, обновление классов, учеников, преподавателей
* Нагрузка преподавателей

**1.6 Основные процессы и информационные потоки**

В процессе проведения анализа требований к разрабатываемой системе, была создана модель в виде диаграммы IDEF0 (рис. 1.5.). Данная диаграмма показывает процессы, которые протекают внутри школы в ходе выполнения работ, что позволяет более детально рассмотреть проблемы и определить уязвимые места системы.

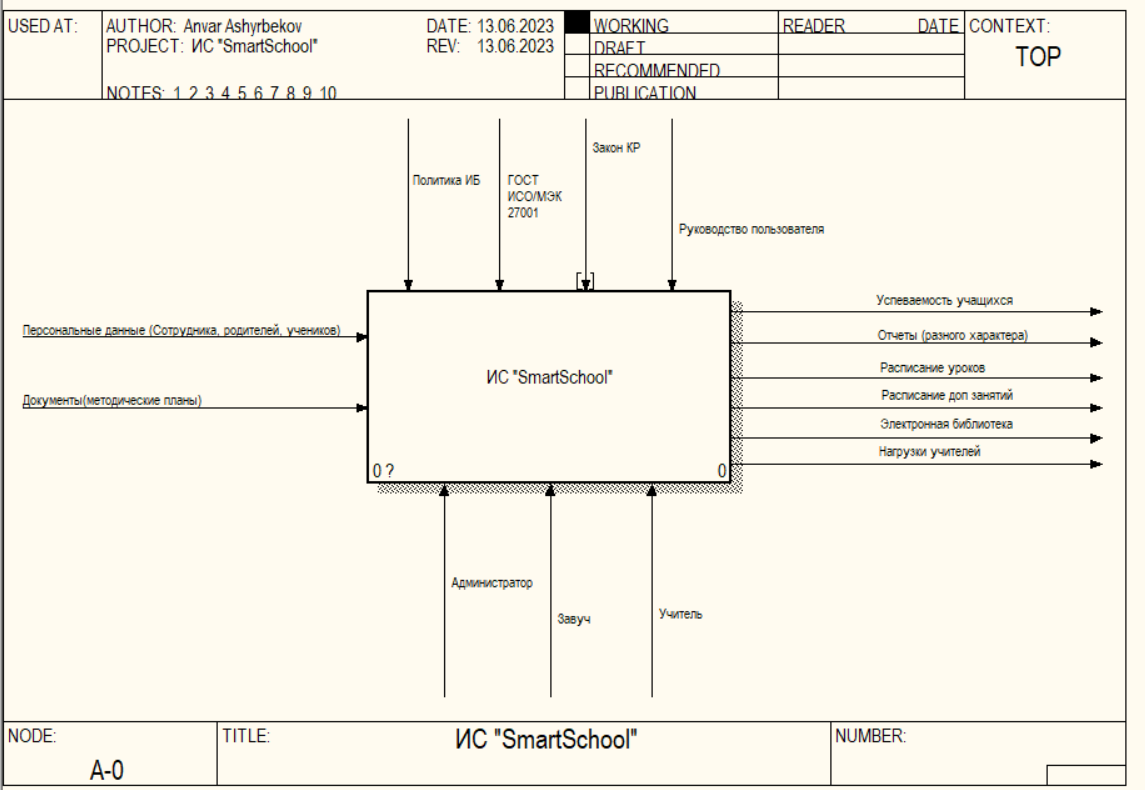


Рис.1.5. Основной процесс школы

**1.7 Требования к составу и параметрам технических средств**

Требования к аппаратным и программным средствам.

Для успешной работы клиента необходимо любое устройство с выходом в интернет и поддержкой веб-браузеров, таких как Google Chrome, Opera, Mozilla.

Требование к программным средствам:

* Java v11
* Spring Boot
* MySQL

Требования к аппаратному обеспечению сервера:

* 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.

**ГЛАВА 2. КОНСТРУКТОРСКИЕ РАБОТЫ**

**2.1 Декомпозиция концептуальной работы**

На Рис.2.1. представлена декомпозиция контекстной диаграммы веб-приложения.

