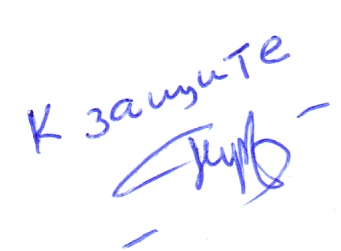
Министерство транспорта Российской Федерации

Федеральное агентство железнодорожного транспорта

ФГБОУ ВО “ДАЛЬНЕВОСТОЧНЫЙ ГОСУДАРСТВЕННЫЙ

УНИВЕРСТИТЕТ ПУТЕЙ И СООБЩЕНИЯ”

14.03.2019

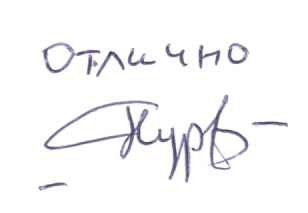
Кафедра: «Информационные технологии

и системы»

ОТЧЕТ

по производственной практике

(по получению профессиональных умений и опыта профессиональной деятельности)

14.03.2019

Студент гр. 25К Буквина Е.А.

Руководитель

доцент, к.т.н. Гурвиц Г.А.

Хабаровск – 2019

СОДЕРЖАНИЕ

[ЗАДАНИЕ 3](#_Toc10574411)

[ХАРАКТЕРИСТИКА 4](#_Toc10574412)

[ПОЯСНИТЕЛЬНАЯ ЗАПИСКА 5](#_Toc10574413)

[ВВЕДЕНИЕ 6](#_Toc10574414)

[1. Нормативно-правовые акты в области защиты информации 8](#_Toc10574415)

[2. Описание информационной системы предприятия 11](#_Toc10574416)

[2.1.Описание функционала используемой платформы 11](#_Toc10574419)

[2.2.Основные структурные характеристики и механизмы функционирования платформы 12](#_Toc10574420)

[2.2.1.Модель данных 12](#_Toc10574421)

[2.2.2.Конфигурации 18](#_Toc10574422)

[2.2.3.Контекст данных 21](#_Toc10574423)

[2.2.4.Отображения и блоки данных 22](#_Toc10574424)

[2.2.5.Описание микросервисной архитектуры платформы 23](#_Toc10574425)

[2.3.Описание взаимодействия компонентов информационной системы предприятия 25](#_Toc10574426)

[2.4.Безопасность данных в информационной системе предприятия 27](#_Toc10574427)

[ДНЕВНИК ПРАКТИКИ 30](#_Toc10574428)

[ЗАКЛЮЧЕНИЕ 34](#_Toc10574429)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 35](#_Toc10574430)

# ЗАДАНИЕ

на производственную (по получению профессиональных умений и опыта профессиональной деятельности) практику для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем»

**Цель практики**: Получение профессиональных умений и опыта профессиональной деятельности по проектированию информационных систем в защищенном исполнении

**Содержание практики:**

* посещение лекций, проводимых представителями ФСТЭК РФ;
* изучение требований к защите информации в информационных системах;
* изучение структурно-функциональных характеристик информационной системы Института дополнительного образования ДВГУПС;
* обоснование создания системы защиты для информационной системы предприятия;
* оформление отчета.

**Примерное содержание отчета по производственной практике (практике по получению профессиональных умений и опыта профессиональной деятельности):**

Оглавление

1. Требования к защите информации в информационных системах
2. Структурно-функциональные характеристики информационной системы Института дополнительного образования ДВГУПС
3. Обоснование создания системы защиты для информационной системы предприятия
4. Дневник практики
5. Список литературы

|  |  |  |
| --- | --- | --- |
| Задание выдано студенту | Буквиной Е.А.\_\_\_\_\_\_\_  (Фамилия И.О.) | группы 25К |
| Руководитель практики | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) | Г.А. Гурвиц |

# ХАРАКТЕРИСТИКА

студента 5-го курса Дальневосточного государственного университета путей сообщения института «Управления, автоматизации и телекоммуникаций» по *специальности «Информационная безопасность автоматизированных систем» Буквиной Екатерины Алексеевны,* проходившей производственную практику с 11.02.2019 по 12.03.2019.

Во время прохождения практики (по получению профессиональных умений и опыта профессиональной деятельности) изучала нормативно-правовую базу в сфере информационной безопасности, описывала основные структурно-функциональные характеристики существующей информационной системы Института дополнительного образования (ИДО) ДВГУПС, в частности, официального сайта организации, анализировала обрабатываемую в системе информацию и на основе полученных данных обосновывала необходимость создания системы защиты для информационной системы предприятия.

Все рекомендуемые нотации, наставления принимала и выполняла на должном уровне, относилась к работе добросовестно. Екатерина показала себя инициативной и способной действовать самостоятельно, продемонстрировала высокий уровень исполнительной дисциплины. За время практики Буквина Е.А. освоила все необходимые для работы теоретические и практические навыки.

Буквина Е.А. овладела следующими компетенциями:

ПК-12 Способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;

ПК-13 Способностью участвовать в проектировании средств защиты информации автоматизированной системы;

ПК-14 Способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

ПК-15 Способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем;

ПК-16 Способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации.

Достигнут 3 уровень (знать, уметь, владеть) оценки показателей владения вышеуказанными компетенциями.

Замечаний по прохождению практики нет.

В целом работу на практике можно оценить самой высокой оценкой.

Руководитель практики,

к.т.н., доцент Гурвиц Г.А.

# ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Я, Буквина Екатерина Алексеевна, студент 5 курса специальности 10.05.03 «Информационная безопасность автоматизированных систем» Дальневосточного государственного университета путей сообщения с 11.02.19 по 12.03.19 проходила производственную практику в Институте дополнительного образования Дальневосточного государственного университета путей сообщения (ИДО ДВГУПС).

На время прохождения практики основной задачей было ознакомление с характеристиками информационной системы организации и закрепление теоретических аспектов информационной безопасности.

При прохождении практики было выполнено следующее:

* изучены законодательные и нормативные акты, государственные стандарты, методические рекомендации по вопросам информационной безопасности;
* описаны особенности используемой для разработки официального сайта предприятия платформы, в частности, модель данных, конфигурации, контекст данных, отображения и блоки данных;
* рассмотрена микросервисная архитектура платформы;
* определена схема взаимодействия основных компонентов информационной системы;
* проанализированы данные, обрабатываемые в информационной системе;
* приведено обоснование необходимости разработки средств защиты информации в рассматриваемой системе.

# ВВЕДЕНИЕ

Сегодня практически вся информация становится электронной, сведения о деятельности компании сосредоточены в информационных системах, электронные коммуникации стали основным видом связи, все чаще используются сетевые бизнес - услуги. По сетевым каналам передается важнейшая коммерческая информация, а в рамках сервисов циркулируют реальные деньги, что создает серьезный мотив для совершения компьютерных преступлений. Поэтому защита информационных активов и управление ими становится актуальной и важной задачей.

На данный момент сформулировано три базовых угрозы информационной безопасности:

* угроза конфиденциальности информации (опасность незаконного разглашения, утечки информации);
* угроза целостности информации (опасность несанкционированной модификации данных, а также их уничтожения);
* угроза доступности информации (опасность отказов в обслуживании).

Реализация хотя бы одной из этих угроз может привести к невозможности нормального функционирования предприятия. С учетом стремительного развития информационного общества, можно сделать вывод о тенденции к росту количества угроз информационной безопасности.

Обеспечение информационной безопасности определяется целым сочетанием предпринимаемых мер. Все эти меры можно разделить на три группы:

– организационные;

– методологические;

– технические меры.

