МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Южно-Уральский государственный университет»
(национальный исследовательский университет)
Факультет Вычислительной математики и информатики
Кафедра системного программирования

РАБОТА ПРОВЕРЕНА

Рецензент
заместитель директора по ИТ и ИБ
ГБУЗ «ЧОМИАЦ»
_____ А.С. Староверов
“23” мая 2016 г.

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой, д.ф.-м.н.,
профессор
_____ Л.Б. Соколинский
“09” июня 2016 г.

Разработка системы автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
ЮУрГУ – 010300.62.2016.12-011-1881.ВКР

Научный руководитель
к.ф.-м.н., ст. преп. кафедры СП
_____ Е.В. Иванова

Автор работы,
студент группы ВМИ-401
_____ А.Н. Лычагов

Ученый секретарь
(нормоконтролер)
_____ О.Н. Иванова
“23” мая 2016 г.

Челябинск-2016

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Южно-Уральский государственный университет»
(национальный исследовательский университет)
Факультет Вычислительной математики и информатики
Кафедра системного программирования

УТВЕРЖДАЮ
Зав. кафедрой СП
_____ Л.Б. Соколинский
09.02.2016

ЗАДАНИЕ
на выполнение выпускной квалификационной работы бакалавра
студенту группы ВМИ-401
Лычагову Александру Николаевичу,
обучающемуся по направлению
010300.62 «Фундаментальная информатика и информационные технологии»

1. **Тема работы** (утверждена приказом ректора от 15.04.2016 № 661)

Разработка системы автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ»

2. **Срок сдачи студентом законченной работы:** 05.06.2016.

3. **Исходные данные к работе**

3.1. Регламент работы Удостоверяющего и ключевого центра ГБУЗ «Челябинский областной медицинский информационно-аналитический центр». – Челябинск: ГБУЗ «Челябинский областной медицинский информационно-аналитический центр», 2015. – 20 с.
3.2. Чан У., Биссекс П., Форсье Д. Django. Разработка веб-приложений на Python. – СПб.: Символ-Плюс, 2009. – 456 с.
3.3. Лутц М. Программирование на Python. 4-е изд. – СПб.: Символ-Плюс, 2011. – 992 с.

4. **Перечень подлежащих разработке вопросов**

4.1. Ознакомиться с регламентом работы Удостоверяющего и ключевого центра ГБУЗ «Челябинский областной медицинский информационно-аналитический центр».
4.2. Выполнить обзор существующих решений по автоматизации отделов, занимающихся информационными технологиями.

4.3. Спроектировать и реализовать систему автоматизации деятельности отдела информационной безопасности ГБУЗ «Челябинский областной медицинский информационно-аналитический центр».
4.4. Протестировать работу системы.

5. Дата выдачи задания: 09.02.2016.

Научный руководитель

Ст. преп. кафедры СП, к.ф.-м.н. Е.В. Иванова

Задание принял к исполнению А.Н. Лычагов

Студент: Лочалов Александр Николаевич ВММ-401

ФИО, группа

Руководитель: к.ф.-м.н. Иванова Елена Владимировна

Ученая степень, ФИО

Тема: Разработка системы автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ»