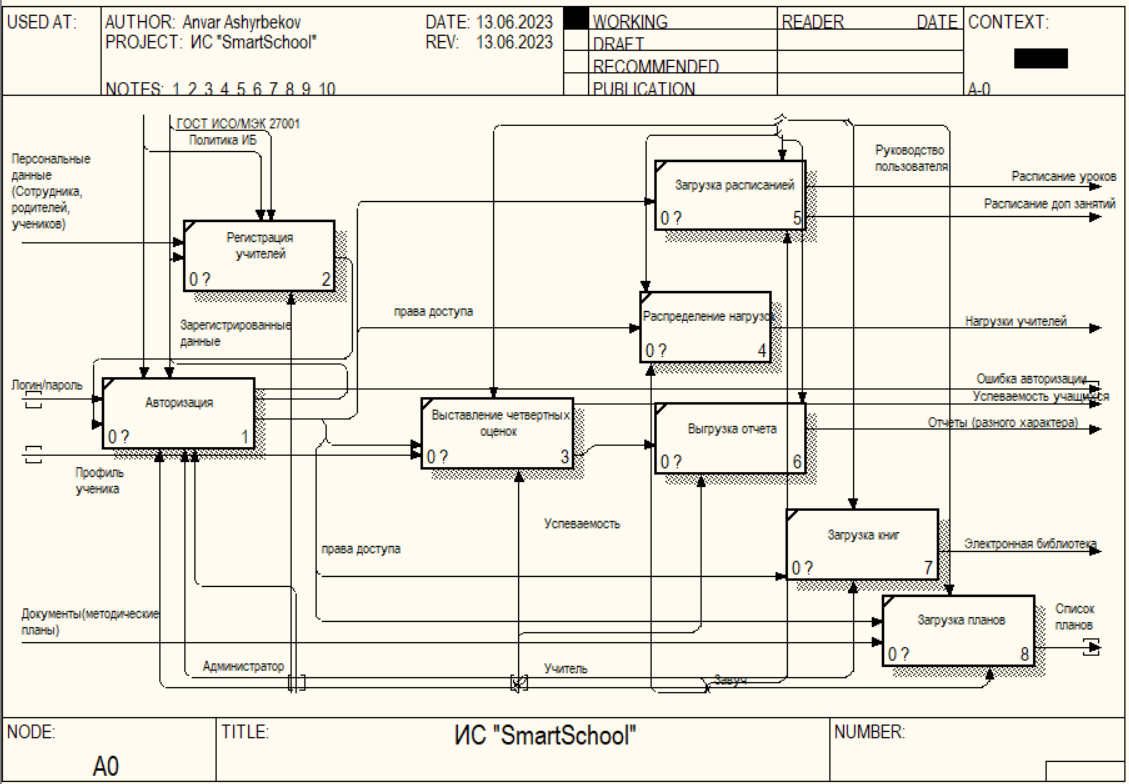


Рис. 2.1. Декомпозиция контекстной диаграммы

## 2.2 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.

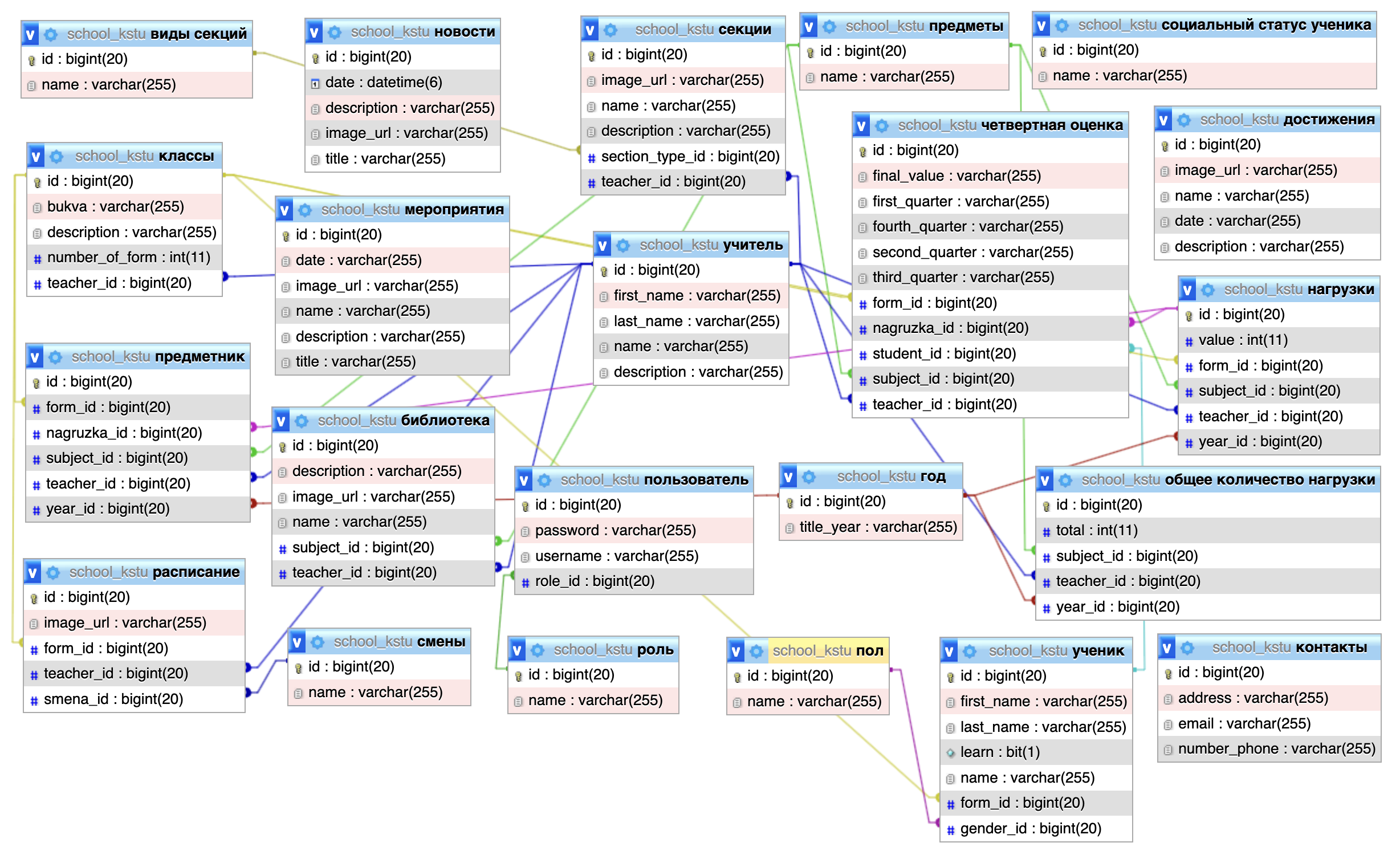


Рис.2.2. ER-диаграмма

## 2.3 Архитектура разрабатываемой системы

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. Монолит — это сила и на века.

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.

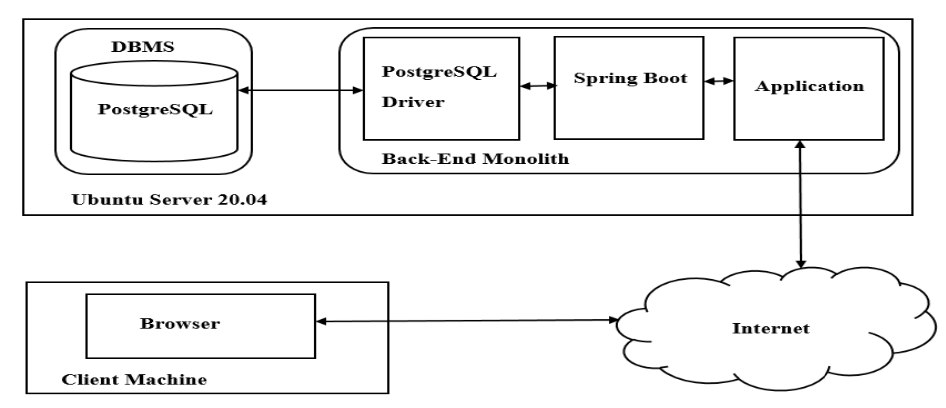


Рис.2.3. Архитектура системы

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.

Также преимуществом монолитной архитектуры является улучшенная производительность, если учитывать, что приложения были собраны правильно, то одно и то же приложение при монолитной архитектуре будет работать более производительно, чем при микросервисах. Это, опять же, обеспечивается единым кодом программы и работой из «одного» места.

**2.4 Уязвимости в процессах системы**

Чтобы выявить способы защиты системы, необходимо определить на каких процессах возникают уязвимые инциденты на (Рис.2.4.) представлена абстрактная модель взаимодействие разных типов пользователей с ИС.

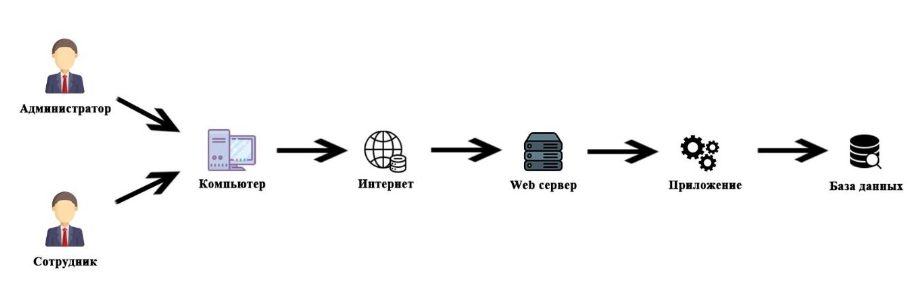


Рис.2.4. Схема взаимодействия пользователей с системой

Исходя из схемы самой главной уязвимостью, веб-приложения является уровень транспорта, данные перемещаются по глобальной сети (интернет) где вероятность искажения информации велик (получение и отправка данных между клиентом и сервером):

•  Уязвимость на уровне клиентского приложения;

•  Сервер, который обрабатывает поступающие от клиентского приложения запросы.

На данные уязвимости распространены такие атаки, как CSRF (межсайтовая подделка запроса), атака ботов, SQL injection (Внедрение SQL-кода), DDoS атака.

**2.5 Классификация и анализ источников угроз и уязвимостей**

Под угрозой информационной безопасности принято понимать потенциально возможные действия, процессы, способные оказать отрицательное воздействие на систему или хранящуюся в ней информацию.

Наиболее значимыми угрозами безопасности информации для информационного портала являются:

•  Нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов, а также подделка данных.

•  Нарушение конфиденциальности (раскрытие) информации.

Для обеспечения защиты информации от атак, необходимо составить:

•  Модель угроз.

•  Модель нарушителя.

•  Политику безопасности.

•  Список часто вызываемых атак на веб-приложения.

**ГЛАВА 3. ПРОЕКТИРОВАНИЕ БЕЗОПАСНОСТИ**

**3.1 Процессы организации**

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

- Регистрация

- Авторизация

- Выставление четвертных оценок

- Выгрузка расписания уроков

- Распределение нагрузок

- Выгрузка отчетов (поурочные/годовые, успеваемости, сотрудников)

- Электронная библиотека

**3.2 Инфраструктура веб-приложения**

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

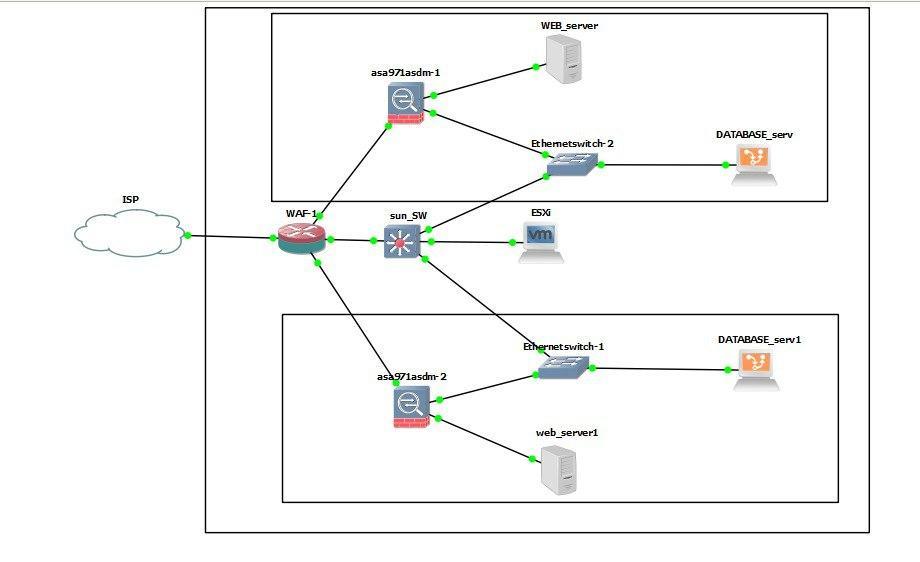


Рис.3.1. Архитектура сети веб-приложения

**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 со школой:

1. Информационный актив:
   1. Персональные данные
   2. Данные ограниченного доступа (отчеты, планы, классы, журналы и т.д.)
   3. Данные открытого доступа (учебные материалы, методички и др.)
   4. Аутентификационные данные (логин/пароль)
2. Ресурсы:
   1. Программные:
      1. Операционные системы
      2. Программные обеспечениФайлы
   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).