Организационные меры заключаются в формальных процедурах и установлении правил работы с информацией разного уровня критичности, информационными сервисами и средствами защиты. Технические меры включают в себя использование различных программных и аппаратных средств защиты информации. Методологические меры связаны с изменением принципов построения информационного пространства в широком смысле, перегруппировкой информационных потоков, направленных на увеличение отказоустойчивости информационной системы, а также снижение критичности успешной атаки на рабочее место пользователя.

Таким образом, во избежание потерь, вызванных вмешательством в работу информационной системы со стороны злоумышленника, руководству любого предприятия необходимо уделять пристальное внимание вопросу информационной безопасности и реализации совокупности вышеуказанных мер защиты информации.

# Нормативно-правовые акты в области защиты информации

ФЗ-149 «Об информации, информационных технологиях и о защите информации» от 27.07.2006 в достаточно широком смысле трактует понятие информационная система: «информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств». А сайт в сети «Интернет» - совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет" [1].

Говоря простым языком, сайт – это совокупность программ, которые способны обрабатывать запросы от пользователей, приходящие из сети «Интернет», взаимодействовать с информацией, содержащейся в информационной системе (в ее базах данных) и передавать ответ обратно пользователю.

Таким образом, сайт является частью информационной системы. И поскольку основой сайта, как и любой информационной системы, является информация, то и требования к обеспечению безопасности будут похожи.

В пункте 2 статьи 5 [1] указано, что, в зависимости от категории доступа, информация подразделяется на:

* общедоступную информацию;
* информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

При этом пункт 2 статьи 9 ФЗ-149 обязует соблюдать конфиденциальность информации ограниченного доступа.

Это говорит о том, что если на сайте располагается информация, доступ к которой ограничен федеральными законами, то владелец сайта и оператор информационной системы должны позаботиться о том, чтобы доступ к такой информации был предоставлен только лицам, имеющим на это право.

Согласно пункту 1 статьи 16 ФЗ-149, защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Если речь идет об информационных системах общего пользования, которые располагают информацией общего пользования, то, согласно пункту 3 статьи 16 ФЗ-149, требования о защите такой информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 статьи 16 (то есть для достижения целостности и доступности).

В соответствии со статьей 13 ФЗ-149 информационные системы включают в себя:

– государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответствующих федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

– муниципальные информационные системы, созданные на основании решений органов местного самоуправления;

– иные информационные системы [1].

Требования, предъявляемые к защите информации в государственных информационных системах (ГИС) и муниципальных информационных системах (МИС), регламентируются Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Приказом ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Приказ ФСТЭК №17 регламентирует использование сертифицированных средств защиты информации и обязательную аттестацию ИС.

Если в ГИС обрабатываются персональные данные, то, помимо требований Приказа ФСТЭК № 17, необходимо выполнять также требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

Если речь идет о защите персональных данных в негосударственных ИС, требования определяются Постановлением Правительства от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" и Приказом №21 ФСТЭК России от 18.02.2013 №21 "Об утверждении Состава и содержания организационных и технических мер пообеспечению безопасности персональных данных".

Требования, предъявляемые к информационным системам общего пользования, определяются следующими правовыми актами:

* [Приказ Минкомсвязи РФ от 25.08.2009 № 104 "Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования";](http://www.consultant.ru/document/Cons_doc_LAW_92160/)
* Приказ ФСБ РФ № 416, ФСТЭК РФ № 489 от 31.08.2010 "Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования".

Также требования к обеспечению безопасности информации, необходимой для размещения в сети "Интернет" в форме открытых данных, регламентируют:

* пункт 11 Приказа Минкомсвязи России от 27.06.2013 № 149;
* пункт 1 Постановления Правительства РФ от 18.05.2009 № 424;
* пункт 6 Приказа Минэкономразвития России от 16.11.2009 № 470;
* пункт 4 Постановления Правительства РФ от 24 ноября 2009 г. № 953;
* пункт 10 Постановления Правительства РФ от 10 июля 2013 г. № 582.

Таким образом, для обеспечения безопасности информационной системы, частью которой является сайт, необходимо:

* обеспечение безопасности самой информационной системы;
* обеспечение безопасности ИС при подключении ее к сетям общего пользования;
* обеспечение безопасности совокупности программ, которые обеспечивают доступ к информации, содержащейся в ИС, из информационно-телекоммуникационной сети "Интернет" (то есть программ, которые обеспечивают работу сайта).

# Описание информационной системы предприятия



## Описание функционала используемой платформы

Основная цель рассматриваемой платформы – автоматизировать бизнес-процессы предприятия независимо от характера его деятельности. При этом предполагается отказ от найма компании программистов для разработки специализированного программного обеспечения, ориентированного на конкретно заданную предметную область.

Данное SaaS-приложение находится в стадии завершения разработки; оно станет гибким инструментом для эффективной поддержки оперативной деятельности предприятия. Каждый сотрудник сможет настроить приложение под себя, собрав свой «личный кабинет». Простой конструктор позволит формировать данные в табличной, календарной, блочной и любой другой форме с поиском, фильтрами и отчетами.

Приложение даст возможность осуществлять планирование и анализ деятельности, контролировать динамику и эффективность производства, увеличивать рост согласованности действий персонала и качества его работы.

## Основные структурные характеристики и механизмы функционирования платформы

Имеющаяся SaaS-платформа позволяет без знания программирования проектировать бизнес-процессы. Система обеспечивает использование гибкой модели данных (для выстраивания бизнес-логики приложения) и дает инструментарий, позволяющий реализовать бизнес-логику в виде интерфейсов.

### Модель данных

В платформе используется графо-ориентированная модель данных, позволяющая моделировать любые бизнес-процессы через создание классов объектов и фиксацию связей экземпляров (другими словами, в основе проектирования лежит методология нейро-ориентированной организации данных, где в узлах находятся объекты, и между объектами выстраиваются связи). Для этого был применен фрактальный подход построения объектов в рамках табличного отображения данных.

Графо-ориентированная модель данных идеально накладывается на любую документно-ориентированную базу данных, где объекты и связи являются отдельными документами, обеспечивающими связанность данных. В качестве основного подхода в хранении данных было выбрано семейство SQL-баз данных.

Принцип хранения информации реализован без необходимости выстраивания реляционной модели данных с использованием подхода хранения данных в одной таблице (для дальнейшего портирования в другие семейства баз данных, а также реализации собственного in-memory хранилища). Фактически в единой таблице организовано multikey-value хранилище с использованием фрактально-повторяемой модели данных. Такой подход позволил получить необходимую абстракцию модели хранения данных от реализации модели бизнес-процессов.

Поля в хранилище данных представлены в таблице 1.

Таблица 1 – Поля в хранилище данных

|  |  |
| --- | --- |
| Объекты | Описание |
| Uuid | Уникальный идентификатор записи |
| Uid | Уникальный идентификатор сущности |
| Id | Алиас идентификатора сущности |
| Parent | Идентификатор шаблона – родителя, на основании которого был создан объект |
| Source | Идентификатор шаблона, к которому относится данный объект |
| Element | Идентификатор поля |
| Value | Значение поля (для объектов) |
| Src | Идентификатор связанного объекта |
| Tpls | Идентификатор шаблона связанного объекта |
| Type | Тип поля |

Единое multikey-value хранилище позволяет понизить минимальный уровень доступа к данным до уровня поля объекта (атрибута экземпляра класса). Это означает, что данные могут быть изменены различными пользователями в рамках одного объекта в разных полях.

Данный подход позволил реализовать безопасную модель обновления данных как в архитектуре клиент-сервер, так и в одноранговой сети, когда все пользователи являются равноправными участниками.