Календарный план
выполнения выпускной квалификационной работы (ВКР) бакалавра

№ п/п	Этап	Длительность	Срок сдачи	Отчетность	Дата выполнения	Подпись научного рук-ля
1.	Введение и обзор литературы	1 месяц	25 февраля	1. Задание на выполнение ВКР 2. Текст введения. 3. Список литературы.	25.02.16	
2.	Разработка модели, проектирование системы	1 месяц	15 марта	Текст гл. 1 (теоретическая часть).	15.03.16	
3.	Программная реализация системы	1 месяц	15 апреля	1. Программная система. 2. Текст гл. 2 (реализационная часть).	15.04.16	
4.	Тестирование и отладка системы, эксперименты	2 недели	1 мая	1. Набор тестов. 2. Текст гл. 3 (экспериментальная часть).	1.05.16	
5.	Компоновка текста ВКР	2 недели	15 мая	Полный текст ВКР.	15.05.16	
6.	Проверка текста работы научным руководителем	1 неделя	22 мая	Электронная версия текста ВКР, проверенного научным руководителем.	22.05.16	
7.	Нормоконтроль	3 дня	25 мая	Переплетенный текст ВКР, подписанный студентом, научным руководителем и нормоконтролером.	23.05.16	
8.	Предзащита	1 неделя	25 мая … 1 июня	1. Переплетенный текст ВКР, подписанный студентом, научным руководителем и нормоконтролером для подписи зав. кафедрой о допуске к защите. 2. Отзыв на ВКР, подписанный научным руководителем. 3. Рецензия на ВКР, подписанная рецензентом и заверенная по месту его работы (если рецензент не является сотрудником ЮУрГУ). 4. Акт(ы) о внедрении программной системы (при наличии). 5. Презентация доклада в PowerPoint.		

ОГЛАВЛЕНИЕ

Введение 6
1. Обзор существующих решений и технологий 9
1.1. Обзор существующих решений 9
1.2. Обзор платформ для построения веб-приложений 10
1.3. СУБД для информационных систем 11
1.4. Вывод 13
2. Анализ предметной области 14
2.1. Термины и определения 14
2.2. Описание бизнес-процессов 14
2.3. Требования к системе 18
2.3.1. Функциональные требования 18
2.3.2. Нефункциональные требования 22
2.3.3. Варианты использования системы 22
2.3.4. Детализация прецедентов 23
2.4. Вывод 26
3. Проектирование 27
3.1. Паттерн проектирования. Особенности MVC в Django 27
3.2. Компоненты системы 28
3.3. Концептуальная схема БД 29
3.4. Вывод 30
4. Реализация 31
4.1. Модели в системе 31
4.2. Реализация представлений 32
4.3. Генерация заявления 33
4.4. Реализация автоматической проверки паспортов 34
4.5. Реализация интерфейса. Bootstrap 34
4.6. Вывод 36
5. Тестирование 37
5.1. Функциональное тестирование 37
5.2. Юзабилити-тестирование 38
5.3. Тестирование пользовательского интерфейса 38

5.4. Вывод 38
Заключение 39
Список литературы 40
Приложения 42
Приложение 1 42
Приложение 2 44
Приложение 3 46
Приложение 4 47
Приложение 5 49
Приложение 6 51
Приложение 7 53
Приложение 8 54
Приложение 9 56
Приложение 10 57
Приложение 11 61

ВВЕДЕНИЕ

Актуальность

В настоящее время отдел информационной безопасности ГБУЗ «ЧОМИАЦ» ведет работу в нескольких направлениях, одно из которых – учет, выдача и внесение изменений в дистрибутивы ключей для подключения к ведомственной сети передачи данных средств криптографической защиты информации ViPNet [8]. Для каждого учреждения заводится картонная папка, в которой хранятся документы по этому учреждению: договор, заявления, приказы и т.п. Все документы набираются в формате MS Word, печатаются и хранятся только в бумажном виде. В рамках каждого учреждения создаются несколько пользователей (порядка 10 в среднем). По каждому пользователю хранится следующая информация: бумажные копии паспорта и СНИЛС, справка с места работы, согласие на обработку персональных данных. Информация по каждому пользователю хранится в отдельной картонной папке. Связь между учреждением и пользователем можно установить на основании заявлений пользователей, которые хранятся в папке учреждения. При такой организации отсутствует возможность быстрого поиска необходимого документа, ответы на запросы пользователей оформляются вручную, что занимает много времени.

Таким образом актуальной является задача разработки системы автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ».

Цель и задачи работы

Целью данной работы является разработка системы автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ». Разрабатываемая система предназначена для упрощения выдачи и учета средств криптографической защиты информации, организации работы отдела информационной безопасности ГБУЗ «ЧОМИАЦ» в целом. Система должна предоставлять пользователям возможность оперативного поиска

по документам, внесения изменений в существующие, генерации сопроводительных писем и другие.