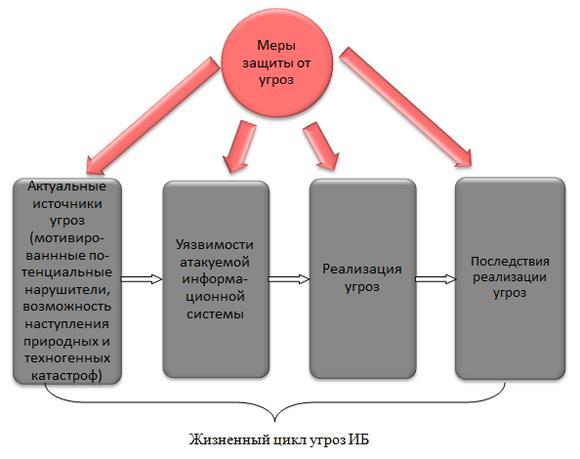


Рис.3.2. Жизненный цикл угроз ИБ

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 доступа к панели админа | 0 | 2 | 0,1 | неактуальная |
| Сбои и отказы в обслуживании | 5 | 10 | 0,75 | актуальная |
| SQL-инъекции | 10 | 10 | 1 | актуальная |
| Кража аутентификационных данных | 10 | 5 | 0,75 | актуальная |
| Обход контроля доступа | 5 | 5 | 0,5 | актуальная |
| Межсайтовый  скриптинг XSS | 10 | 5 | 0,75 | актуальная |
| Повышение  привилегий | 5 | 10 | 0,75 | актуальная |

**3.6 Способы защиты от вероятных атак**

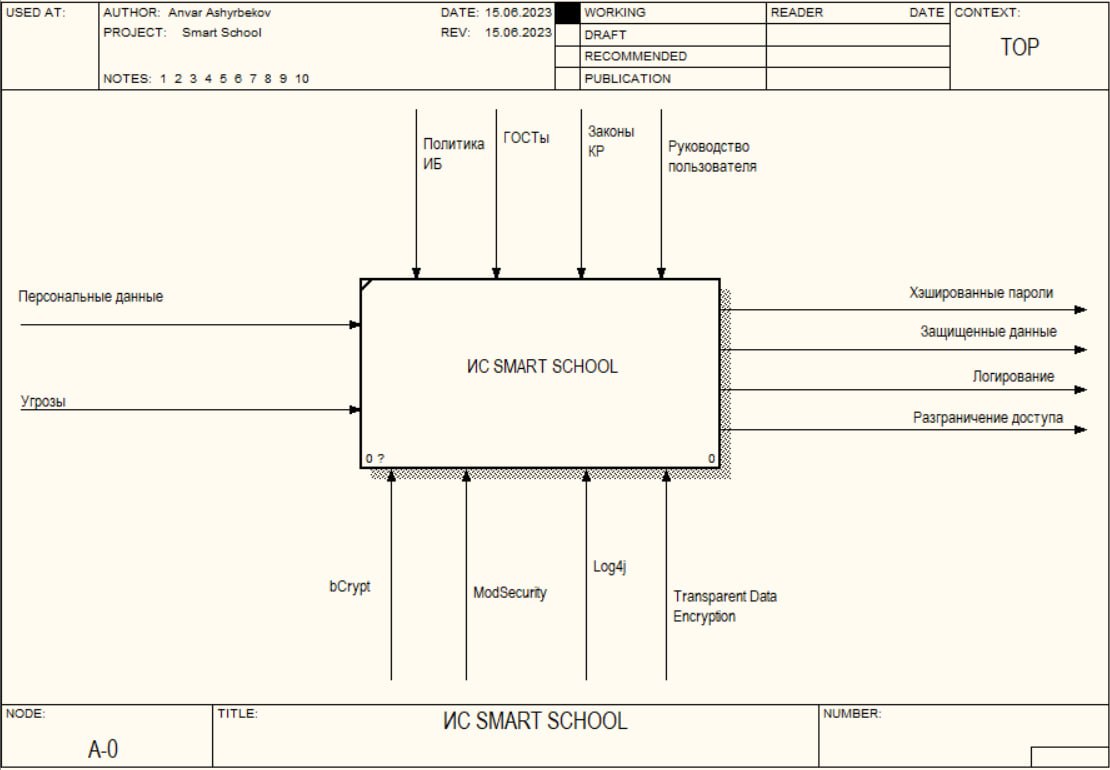


Рис.3.3. Диаграмма IDEF0

Входные данные:

- Персональные данные

- Угрозы

Управление:

- Политика ИБ

- Модель угроз

- Модель нарушителя

- ГОСТ ИСО/МЭК 27001

- ГОСТ Р 53114-2008

Механизмы:

- bCrypt

- MySQL Enterprise Transparent Data Encryption

- WAF (web-application firewall). ModSecurity

- Log4j

- Google Auth

Выходные данные:

- Хэшированные пароли

- Защищенные данные

- Разграничение доступа

- Логирование

### 3.6.1 bCrypt

bcrypt - это алгоритм хеширования паролей, который используется для обеспечения безопасности хранения паролей в системах. Он является одним из наиболее безопасных способов хеширования паролей, так как он медленный и устойчив к атакам перебора паролей.

Алгоритм bcrypt основан на функции хеширования Blowfish и использует множество итераций и случайно сгенерированную "соль" для хеширования пароля. Соль - это случайная строка, которая добавляется к паролю перед его хешированием. Это позволяет создавать уникальный хеш для каждого пароля, даже если сами пароли совпадают.

Использование bcrypt обеспечивает дополнительный уровень безопасности, так как хешированный пароль не может быть обратно преобразован в исходный пароль. Это означает, что даже в случае компрометации базы данных с хешами паролей, злоумышленнику будет крайне сложно восстановить и использовать исходные пароли.

bcrypt также автоматически увеличивает время хеширования паролей с течением времени. Это важно для противодействия атакам перебора паролей, так как они требуют больше времени на проверку каждого возможного пароля.

В целом, bcrypt является эффективным и безопасным способом хеширования паролей, который рекомендуется для использования в системах, где требуется хранение паролей пользователей.

На рисунках 3.4. - показана как работает bCrypt в моей системе. При регистрации пользователя пароли будут храниться в хешированном виде, это означает что, даже если злоумышленник получит пароли в базе данных, он не сможет прочитать исходные пароли



Рис.3.4. Подключение модуля bCrypt

Нужно прописать конфигурацию для класса BcyptConf в конфигурационном файле, чтобы при вызове класса модуль мог автоматически генерировать хэш.

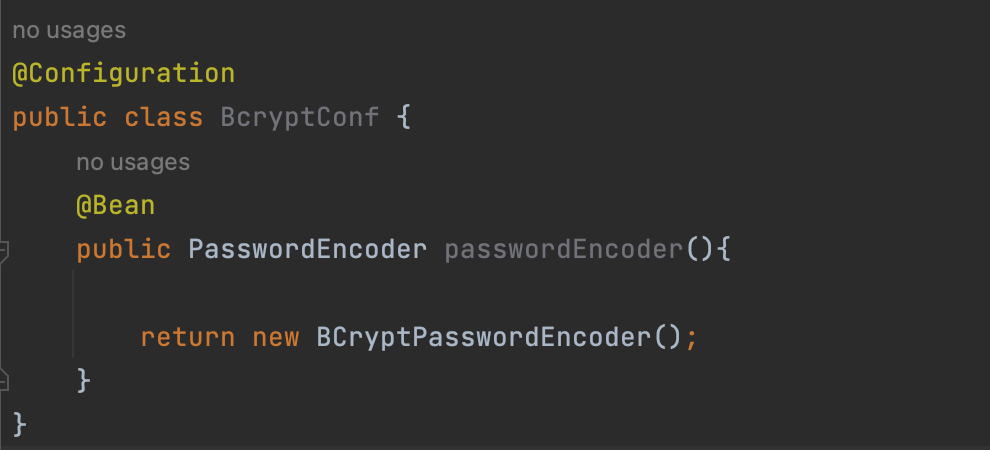


Рис.3.5. Генерация хэша

На Рис.3.6.1.3. приведены фрагменты записи из базы данных, на которых показаны хэшированные пароли пользователей системы.

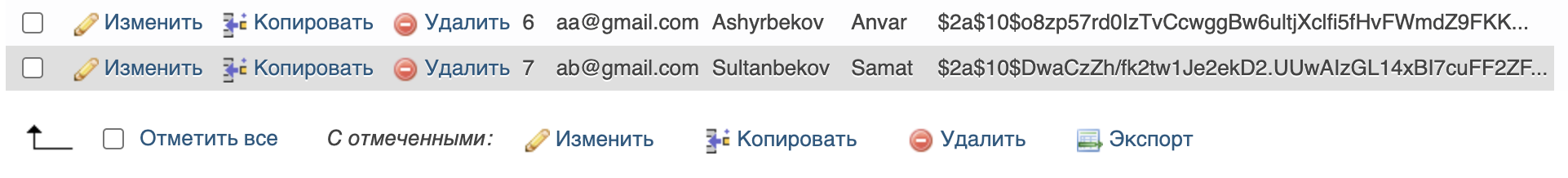


Рис.3.6. Хэшированные пароли в базе данных

### 3.6.2 MySQL Enterprise

MySQL Enterprise Transparent Data Encryption (TDE) - это функциональность, предоставляемая MySQL Enterprise Edition, которая обеспечивает прозрачное шифрование данных в базе данных MySQL. TDE позволяет шифровать данные на уровне хранения, то есть данные автоматически шифруются перед записью на диск и автоматически расшифровываются при чтении.