В целом, для пользователей работа с данными происходит на уровне шаблонов, объектов, полей, запросов. Набор сущностей представлен в таблице 2.

Таблица 2 – Базовые сущности системы

|  |  |
| --- | --- |
| Объекты | Описание |
| Шаблон | Представляет объект шаблона (класс). Содержит перечень полей (атрибутов класса) и идентификационные данные. |
| Объект | Содержит перечень данных в соответствии с полями шаблона-родителя. |
| Поле | Элемент шаблона (атрибут) |
| Запрос | Массив данных в соответствии со сформированной цепочкой запросов и заданными критериями |

Все объекты повторяют свою структуру, и вся логика их взаимосвязи укладывается в наличие связей одного объекта с другими. Доступ к данным сущностям осуществляется через ID данного объекта и подразумевает получение данных в формате JSON.

Шаблоны имеют лишь формальное значение и также являются объектами. Это означает, что общеизвестные паттерны объектно-ориентированной парадигмы тут применимы отчасти. В данном случае не существует наследования в понимании ООП. Объект не есть потомок шаблона, а есть лишь еще один объект, который включает в себя структуру полей, заданную объектом шаблона. Но сама привязка объекта к шаблону широко применяется для удобной классификации объектов при формировании связей.

При создании любого объекта используется набор полей определенных типов, представленных на рисунке 1.

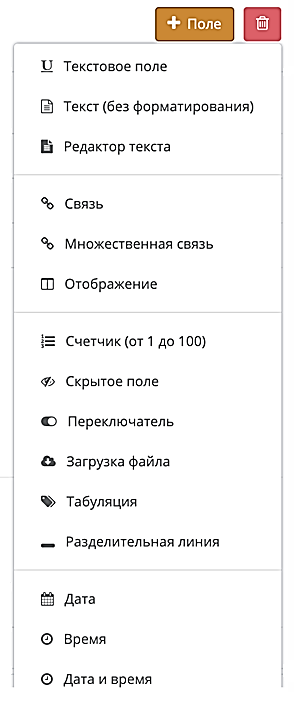
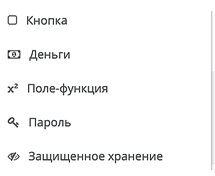


Рисунок 1 - Типы полей

Стоит заметить, что поле также является объектом типа шаблон, позволяющим создать объект своего типа с привязкой к шаблону, на котором данное поле находится.

Каждое поле, в свою очередь, имеет набор атрибутов (полей), которые были созданы при использовании данного поля (в этом, собственно, и заключается фрактальная организация данных; таким образом, все сущности данной системы имеют одинаковую внутреннюю структуру и могут взаимонаследоваться).

Первоначально при создании модели работы с данными в ручном режиме были созданы базовые примитивы (шаблон для создания шаблонов, текстовое поле). Далее, с использованием этих примитивов, были созданы другие объекты полей, которые также применялись для расширения создаваемых объектов. Тем не менее, базовый примитив шаблона сохранился и является первичной формой создания любого объекта шаблона (рисунок 2).

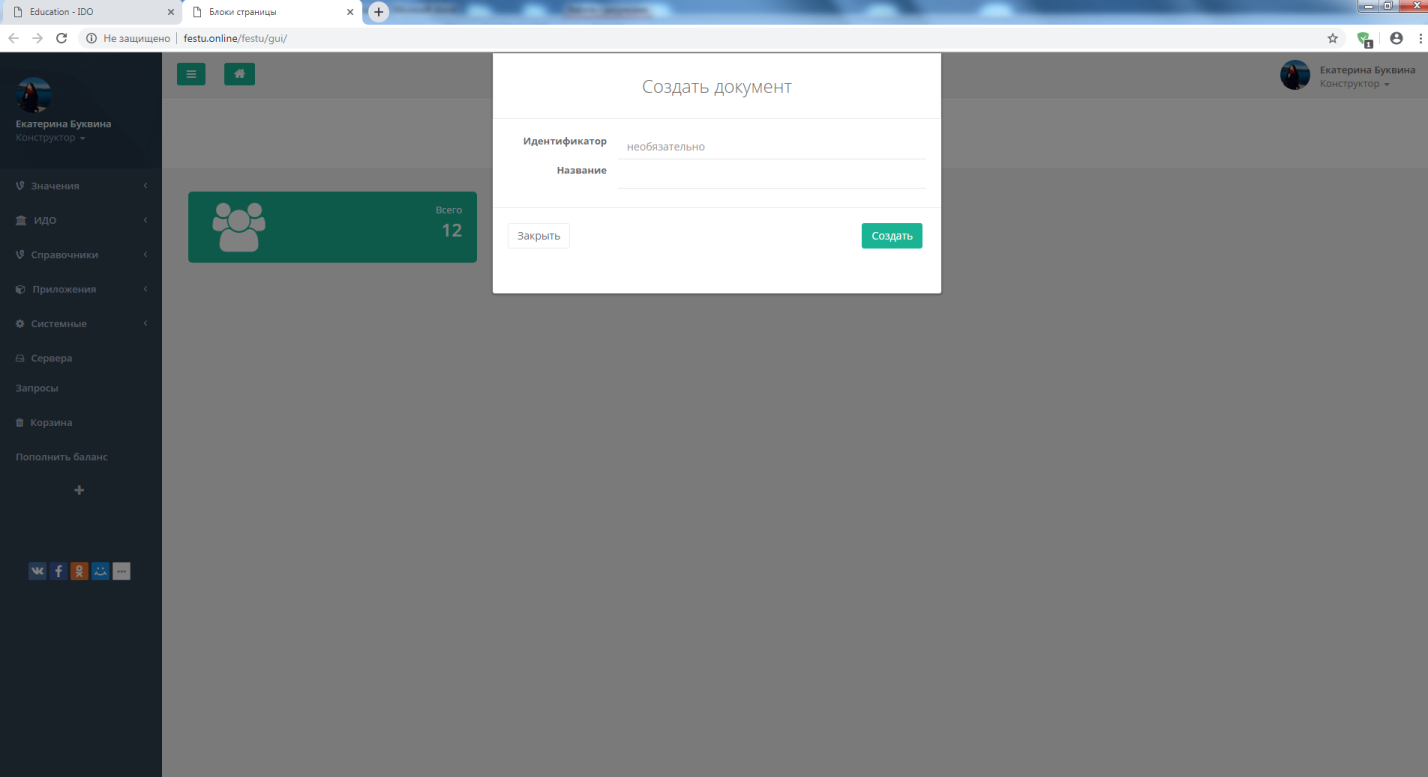


Рисунок 2 - Создание шаблона через базовый примитив

Операции с данными являются однообразными и для объектов, и для шаблонов. Поскольку шаблон также является объектом, он имеет настройки отображения (идентификатор, порядок вывода, разделитель и так далее).

Для редактирования полей шаблона существует специальный шаблон. В данном случае мы можем говорить о том, что один объект может быть создан одним шаблоном, но редактироваться - другим. Пример редактирования полей шаблона поля представлен на рисунке 3.