Для достижения данной цели необходимо решить следующие задачи:

1) ознакомиться с Регламентом работы Удостоверяющего и ключевого центра ГБУЗ «ЧОМИАЦ»;

2) изучить существующие решения по автоматизации отделов, занимающихся информационными технологиями;

3) спроектировать и реализовать систему автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ»;

4) протестировать работу системы.

Структура и объем работы

Работа состоит из введения, пяти глав, заключения, библиографии и приложений. Объем работы составляет 63 страницы, объем библиографии – 23 источника.

В первой главе дается обзор существующих технологий построения информационных систем и решений, реализующих автоматизацию как предприятия в целом, так и отделов, занимающихся информационными технологиями. В этом разделе рассмотрены платформы для разработки веб-приложений и выявлены наиболее перспективные из них.

Вторая глава содержит описание бизнес-процессов, реализуемых отделом информационной безопасности ГБУЗ «ЧОМИАЦ», описание и анализ требований к системе.

В третьей главе описано проектирование системы автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ». В этом разделе подробно рассмотрены проектирование базы данных, компоненты приложения.

Четвертая глава посвящена реализации системы с использованием фреймворка Django и базы данных MySQL.

В пятой главе представлены результаты тестирования разработанной системы.

В заключении кратко приведены результаты работы.

Приложения содержат образцы документов, предоставляемых в ГБУЗ «ЧОМИАЦ», образец сопроводительного письма, выдаваемого пользователям, JSON Schema заявления, набор тестовых данных, спецификацию тестовых случаев.

1. ОБЗОР СУЩЕСТВУЮЩИХ РЕШЕНИЙ И ТЕХНОЛОГИЙ

На сегодняшний день существует ряд решений, предлагающих автоматизацию деятельности как предприятия в целом, так и конкретно отделов, занимающихся информационными технологиями. В этом разделе рассмотрены некоторые из них.

1.1. Обзор существующих решений

1С:Предприятие [10]. Система программ «1С:Предприятие» включает в себя платформу и прикладные решения, разработанные на ее основе, для автоматизации деятельности организаций и частных лиц. Для использования в конкретном учреждении необходимо разработать конфигурацию, учитывающую специфику работы и бизнес-процессов в этом учреждении. Помимо этого, имеет высокую цену. Окно редактирование конфигурации в программе 1С:Предприятие приведено на рис. 1.

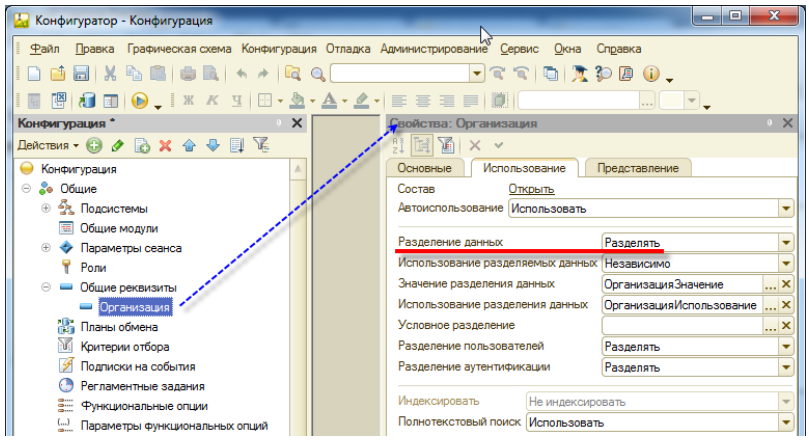

Рис. 1. Окно программы 1С:Предприятие

Программный комплекс: «Аристотель»: Автоматизация работы информационной службы и технического отдела [18]. Предназначен для автоматизации деятельности подразделений информационных технологий, и ориентирован в первую очередь на руководителей ИТ-подразделений малого и среднего бизнеса, но также может использоваться для решения определенных задач и в рамках более крупных организаций. Система обладает большим функционалом, однако для достижения поставленных целей подходит не полностью. Окно редактирования заявки (инцидента)

приведено на рис. 2.