Основные особенности MySQL Enterprise TDE:

* Прозрачность: при использовании TDE нет необходимости изменять код приложений или запросы SQL. Шифрование и расшифровка данных происходят автоматически на уровне хранения, и для приложений это остается незаметным.
* Гранулярное шифрование: TDE позволяет выбирать, какие столбцы или таблицы шифровать. Вы можете выбирать конкретные столбцы, содержащие конфиденциальные данные, или шифровать всю таблицу целиком. Это дает гибкость в определении уровня шифрования в вашей базе данных.
* Управление ключами: MySQL Enterprise TDE предоставляет инструменты для генерации, хранения и управления ключами шифрования. Ключи шифрования хранятся в специальном хранилище ключей, что обеспечивает их безопасность и контроль доступа.
* Высокая производительность: TDE предлагает аппаратное ускорение шифрования и оптимизированные алгоритмы шифрования, что помогает поддерживать высокую производительность базы данных даже при работе с зашифрованными данными.
* Совместимость: MySQL Enterprise TDE совместим с существующими приложениями и инструментами, разработанными для MySQL. Вы можете использовать TDE в существующих базах данных без необходимости изменения приложений или схемы базы данных.

MySQL Enterprise Transparent Data Encryption обеспечивает надежное и прозрачное шифрование данных в базе данных MySQL, что помогает защитить конфиденциальность информации и соответствовать требованиям безопасности данных.

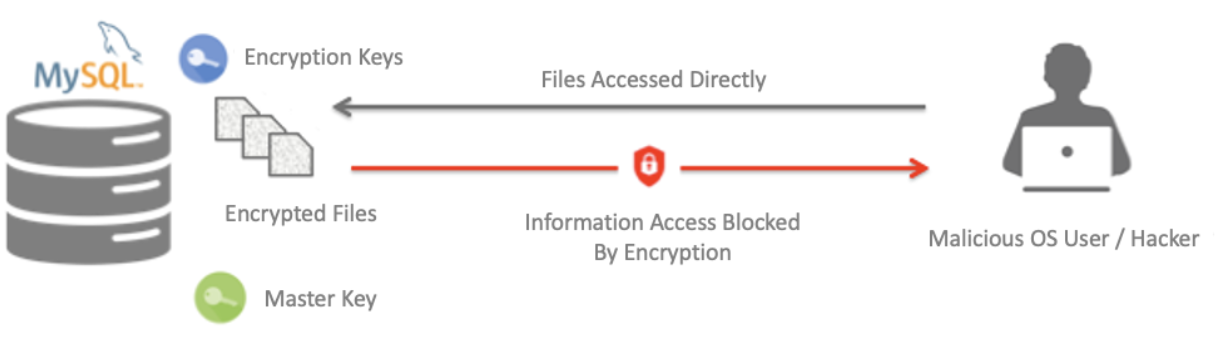


Рис.3.7. Алгоритм работы утилиты

### 3.6.3 WAF (Web application firewall). ModSecurity

ModSecurity — это мощный веб-приложениями брандмауэр (WAF), который обеспечивает защиту веб-приложений от различных атак и уязвимостей. Он работает на уровне веб-сервера и просматривает входящий и исходящий трафик, анализируя его на наличие злонамеренных действий и потенциально опасных паттернов.

Основные особенности ModSecurity:

* Фильтрация и блокировка атак: ModSecurity может обнаруживать и блокировать различные типы атак, такие как инъекции SQL, кросс-сайтовый скриптинг (XSS), внедрение кода и другие. Он использует набор предварительно определенных правил и паттернов, а также дает возможность создания пользовательских правил.
* Отслеживание и аудит: ModSecurity позволяет вести детальный журнал событий, включая информацию о блокированных запросах и атаках. Это обеспечивает возможность проведения анализа инцидентов и выявления уязвимостей в веб-приложениях.
* Защита от известных уязвимостей: ModSecurity поддерживает обновляемые наборы правил, которые содержат информацию о новых уязвимостях и методах атак. Это позволяет быстро реагировать на новые угрозы и обеспечивать защиту от них.
* Гибкая конфигурация: ModSecurity предлагает широкие возможности для настройки и персонализации. Вы можете задать свои собственные правила, блокировать или разрешать определенные запросы или параметры, настраивать уровень журналирования и многое другое.
* Интеграция с веб-серверами: ModSecurity является модулем, который может быть интегрирован с различными веб-серверами, такими как Apache, Nginx и другие. Это обеспечивает удобство установки и использования в различных окружениях.