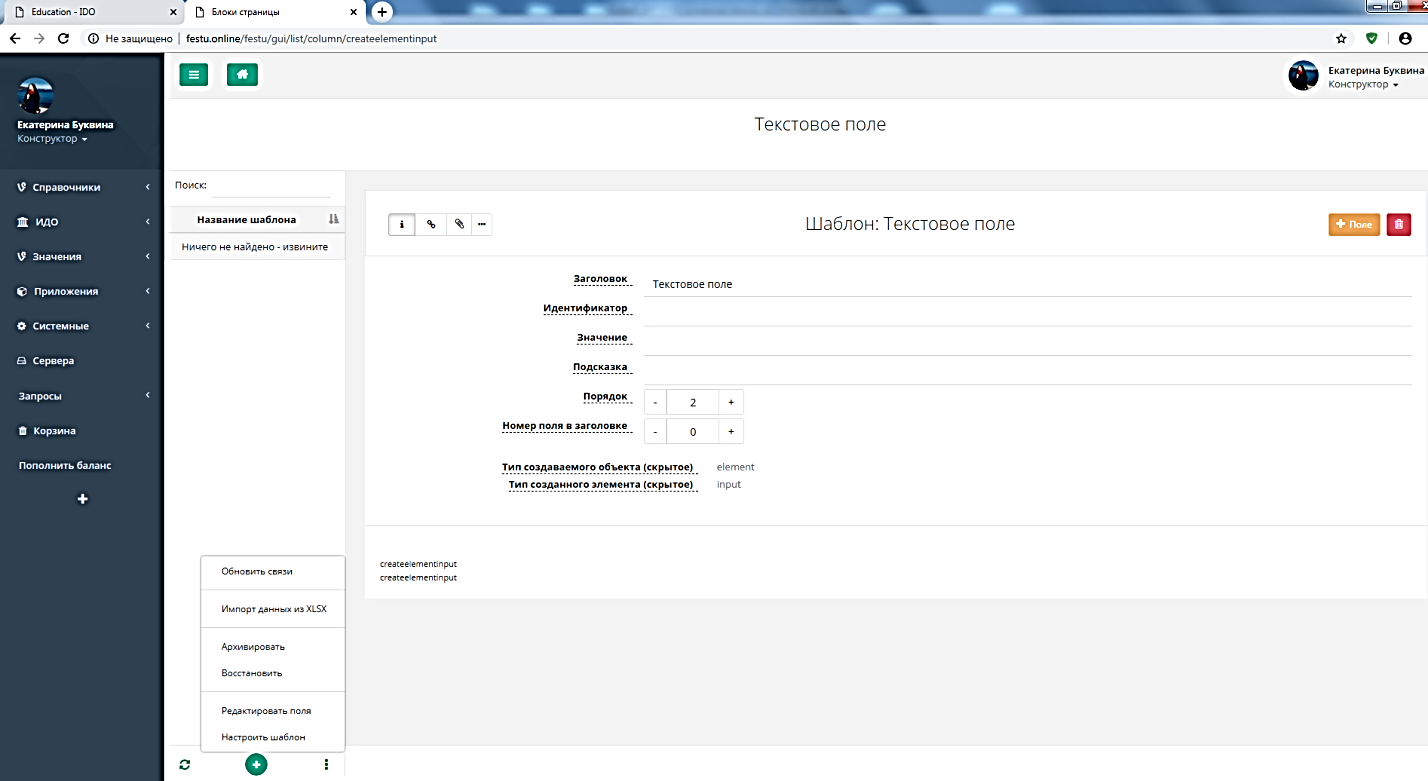


Рисунок 3 - Пример редактирования полей шаблона поля

Также мы можем получить доступ к редактору полей шаблона, находясь в самом режиме редактирования (рисунок 4).

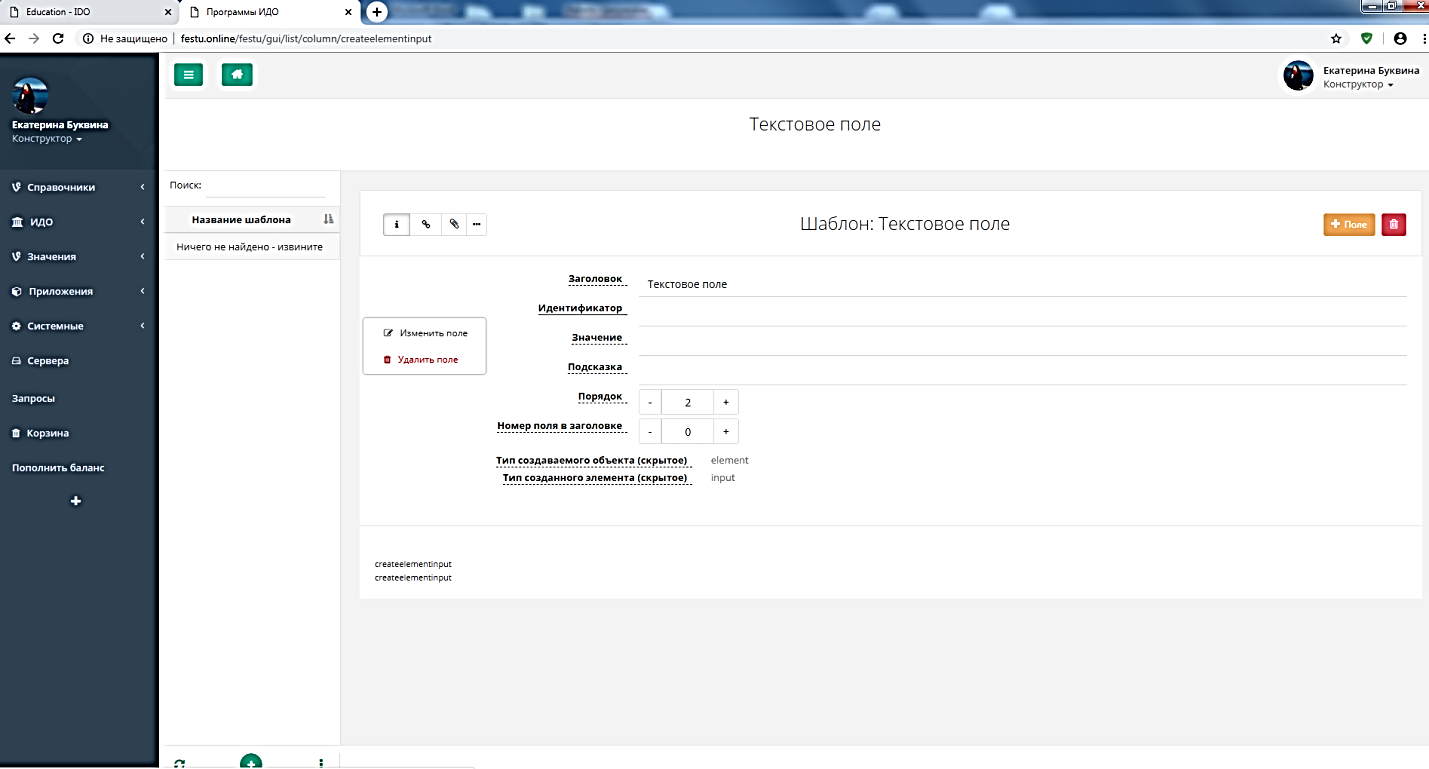


Рисунок 4 - Редактирование атрибутов поля

При редактировании (настройке) созданного при помощи базового примитива шаблона мы имеем уже другой набор полей, более расширенных, в котором часть полей существует, а часть является пустыми. Это происходит потому, что мы открываем созданный объект шаблона другим шаблоном, где наложение наименований полей является запроектированной особенностью группового доступа к одним объектам, но через разные шаблоны (рисунок 5).

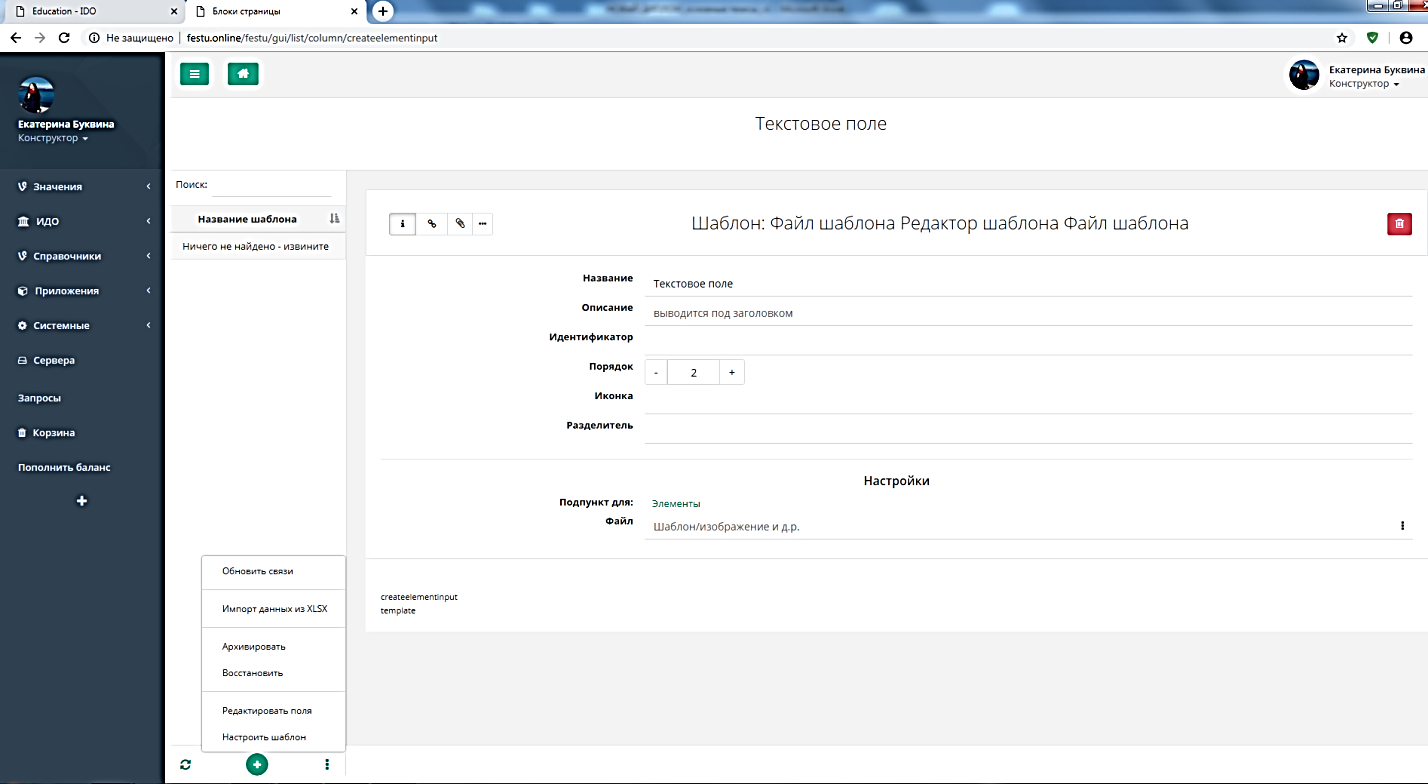
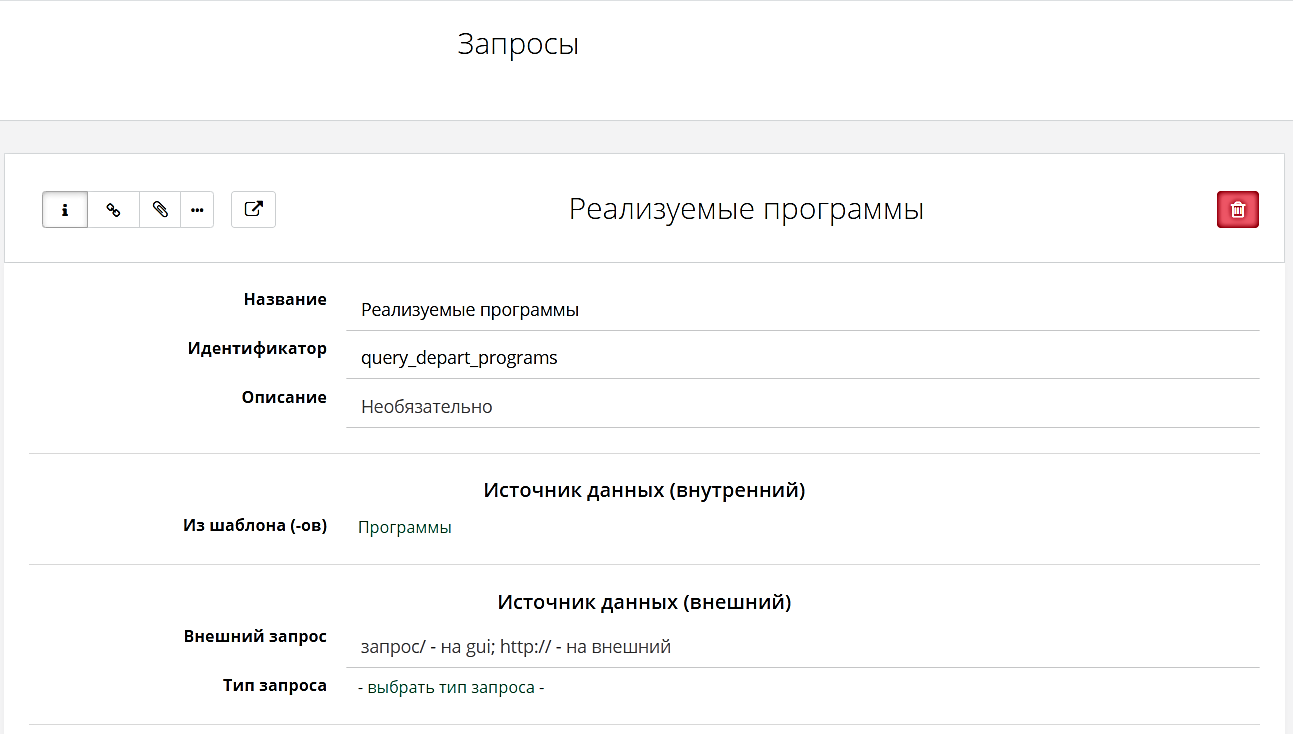
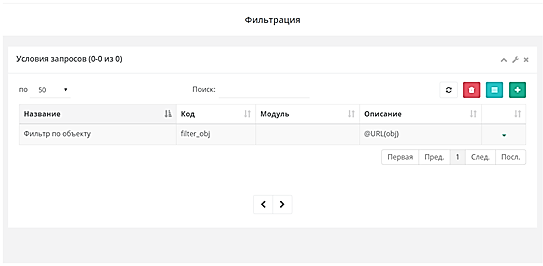


Рисунок 5 - Дополнительные атрибуты шаблона после создания

### Конфигурации

Для вывода информации из базы данных на внешней странице (или в системной консоли) необходимо создать объект запроса, в котором предварительно нужно настроить условия фильтрации и поиска данных (рисунок 6).