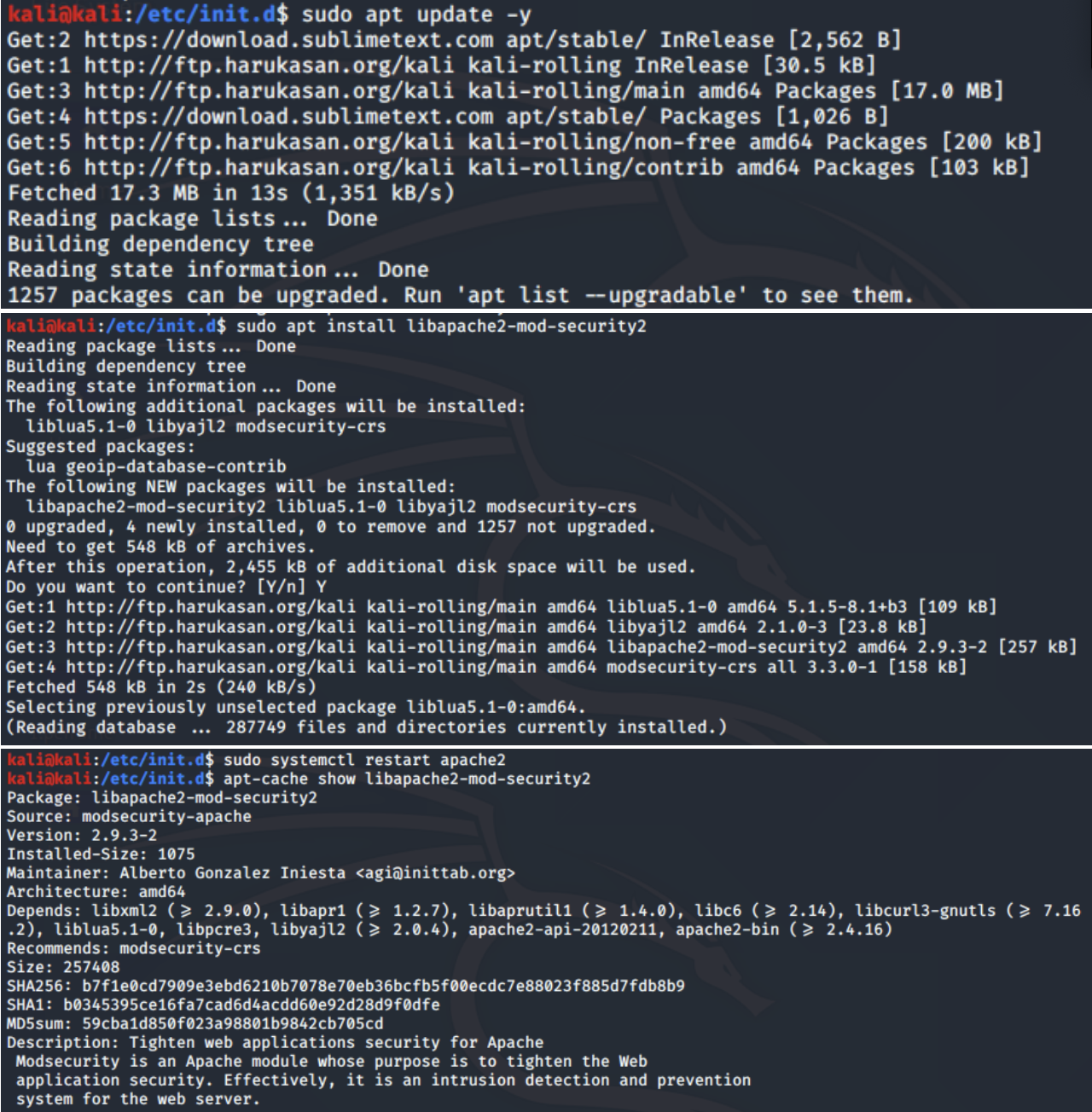


Рис.3.8. Установка ModSecurity

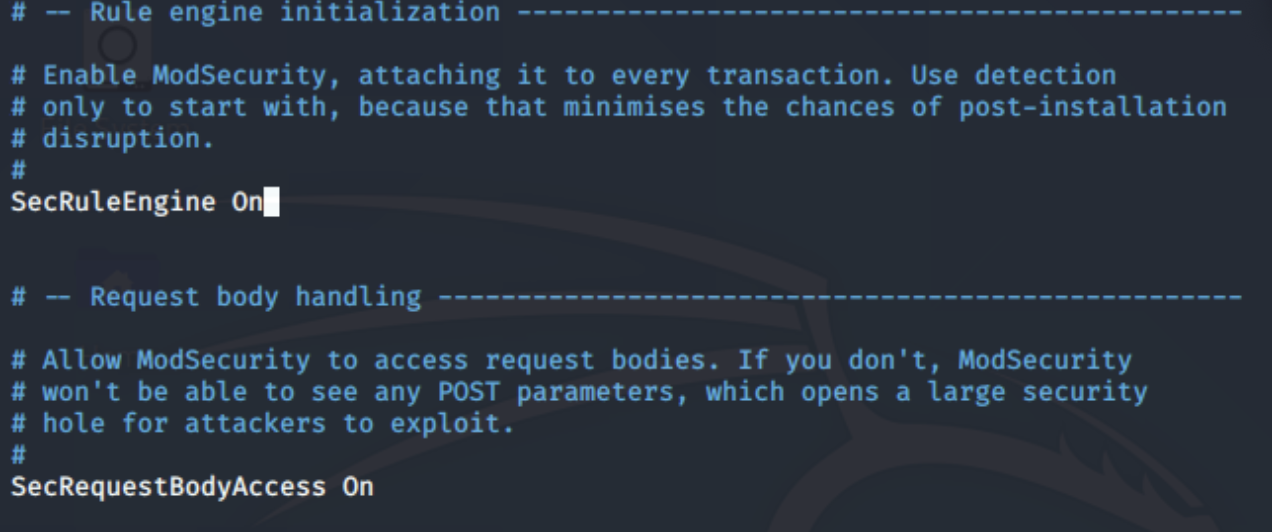


Рис.3.9. Настройка ModSecurity

### 3.6.4 Log4j

Log4j - это популярный инструмент для логирования в Java. Он предоставляет гибкую и удобную функциональность для записи и управления логами в приложениях.

Основные преимущества Log4j:

* Простота использования: Log4j предоставляет простой и понятный API для логирования. Он позволяет логировать сообщения различных уровней, таких как отладочные, информационные, предупреждения, ошибки и другие.
* Гибкая конфигурация: Log4j поддерживает конфигурацию через файлы XML, свойства или программно. Вы можете настроить различные аппендеры (например, консоль, файл, база данных) и уровни логирования для каждого логгера в вашем приложении.
* Поддержка разных форматов сообщений: Log4j позволяет настраивать формат сообщений логов, включая дату, время, уровень логирования, имя логгера и само сообщение. Вы можете определить собственный формат или использовать предварительно определенные шаблоны.
* Поддержка разных целевых систем: Log4j интегрируется с различными целевыми системами, такими как файлы, консоль, базы данных, электронная почта и другие. Вы можете выбрать подходящий аппендер в зависимости от ваших потребностей.

Для того чтобы настроить Log4j нужно установить нужные зависимости, как показана на Рис. 3.10.

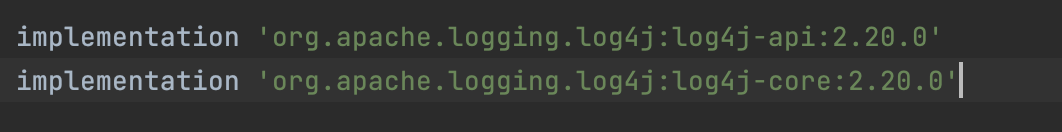


Рис.3.10. Установка зависимостей

Далее, нужно создать конфигурационный файл, чтобы задать параметры логирования.

Рис.3.11. Настройка модуля

### 3.6.5 Разграничение доступа

Разграничение доступа — это процесс установления и контроля уровней доступа к определенным данным, информации или функциональности в системе. Это мероприятие направлено на обеспечение безопасности и защиты данных, а также предотвращение несанкционированного доступа к конфиденциальной информации или чувствительным данным.

В рамках разграничения доступа, обычно устанавливаются различные уровни привилегий или ролей для пользователей или групп пользователей. Каждый уровень доступа предоставляет определенные права и привилегии, определяющие, какие действия или операции может выполнять пользователь в системе.

Ролевая модель разграничения доступа (Role-Based Access Control) — это модель управления доступом, основанная на назначении прав доступа пользователям на основе их ролей в системе. В RBAC каждому пользователю присваивается определенная роль, которая определяет набор разрешений и привилегий, доступных этой роли. Пользователи получают доступ к ресурсам и функциональности системы в соответствии с назначенной им ролью.

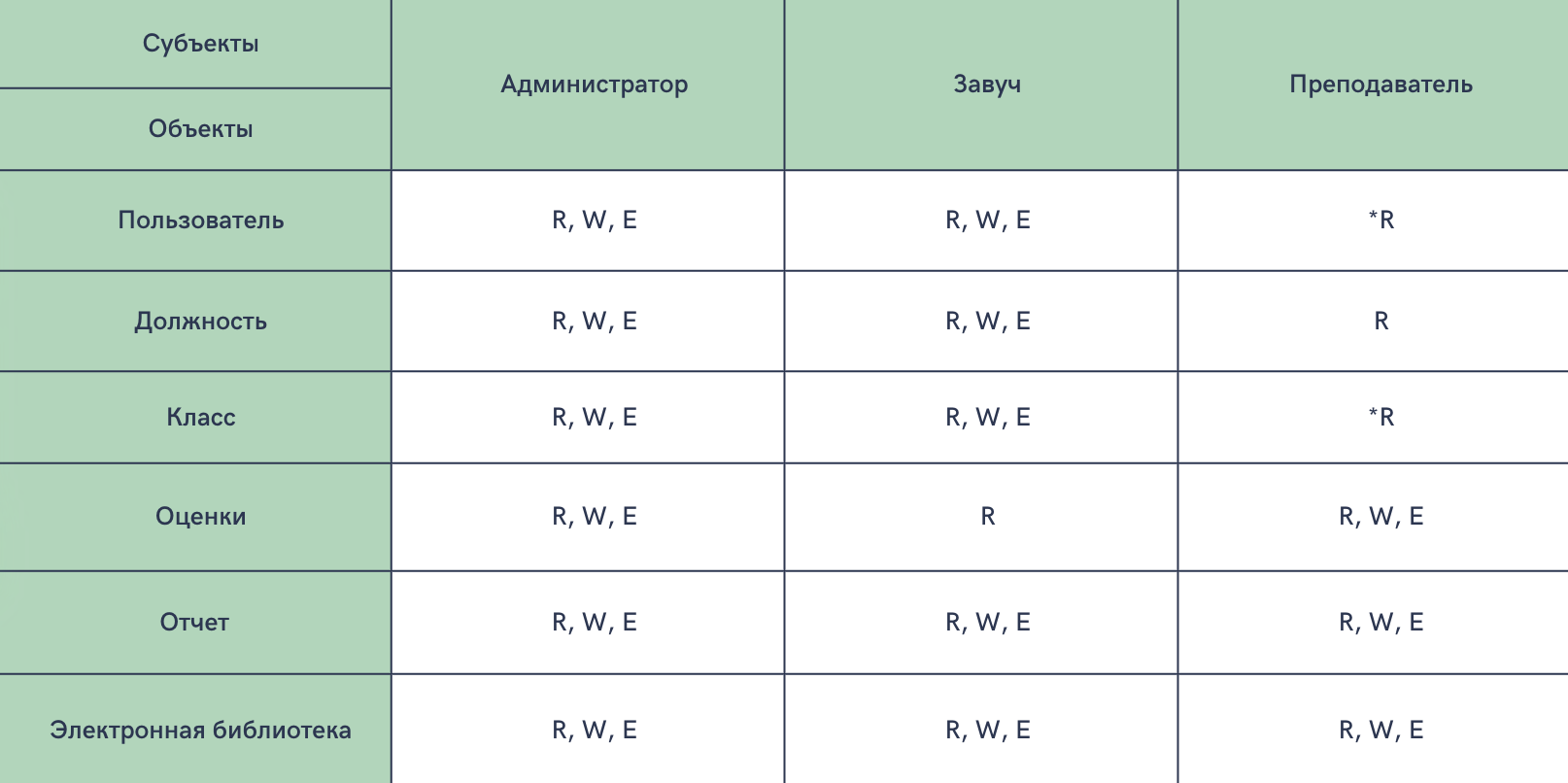


Рис.3.12. Модель разграничения доступа

Обозначения:

* R(read) – чтение объекта
* W(write) – запись объекта
* E(execute) – запись объекта на выполнение
* \* - индивидуальные доступы

**ГЛАВА 4. РАЗРАБОТКА ДОКУМЕНТАЦИИ**

## 4.1 Описание программы

Разрабатываемое веб-приложение предназначено для автоматизации процессов школы.