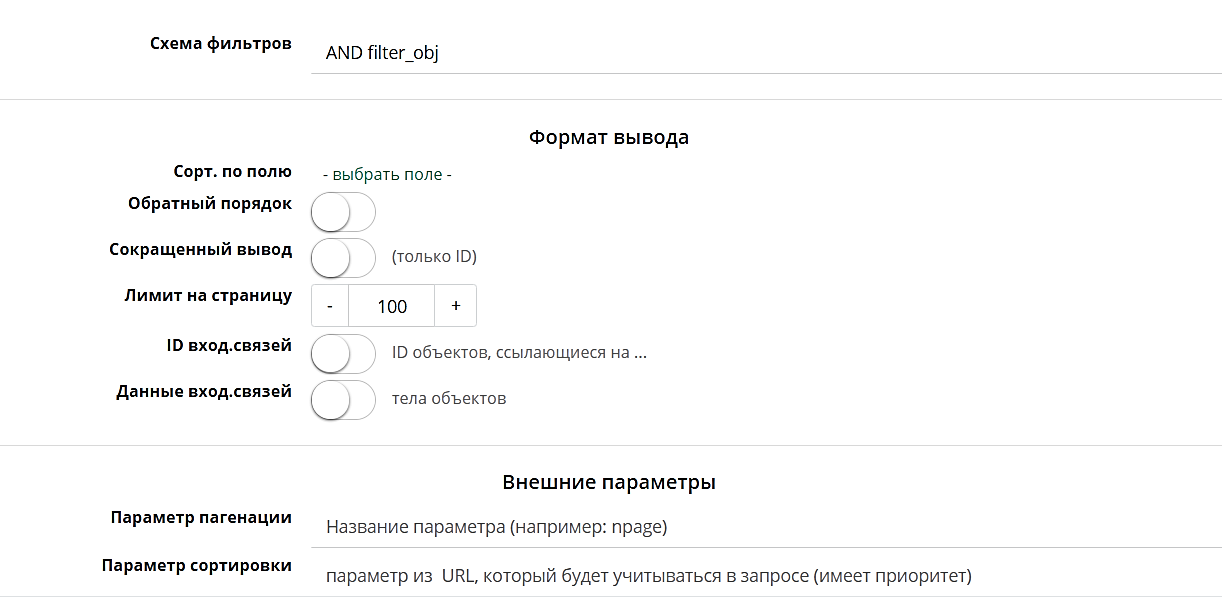


Рисунок 6 - Создание объекта запроса

Далее созданный запрос необходимо выбрать в настройках блока (рисунок 7) или отображения.

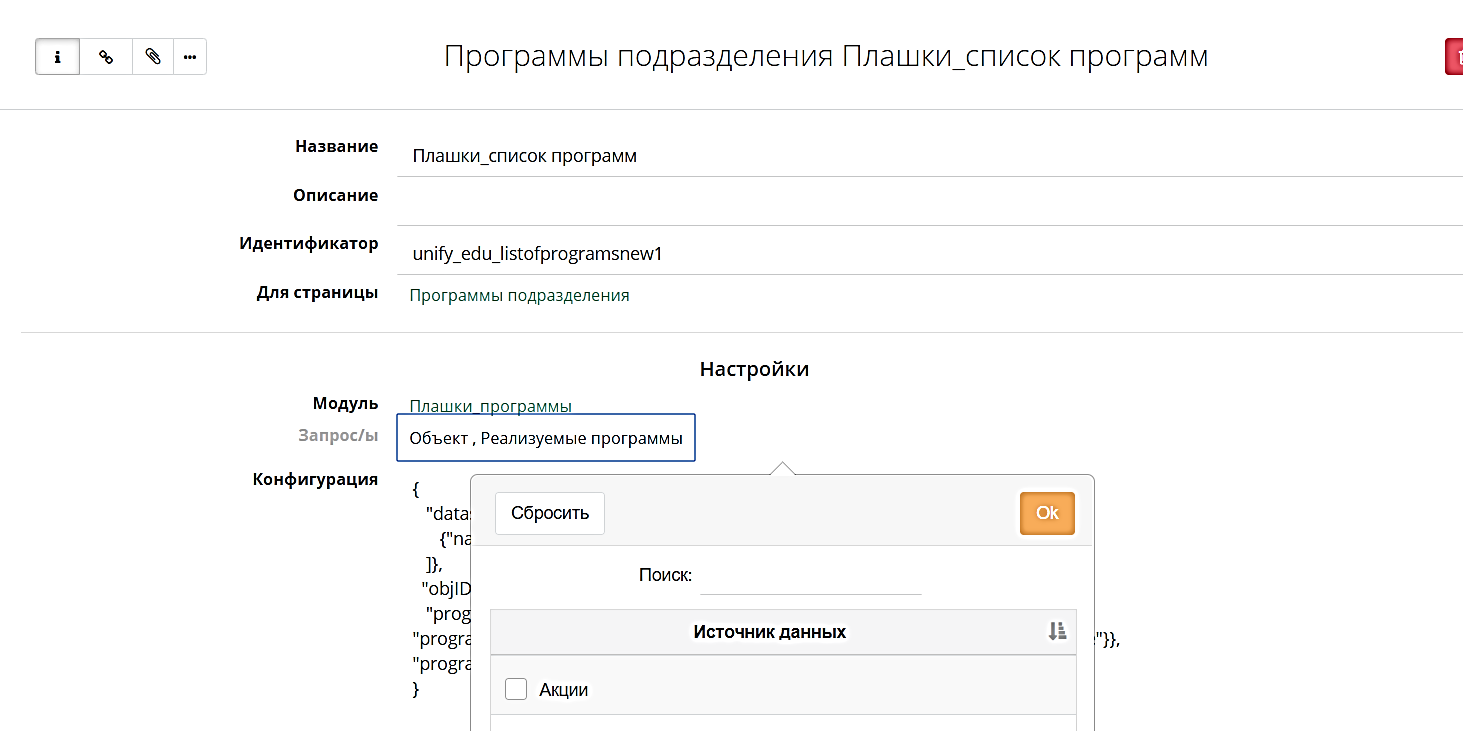


Рисунок 7 - Выбор используемых запросов в настройках блока данных

Если запрос был выбран один, то все данные этого запроса доступны в переменных контекста в переменной ".Data.default.Data" и представляют собой массив объектов запроса.

Если в блоке или отображении необходимо оперировать данными различных запросов, то необходимо отметить требуемые запросы в настройках "галочками".

Данные запросов, отмеченных в настройках блока/отображения, попадают в контекст страницы, и для доступа к ним необходимо произвести именование данных запросов.

В данной реализации необходимо в конфигурации блока/отображения создать раздел "dataset", в котором происходит именование запроса через связывание его идентификатора с именем, где:

* name - имя запроса, по которому его данные будут доступны в контексте;
* uid - идентификатор запроса.

Пример получения массива данных из различных запросов:

{…  
"datasets":{"type":"dataset","source":[  
{"name":"default","uid":"de18b2af-824d-4703-a49d-8808146f450e"},  
{"name":"aucslinks","uid":"8197c7e9-4066-409e-a5fc-623578a16e88"}]}  
...}

### Контекст данных

При обращении к странице происходит ее HTML-генерация (сборка страницы) с использованием полученных из запросов данных, а также ряда системных переменных.

На самом деле, контекст - это всего лишь структура данных с заполненными полями, а именно (точка означает обращение к корню контекста -  самой структуре):

* + - .Value.Host - адрес сайта;
    - .Value.Path - путь текущей страницы;
    - .Value.Prefix - путь к файлам шаблона относительно корня;
    - .Value.Domain - добавочный путь относительно адреса сайта (например, ru/ru);
    - .Value.CDN - путь размещения стилей и скриптов шаблона;
    - .Value.URL;
    - .Value.Rand - случайное шестизначное число;
    - .Value.Referer - адрес предыдущей страницы;
    - .Value.RequestURI - адрес страницы;
    - .Data - структура, содержащая данные запроса/ов:
    - для единичного запроса (на странице используется один запрос) данные находятся по адресу .Data.default.Data;
    - для нескольких запросов данные будут находиться по адресам .Data.Название\_запроса\_указанного\_в\_конфигурации.Data;
* .Configuration - объект конфигурации текущего блока (отображения);
* .Page - объект текущей страницы;
* .Metric - код метрики, указанной в поле "Метрика" в настройках приложения.

### Отображения и блоки данных

Отображение – это такой тип объекта, который может включать в себя разные модули вывода (к примеру, редактор объектов, таблица, тайм-лайн, плитка, календарь). Данный объект включает в себя запрос (данные в формате JSON) и вид, как их показать.

Когда происходит формирование объекта данных, все отображения получают определенную структуру данных (рисунок 8).

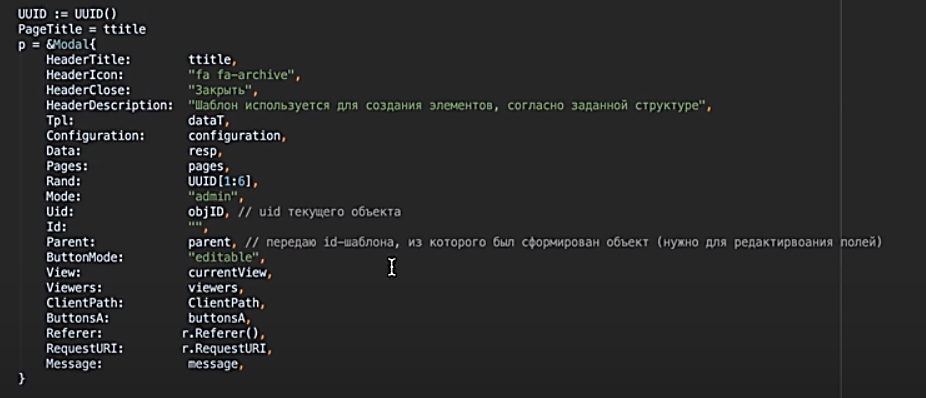


Рисунок 8 - Структура данных отображения

Здесь есть данные о конфигурации, данные о шаблонах, которые использовались в конкретном отображении, собственно сами данные, режим работы, идентификаторы, системные пути, набор кнопок и прочее. Это полный набор данных, который отправляется в шаблон, формирующий отображение. Шаблоном является обычный HTML-документ, который, имея стандартный синтаксис шаблонизации, позволяет взаимодействовать пользователю с данными.

Следует заметить, что отображения применяются только для формирования системной консоли, то есть «личного кабинета» пользователя. При этом есть возможность менять расположение базовых элементов консоли.

Для сборки внешних страниц сайта используются блоки данных, имеющие схожую с отображениями структуру. Разница лишь в том, что отображения используют заранее запроектированные базовые формы представления, а также, в отличие от блоков, могут иметь кнопки управления, модификаторы и триггеры. В блоках данных используются различные модули (типы представления), создаваемые редактором портала.

Разметка (сетка) внешнего сайта проектируется в самом сайте, и при сборке страницы для формирования каждого блока сайт обращается к API приложения, передавая различные параметры (например, какие данные взять и посредством какого модуля их сверстать для показа на сайте). При желании, пользователь может добавлять свои HTML-шаблоны, через которые данные будут выводиться, без необходимости написания кода.

### Описание микросервисной архитектуры платформы

Архитектура платформы включает в себя следующие составляющие:

* веб-приложение;
* RESTful API;
* хранилище данных.

Рассмотрим подробнее каждый из компонентов.

Веб-приложение (BuildBox Application) получает данные из системы через RESTful API, обрабатывает и генерирует веб-страницы. Для этого существует несколько основных элементов:

1. макеты;
2. страницы;
3. модули;
4. блоки.

Веб-приложение можно представить в виде модели проектирования MVC (Модель, Представление, Контроллер), где модели обрабатывают данные, представления показывают результаты и, наконец, контроллеры обрабатывают запросы пользователей.

В системе BuildBox задачи уровня моделей переложены на само ядро системы; разработка и настройка моделей осуществляется через графический интерфейс (BuildBox GUI). На выходе пользователь получает спроектированную модель данных, которая может быть изменена в любой момент времени.

Задачи уровня контроллера  решаются путем настройки запросов (Query) данных (также через BuildBox GUI). Формат полученных данных стандартизован и неизменен для всех без исключения запросов.

Задачи уровня представления (отображения данных пользователю) решаются через запуск отдельного приложения, которое получает данные в стандартизованном формате и генерирует HTML-код на основании шаблонов пользователя.

Далее рассмотрим RESTful API BuildBox, позволяющий пользователю программно получать доступ к данным, хранящимся на SaaS-сервере, при помощи сформированных запросов как внутри приложения, так и с применением внешних сервисов. RESTful - это общие принципы организации взаимодействия приложения/сайта с сервером посредством протокола HTTP.

Все взаимодействие с сервером сводится к 4 основным операциям:

1. получение данных с сервера (в нашем случае в формате JSON);
2. добавление новых данных на сервер;
3. модификация существующих данных на сервере;
4. удаление данных на сервере.

Для каждого типа операции используется свой метод HTTP-запроса:

1. получение данных - GET;
2. добавление данных - POST;
3. модификация данных - PUT;
4. удаление данных - DELETE.

Фактически в REST существует единый интерфейс для запросов, например, к базам данных, что является его важнейшим преимуществом.

Итак, при вызове триггеров и цепочек обработчиков на изменение состояния данных в GUI происходит обращение к API, который, в свою очередь, предоставляет «драйверы» для работы с различными СУБД.

Хранение данных в нашем случае обеспечивают две СУБД – SQLite (data storage, хранит строки полей) и Reindexer (cache, хранит объекты полей). Все запросы на чтение данных обращены к кэшу; остальные типы запросов (добавление, изменение, удаление) обращаются к обеим СУБД одновременно.

## Описание взаимодействия компонентов информационной системы предприятия

Схема взаимодействия основных компонентов рассматриваемой информационной системы приведена на рисунке 9.

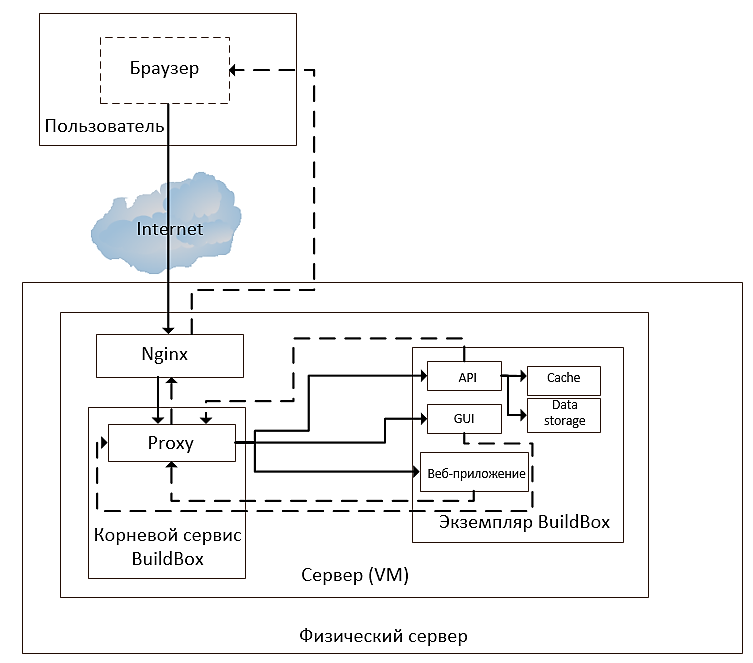


Рисунок 9 - Схема взаимодействия основных компонентов

информационной системы

Запросы от пользователей через публичную сеть поступают на 443-ий TCP-порт сервера, где стартует корневой сервис BuildBox. Полученный запрос обрабатывается прокси-сервером Nginx. Задача последнего заключается в том, чтобы переименовать запрашиваемый адрес путем добавления к нему суффиксов /*доменное имя нижнего уровня*/*ru*. Так, адрес festu.online будет переименован в festu.online/festu/ru.