В системе есть три вида пользователей – администратор, завуч, учитель.

Администратор имеет полный доступ к системе, кроме выставления четвертных оценок. Может создать учетные данные к завучам.

Завуч имеет привилегированный доступ к системе, может: создать классы, учеников, загрузить на сайт расписание уроков и дополнительных занятий, выгрузить отчеты и так далее.

Учитель имеет доступы, такие как, создание профилей для учащихся, загрузка поурочных/годовых планов, выставление четвертных оценок, выгружать книги в портал.

## 4.2 Руководство разработчика

**4.2.1 Назначение и условия применения**

Данная система предназначена для управления проектами по разработке программного обеспечения. Она представляет с собой веб ориентированное приложение с архитектурой Клиент-Сервер.

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 веб-приложения были использованы следующие технологии:

* язык программирования Java от 8 версии;
* фреймворк для создания веб-приложения Spring boot;
* сборщик приложения Gradle;
* система управления базами данных: MySQL;

**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 учеников;
* данные отчетов;
* редактированные персональные данные.

А в качестве выходных:

* список классов;
* список учеников;
* список расписаний;
* список пользователей;
* список достижений;
* список мероприятий;
* 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.

**5.1 DoS атака**

ModSecurity- это бесплатный модуль для Apache с открытым кодом, организующий функции firewall. Он позволяет организовать защиту от большого количества атак против web-сайтов, используя мониторинг и анализ всех запросов в реальном времени

Для этого модуля есть большое число [правил](https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project), написанных сообществом для предотвращения популярных атак

Мы же будем использовать этот модуль для блокирования DDoS атак

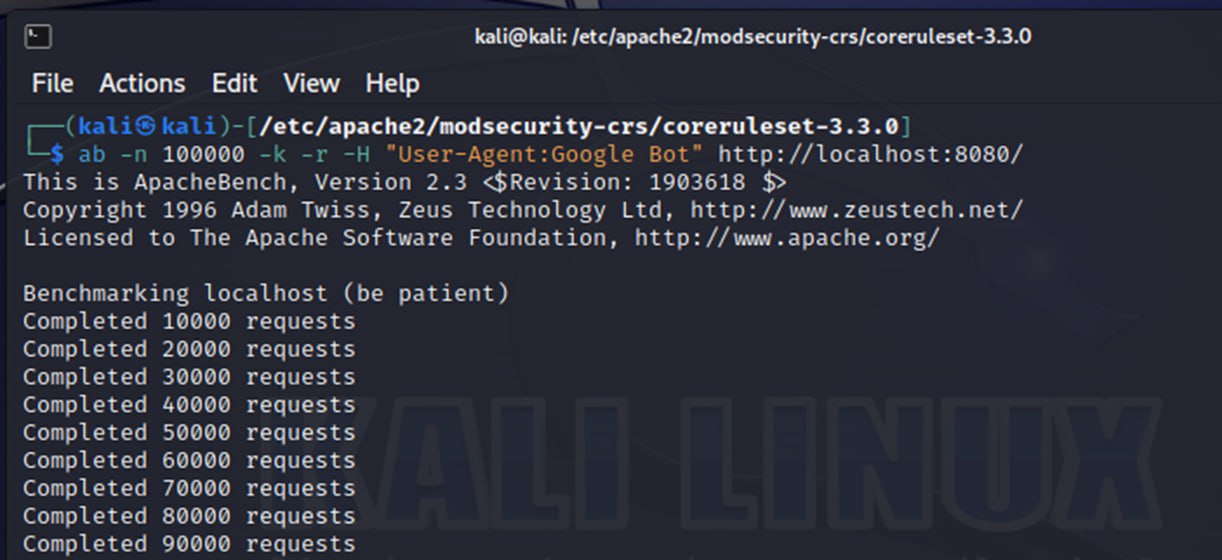
****

Рис.5.1. Отправка запросов. Реализация Dos атаки

На Рисунке 5.2 можно увидеть, что ModSecurity заблокировал запросы. При настройке ModSecurity нужно подключить отдельный модуль, направленный на блокировку таких атак

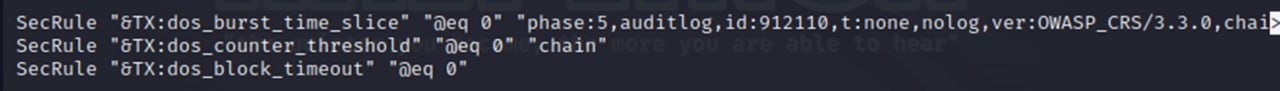
****

Рис. 5.2. Блокировка DoS атаки

**5.2 SQL инъекция**

SQL-инъекция (SQL Injection) — это вид атаки на веб-приложения, при которой злоумышленник внедряет вредоносный SQL-код в строку запроса, предназначенную для выполнения SQL-запросов к базе данных. Целью атакующего является получение несанкционированного доступа к данным или выполнение опасных операций в базе данных.

SQL-инъекции возникают, когда веб-приложения недостаточно проверяют и экранируют пользовательский ввод, прежде чем использовать его в SQL-запросах. Злоумышленник может внедрить вредоносный SQL-код, используя различные методы, включая ввод веб-форм, параметры URL или HTTP-заголовки.

Примеры возможных последствий SQL-инъекций включают:

* Получение доступа к конфиденциальным данным: Злоумышленник может использовать SQL-инъекцию для извлечения, изменения или удаления данных из базы данных. Это может включать получение личных данных пользователей, паролей, финансовой информации и т. д.
* Выполнение несанкционированных операций: Атакующий может использовать SQL-инъекцию для выполнения опасных операций в базе данных, таких как удаление или изменение данных, создание новых учетных записей или даже уничтожение базы данных.
* Обход авторизации и аутентификации: Злоумышленник может использовать SQL-инъекцию для обхода механизмов аутентификации и авторизации, получая доступ к защищенным разделам приложения или выполняя действия от имени других пользователей.

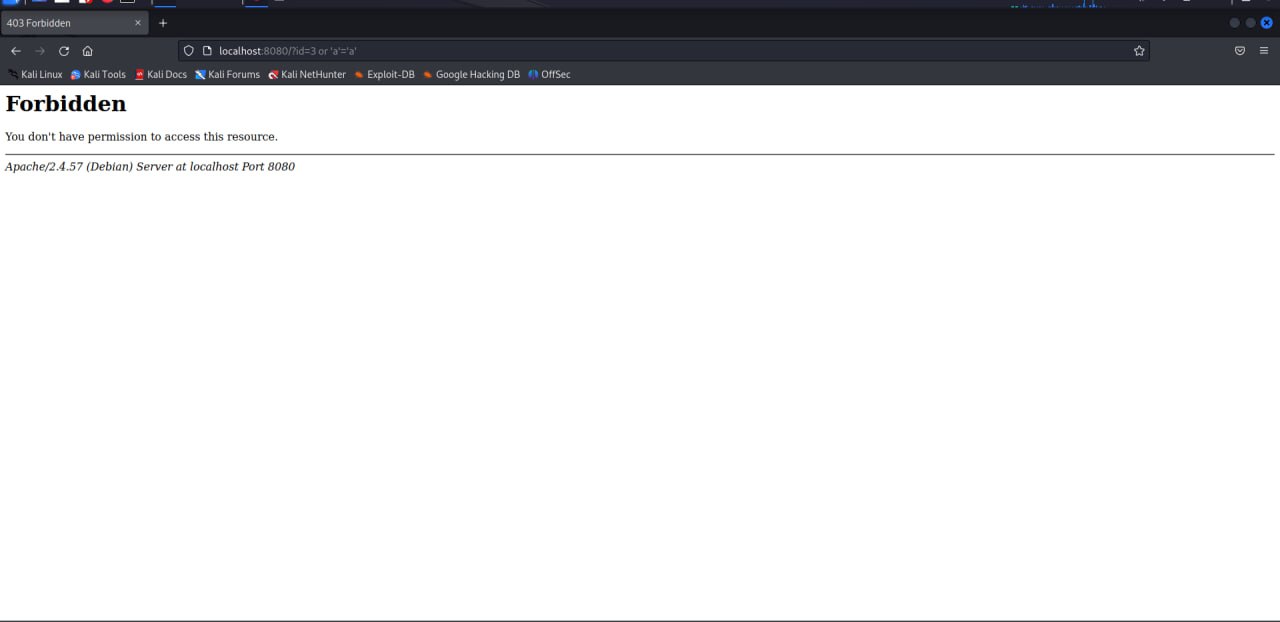


Рис.5.3. Реализация SQL инъекции

На рисунке 5.4. можно увидеть, как, ModSecurity выявил и предотвратил нашу атаку. Также отдельно устанавливается модуль OWASP-TOP10.

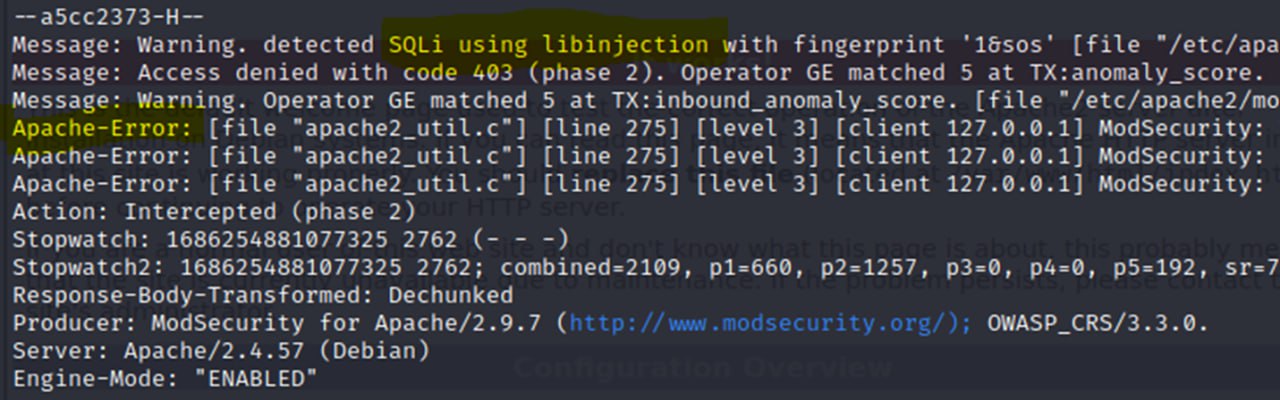


Рис.5.4. Отчет ModSecurity

**ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

БД  
ИА  
ИБ  
ИС  
ИТ  
НСД  
ОЗУ  
ОС  
ПК  
ПО  
ПДн  
СВР угроз ИБ СЗПДн

СЗПД

СКЗ

WAF

TDE

База данных  
Информационный актив  
Информационная безопасность  
Информационная система  
Информационные технологии Несанкционированный доступ  
Оперативное запоминающее устройство Операционная система  
Персональный компьютер  
Программное обеспечение  
Персональные данные  
Степень возможности реализации угроз ИБ Система защиты персональных данных  
Средство криптографической защиты информации

Web-application firewall  
Transparent Data Encryption

**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://start.spring.io/>

8. <https://www.baeldung.com/security-spring>

# **ЗАКЛЮЧЕНИЕ**

Цель выпускной квалификационной работы, которая заключалась в разработке веб-приложения школы, автоматизации ее процессов и обеспечении вокруг нее защиты, была успешно достигнута. В ходе выполнения данной работы были построены диаграммы, проанализированы решения по обеспечению информационной безопасности, по результатам которых были разработаны модели нарушителей, угроз и ограничения доступом, а также проект политики ИБ.

По части работы были выполнены следующие задачи:

* изучена исходная информационная и организационная структура;
* по результатам анализа исходной информационной структуры были определены

конкретные угрозы и уязвимости информационной безопасности;

* разработана модель нарушителя ИБ;
* разработана модель угроз ИБ;
* разработан проект Политики ИБ;
* реализована ролевая модель разграничения доступом;
* разработано приложение;
* разработана двухфакторная аутентификация;
* внедрено хэширование BCrypt;
* web-application firewall;
* шифрование БДMySQL Enterprise Transparent Data Encryption;

# **ПРИЛОЖЕНИЯ**

## ПРИЛОЖЕНИЕ А

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Таблица 1.П-А. Идентификация активов | | | | |
| **Процесс** | **Типы активов** | **Свойства ИБ в порядке приоритета** | **Среда обработки** | **Уязвимость среды** |
| **Информационные активы** | | | | |
| **Регистрация** | Персональные данные  (Паспортные данные, Место работы, Место жительства) | Конфиденциальность  Целостность  Доступность | Spring v5.0 | BDU:2021-00919,  BDU:2021-00717,  BDU:2021-01068 |
| Java v11 | BDU:2021-05969,  BDU:2019-00272,  BDU:2015-00556 |
| Ubuntu Server v18.04 | BDU:2015-09847,  BDU:2015-10386,  BDU:2020-02766 |
| PostgreSQL v11 | BDU:2019-02120,  BDU:2020-05467,  BDU:2021-04174 |
| **Авторизация** | Аутентификационные данные  (логин/пароль) | Конфиденциальность  Целостность  Доступность | Spring v5.0 | BDU:2021-00919,  BDU:2021-00717,  BDU:2021-01068 |
|  |  |  |  |  |
| Продолжение таблицы 1. П-А. Идентификация активов | | | | |
|  |  |  | Java v11 | BDU:2021-05969,  BDU:2019-00272,  BDU:2015-00556 |
| Ubuntu Server v18.04 | BDU:2015-09847,  BDU:2015-10386,  BDU:2020-02766 |
| PostgreSQL v11 | BDU:2019-02120,  BDU:2020-05467,  BDU:2021-04174 |
| **Выставление четвертных оценок** | Данные ограниченного доступа  (данные о успеваемости ученика) | Доступность  Целостность  Конфиденциальность | Spring v5.0 | BDU:2021-00919,  BDU:2021-00717,  BDU:2021-01068 |
| Java v11 | BDU:2021-05969, BDU:2019-00272,  BDU:2015-00556 |
| Ubuntu Server v18.04 | BDU:2015-09847,  BDU:2015-10386,  BDU:2020-02766 |
| PostgreSQL v11 | BDU:2019-02120,  BDU:2020-05467,  BDU:2021-04174 |
|  |  |  |  |  |
| Продолжение таблицы 1. П-А. Идентификация активов | | | | |
| **Хранение данных** | Персональные данные  (все данные) | Конфиденциальность  Целостность  Доступность | PostgreSQL v11 | BDU:2019-02120,  BDU:2020-05467,  BDU:2021-04174 |
| **Электронная библиотека** | Данные открытого доступа  (книги, методички) | Доступность  Целостность  Конфиденциальность | Spring v5.0 | BDU:2021-00919,  BDU:2021-00717,  BDU:2021-01068 |
| Java v11 | BDU:2021-05969,  BDU:2019-00272,  BDU:2015-00556 |
| Ubuntu Server v18.04 | BDU:2015-09847,  BDU:2015-10386,  BDU:2020-02766 |
| PostgreSQL v11 | BDU:2019-02120,  BDU:2020-05467,  BDU:2021-04174 |
|  |  |  |  |  |
| Продолжение таблицы 1. П-А. Идентификация активов | | | | |
| **Нагрузка** | Данные ограниченного доступа  (нагрузка преподавателя, график преподавателя) | Конфиденциальность  Доступность  Целостность | Spring v5.0 | BDU:2021-00919,  BDU:2021-00717,  BDU:2021-01068 |
| Java v11 | BDU:2021-05969,  BDU:2019-00272,  BDU:2015-00556 |
| Ubuntu Server v18.04 | BDU:2015-09847,  BDU:2015-10386,  BDU:2020-02766 |
| PostgreSQL v11 | BDU:2019-02120,  BDU:2020-05467,  BDU:2021-04174 |
| **Отчет** | Данные ограниченного доступа  (отчеты всех видов) | Конфиденциальность  Доступность  Целостность | Spring v5.0 | BDU:2021-00919,  BDU:2021-00717,  BDU:2021-01068 |
| Java v11 | BDU:2021-05969, BDU:2019-00272,  BDU:2015-00556 |
| Ubuntu Server v18.04 | BDU:2015-09847,  BDU:2015-10386,  BDU:2020-02766 |
|  |  |  |  |  |
| Продолжение таблицы 1. П-А. Идентификация активов | | | | |
|  |  |  | PostgreSQL v11 | BDU:2019-02120,  BDU:2020-05467,  BDU:2021-04174 |
| **Поурочный план**  **/----------/**  **Годовой план** | Данные ограниченного доступа  (методическое пособие преподавателя) | Конфиденциальность  Доступность  Целостность | Spring v5.0 | BDU:2021-00919,  BDU:2021-00727,  BDU:2021-01068 |
| Java v11 | BDU:2021-05969,  BDU:2019-00272,  BDU:2015-00556 |
| Ubuntu Server v18.04 | BDU:2015-09847,  BDU:2015-10386,  BDU:2020-02766 |
| PostgreSQL v11 | BDU:2019-02120,  BDU:2020-05467,  BDU:2021-04174 |