Обработанный запрос ретранслируется на внутренний прокси-сервис BuildBox, который используется только в корневом сервисе, имеющем соответствующие настройки. В процессе своей работы внутренний прокси опрашивает все запущенные дочерние сервисы и веб-приложения и составляет конфигурацию серверов - JSON-документ, в котором указаны соответствия адресов и портов (рисунок 10).



Рисунок 10 - Карта соответствия адресов и портов

внутреннего прокси-сервиса

Итак, прокси-сервис по суффиксам запроса находит в конфигурации серверов адрес сервера и порт, на который необходимо перенаправить данный запрос.

Ответы от сервисов передаются внутренним прокси обратному прокси-серверу Nginx, после чего возвращаются пользователю.

## Безопасность данных в информационной системе предприятия

Информационная система Института дополнительного образования ДВГУПС содержит как общедоступную информацию (доступ к которой не ограничен), отображаемую на официальном сайте организации, так и информацию ограниченного доступа (доступ к которой ограничен федеральными законами), отображаемую в консоли BuildBox GUI. К общедоступной информации относятся данные о предоставляемых услугах, обучающих центрах, коллективе ИДО, нормативная документация, на основании которой осуществляется образовательная деятельность. Как уже было сказано ранее, в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» статьей 16, появляется необходимость обеспечения защиты информации, если устанавливается достижение любой из целей:

* обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
* соблюдение конфиденциальности информации ограниченного доступа;
* реализация права на доступ к информации [1].

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [5].

Информацией с ограниченным доступом в рассматриваемой информационной системе являются персональные данные слушателей курсов (фамилия, имя, отчество, электронная почта, номер телефона), а также данные всех зарегистрированных в системе пользователей (фамилия, имя, электронная почта, фотография, ссылка на профиль в социальной сети). Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [6]. В соответствии со статьей 9 пунктом 2 ФЗ № 149 («обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами») необходимо обеспечить конфиденциальность информации [1].

Итак, согласно постановлению Правительства РФ № 582 пункту 10 и ФЗ № 149 статье 9 пункту 2, в информационной системе ИДО ДВГУПС необходимо обеспечение защиты информации, а именно:

* обеспечение целостности и доступности для общедоступной информации;
* обеспечение конфиденциальности, целостности и доступности для информации ограниченного доступа.

# ДНЕВНИК ПРАКТИКИ

|  |  |  |
| --- | --- | --- |
| Период | Этап | Результат |
| 12.02.201­9 | Посещение лекций, проводимых представителями ФСТЭК РФ | Получена информация по темам «Классификация иностранных технических разведок», «Объект защиты информации, система защиты информации в организации» |
| 13.02.201­9 | Посещение лекций, проводимых представителями ФСТЭК РФ | Получена информация по темам «Особенности лицензирования видов деятельности в области защиты информации, входящих в компетенцию ФСТЭК России», «Система сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00», «Государственный реестр сертифицированных средств защиты информации», «Классификация и характеристика технических каналов утечки информации (обзор)» |
| 14.02.201­9 | Посещение лекций, проводимых представителями ФСТЭК РФ | Получена информация по темам «Основные цели, функции и права подразделения по защите информации от ИТР и от ее утечки по техническим каналам», «Аттестация объектов информатизации по требованиям безопасности информации» |
| 15.02.201­9 | Посещение лекций, проводимых представителями ФСТЭК РФ | Получена информация по темам «Обеспечение безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», «Обеспечение защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» |
| 19.02.201­9 | Посещение лекций, проводимых представителями ФСТЭК РФ | Получена информация по темам «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» |
| 20.02.201­9 | Посещение лекций, проводимых представителями ФСТЭК РФ | Получена информация по темам «Основы организации защиты информации от несанкционированного доступа. Определение угроз безопасности информации, составление модели угроз», «Техническое задание на создание системы защиты информации государственной информационной системы», «Аттестация по требованиям безопасности информации государственной информационной системы» |
| 21.02.201­9 | Посещение лекций, проводимых представителями ФСТЭК РФ | Получена информация по темам «Требования к содержанию и порядку разработки Руководства по защите информации от ИТР и от ее утечки по техническим каналам в организации», «Сертифицированные средства контроля защищенности информации, средства защиты информации, удовлетворяющие требованиям методических документов ФСТЭК России» |
| 22.02.201­9 | Посещение лекций, проводимых представителями ФСТЭК РФ | Получена информация по темам «Технические каналы утечки информации за счет ПЭМИН», «Технические каналы утечки акустической речевой информации (акустический и вибрационный канал)», «Технические каналы утечки акустической речевой информации (акустоэлектрических преобразований, параметрические каналы: ВЧО, ВЧП, ВЧН)» |
| 23.02.2019 – 26.02.2019 | Изучение нормативно-правовых актов в области защиты информации | Составлен список основных требований к защите информации в информационных системах |
| 27.02.2019 | Ознакомление с функционалом используемой платформы | Описан основной функционал программного обеспечения официального сайта ИДО ДВГУПС |
| 28.02.2018-04.03.2019 | Изучение принципов построения данных в рассматриваемой платформе | Описана модель данных |
| 05.03.2019 – 07.03.2019 | Анализ принципов построения запросов и написания конфигураций блока/отображения данных; изучение принципов работы с контекстом данных | Описаны полученные данные о конфигурациях блоков/отображений данных и контексте данных |
| 08.03.2019 -09.03.2019 | Ознакомление с архитектурой платформы с точки зрения микросервисов | Описана микросервисная архитектура платформы |
| 10.03.2019 – 11.03.2019 | Определение схемы взаимодействия основных компонентов информационной системы, частью которой является сайт ИДО ДВГУПС | Описана схема взаимодействия основных компонентов информационной системы |
| 12.03.2019 | Анализ данных, обрабатываемых в информационной системе ИДО ДВГУПС | Приведено общее обоснование создания системы защиты информации в информационной системе ИДО ДВГУПС на основании требований о защите информации |

# ЗАКЛЮЧЕНИЕ

В ходе прохождения практики были получены профессиональные умения и опыт профессиональной деятельности. Получены теоретические навыки разработки информационной системы в защищенном исполнении в результате ознакомления с нормативно-правовыми актами и государственными стандартами. Были подробно изучены особенности функционирования информационной системы, частью которой является официальный сайт Института дополнительного образования ДВГУПС. В конечном итоге был получен общий вывод о необходимости создания системы защиты информации в рассматриваемой информационной системе в соответствии с требованиями о защите информации.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федер. закон от от 27.07.2006 № 149-ФЗ, ред. от 18.03.2019 – Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_61798/, свободный. – Загл. с экрана.
2. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс]: приказ ФСТЭК РФ от 11.02.2013 №17 – Режим доступа: http://fstec.ru/component/attachments/download/567, свободный. – Загл. с экрана.
3. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: постановление Правительства РФ от 01.11.2012 № 1119 – Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_137356/, свободный. – Загл. с экрана.
4. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: приказ ФСТЭК РФ от 18.02.2013 №21 – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21, свободный. – Загл. с экрана.
5. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006 [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/gost-r-50922-2006, свободный. – Загл. с экрана.
6. О персональных данных [Электронный ресурс]: федер. закон от от 27.07.2006 № 152-ФЗ, ред. от 31.12.2017 – Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_61801, свободный. – Загл. с экрана.
7. Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети "Интернет" и обновления информации об образовательной организации [Электронный ресурс]: постановление Правительства РФ от 10.07.2013 № 582 – Режим доступа: https://rg.ru/2013/07/22/sait-site-dok.html, свободный. – Загл. с экрана.