## 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 и  веб разработки | 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;  DNS-spoofing |
| 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 |
|  |  |  |  |  |  |  |
| Продолжение таблицы 2. П-Б. Модель нарушителя | | | | | | |
| 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 | Ubuntu Server v21.04 | 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 | PostgreSQL v13 | BDU:2019-01225 | SQL-инъекция. Внедрение  вредоносного SQL-кода в  запросы к информационной  системе | Нарушение целостности и  конфиденциальности |
|  |  |  |  |  |  |  |  |
| Продолжение таблицы 3. П-В. Модель угроз | | | | | | | |
| Межсайтовый  скриптинг XSS | Антропогенный тип Б | Персональные данные и данные ограниченного доступа | Целостность  Конфиденциальность  Доступность | Клиентское приложение | BDU:2020-01895 | Внедрение в выдаваемую веб-системой страницу вредоносного кода, и взаимодействии этого кода с веб-сервером злоумышленника | Нарушение  конфиденциальности  и целостности  системы |
| Повышение  привилегий | Антропогенный  Тип В | Данные ограниченного доступа | Конфиденциальность  Целостность  Доступность | Ubuntu Server v21.04 | BDU:2021-02185, BDU:2020-02766 | Повышение  привилегий —эксплуатация уязвимостей в  операционной системе или  прикладном ПО | Нарушение  конфиденциальности и  целостности |
|  |  |  |  |  |  |  |  |
| Продолжение таблицы 3. П-В. Модель угроз | | | | | | | |
| Кража  аутентификационных данных | Антропогенный  Тип В | Персональные данные | Конфиденциальность  Целостность Доступность | Ubuntu Server v21.04 | BDU:2021-02185, BDU:2020-02766 | Атака человек по середине | Нарушение  конфиденциальности |
| Обход контроля доступа | Антропогенный  Тип Б | Данные ограниченного доступа,  Персональные данные | Доступность  Конфиденциальность  Целостность | Ubuntu Server v21.04 | BDU:2021-02185 | SQL-атака, подмена, URL-адреса | Нарушение конфиденциальности и доступности |

## ПРИЛОЖЕНИЕ Г

**Политика ИБ**

Согласно стандарту ГОСТ Р ИСО/МЭК 17799-2005, политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью.

Политика информационной безопасности – совокупность регламентов, требований, стандартов, рекомендаций, согласно которым ведется профессиональная деятельность конкретной организации, чтобы обеспечить защиту имеющихся у нее информационных ресурсов.

**1. Общие положения**

* 1. Политика информационной безопасности общеобразовательной школы, определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности (далее-ИБ), которыми руководствуются работники школы при осуществлении своей деятельности.
  2. Основной целью Политики информационной безопасности школы является защита информации школы при осуществлении образовательной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в управлении.
  3. Политика информационной безопасности разработана в соответствии с Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным законом от 27 июля 2006г. № 152-ФЗ «О персональных данных», Федеральным законом от 10 января 2002г. № 1-ФЗ «Об электронной цифровой подписи», Указом Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановлением Правительства РФ №781 от 17.11.07г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ №687 от 15.09.08г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также рядом иных нормативных правовых актов в сфере защиты информации.
  4. Ответственность за соблюдение информационной безопасности несет каждый сотрудник организации.

**2. Цель и задачи политики информационной безопасности**

**2.1 Основными целями политики ИБ являются:**

* сохранение конфиденциальности критичных информационных ресурсов;
* обеспечение непрерывности доступа к информационным ресурсам школы;
* защита целостности информации с целью поддержания возможности школы по оказанию услуг высокого качества и принятию эффективных управленческих решений;
* повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами школы;
* определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности. -повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз ИБ;
* предотвращение и/или снижение ущерба от инцидентов ИБ.

**2.2 Основными задачами политики ИБ являются:**

* разработка требований по обеспечению ИБ;
* контроль выполнения установленных требований по обеспечению ИБ;
* повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию ИБ;
* разработка нормативных документов для обеспечения ИБ школы;
* выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ школы;
* организация антивирусной защиты информационных ресурсов школы;
* защита информации школы от несанкционированного доступа (далее-НСД) и утечки по техническим каналам связи;
* организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору школы.

**3. Концептуальная схема обеспечения информационной безопасности**

1. Политика ИБ школы направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников школы, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.
2. Наибольшими возможностями для нанесения ущерба обладает собственный персонал школы. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.
3. Стратегия обеспечения ИБ школы заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников школы.

**4. Основные принципы обеспечения информационной безопасности**

Основными принципами обеспечения ИБ :

* постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов школы;
* своевременное обнаружение проблем, потенциально способных повлиять на ИБ школы, корректировка моделей угроз и нарушителя;
* разработка и внедрение защитных мер;
* контроль эффективности принимаемых защитных мер;
* персонификация и разделение ролей и ответственности между сотрудниками школы за обеспечение ИБ школы исходит из принципа персональной и единоличной ответственности за совершаемые операции.

**5. Объекты защиты**

* + 1. Объектами защиты с точки зрения ИБ в управлении являются:
* информационный процесс профессиональной деятельности;
* информационные активы школы.
  1. Защищаемая информация делится на следующие виды:
* Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его ФИО, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
* другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

**6. Требования по информационной безопасности**

**Для администратора:**

1. Обеспечить разграничение доступа для всех сотрудников
2. Следить за резервным копированием данных
3. Проводить логирование с помощью SIEM систем
4. Проводить аудит
5. Формировать отчет внешних и внутренних актуальных угроз
6. Следить за актуальностью используемых программ в системе.

**Для сотрудников:**

1. В процессе своей работы сотрудники обязаны постоянно использовать режим "Экранной заставки" с парольной защитой. Рекомендуется устанавливать максимальное время "простоя" компьютера до появления экранной заставки не дольше 15 минут.
2. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация школы.
3. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит администратор ЛВС.
4. Сотрудники школы не должны:

* блокировать антивирусное программное обеспечение;
* устанавливать другое антивирусное программное обеспечение;
* изменять настройки и конфигурацию антивирусного программного обеспечения.

1. Использование сотрудниками школы публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации при условии применения механизмов шифрования.
2. Сотрудникам школы запрещается:

* нарушать информационную безопасность и работу сети школы;
* сканировать порты или систему безопасности;
* контролировать работу сети с перехватом данных;
* получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
* передавать информацию о сотрудниках или списки сотрудников школы посторонним лицам;
* создавать, обновлять и распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

1. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

* проинформировать администратора;
* не использовать и не включать зараженный компьютер;
* не подсоединять этот компьютер к компьютерной сети школы до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором.

1. Сотрудники школы для обмена документами должны использовать только свой официальный адрес электронной почты.
2. Рекомендованные правила:

* сотрудникам школы разрешается использовать сеть Интернет только в служебных целях;
* запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;
* работа сотрудников школы с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации школы в сеть Интернет;
* сотрудники школы перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
* запрещен доступ в Интернет через сеть школы для всех лиц, не являющихся сотрудниками школы, включая членов семьи сотрудников.

1. Все программное обеспечение, установленное на предоставленном школой компьютерном оборудовании, является собственностью школы и должно
2. На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

* персональный межсетевой экран;
* антивирусное программное обеспечение;
* программное обеспечение шифрования жестких дисков;

1. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций. В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю.
2. Не допускается при использования электронной почты:

* рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
* рассылка рекламных материалов;
* подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
* поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
* пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим.

1. Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

**7. Управление информационной безопасностью**

* 1. Управление ИБ школы включает в себя:
* разработку и поддержание в актуальном состоянии Политики информационной безопасности;
* разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению ИБ ;
* обеспечение бесперебойного функционирования комплекса средств ИБ;
* осуществление контроля (мониторинга) функционирования системы ИБ;
* оценку рисков, связанных с нарушениями ИБ.

**8. Реализация политики информационной безопасности**

* 1. Реализация Политики ИБ школы осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в управлении.

**9. Порядок внесения изменений и дополнений в политику информационной безопасности**

* 1. Внесение изменений и дополнений в Политику информационной безопасности производится не реже одного раза в три года с целью приведения в соответствие определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

**10. Контроль за соблюдением политики информационной безопасности**

* 1. Текущий контроль за соблюдением выполнения требований Политики информационной безопасности школы возлагается на сотрудника, назначенного распоряжением директора школы.
  2. Директор школы на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.

**11. Пересмотр Политики ИБ**

Положения Политики безопасности требуют регулярного пересмотра и корректировки

не реже одного раза в год. Внеплановый пересмотр Политики безопасности проводится в случае:

* внесения существенных изменений в структуру системы;
* возникновения инцидентов информационной безопасности.

При внесении изменений в положения Политики безопасности учитываются:

* результаты аудита информационной безопасности;
* рекомендации независимых экспертов по информационной безопасности

Рекомендации по Защите информационной безопасности ИС школы. Строго придерживаться политики