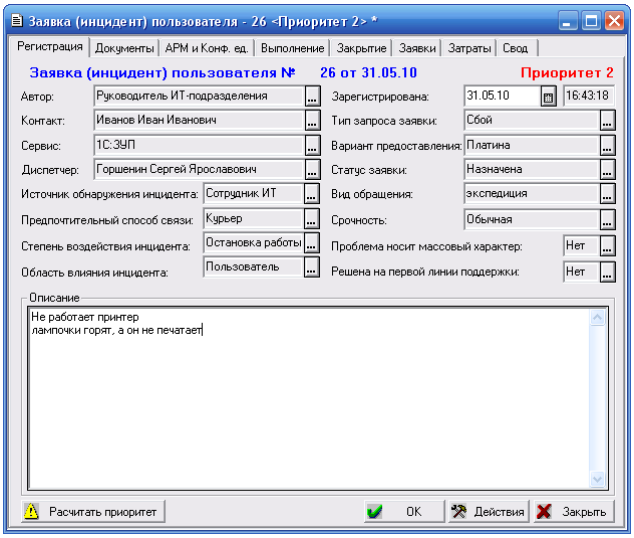

Рис. 2. Программный комплекс: «Аристотель»: Автоматизация работы информационной службы и технического отдела

1.2. Обзор платформ для построения веб-приложений

ASP.NET [22]. Это технология создания веб-приложений и веб-сервисов от компании Майкрософт. Она является составной частью платформы Microsoft .NET и развитием более старой технологии Microsoft ASP. На данный момент последней версией этой технологии является ASP.NET 5.

PHP [16]. PHP (от англ. *PHP* – Hypertext Preprocessor) – скриптовый язык программирования общего назначения, интенсивно применяющийся для разработки веб-приложений. В настоящее время он поддерживается подавляющим большинством хостинг-провайдеров и является одним из лидеров среди языков программирования, применяющихся для создания динамических веб-сайтов (по данным «TIOBE Programming Community Index») [7].

Node.js [1]. Программная платформа, основанная на движке V8 (транслирующем JavaScript в машинный код), превращающая JavaScript из узкоспециализированного языка в язык общего назначения. Node.js добавляет возможность JavaScript взаимодействовать с устройствами ввода-

вывода через свой API (написанный на C++), подключать другие внешние библиотеки, написанные на разных языках, обеспечивая вызовы к ним из JavaScript-кода. Node.js применяется преимущественно на сервере, выполняя роль веб-сервера. В состав Node.js входит собственный установщик пакетов *npm*.

Django (Python) [11, 21]. Свободный фреймворк для веб-приложений на языке Python, использующий шаблон проектирования MVC. Первоначальная разработка Django, как средства для работы новостных ресурсов, достаточно сильно отразилась на его архитектуре: он предоставляет ряд средств, которые помогают в быстрой разработке веб-сайтов информационного характера. Так, например, разработчику не требуется создавать контроллеры и страницы для административной части сайта, в Django есть встроенное приложение для управления содержимым, которое можно включить в любой сайт, сделанный на Django, и которое может управлять сразу несколькими сайтами на одном сервере.

Ruby on Rails (Ruby) [20]. Фреймворк, написанный на языке программирования Ruby. Ruby on Rails предоставляет архитектурный образец Model-View-Controller (модель-представление-контроллер) для веб-приложений, а также обеспечивает их интеграцию с веб-сервером и сервером базы данных. Предоставляет механизмы повторного использования, позволяющие минимизировать дублирование кода в приложениях (принцип *Don't repeat yourself*). По умолчанию используются соглашения по конфигурации, типичные для большинства приложений (принцип *Convention over configuration*). Явная спецификация конфигурации требуется только в нестандартных случаях.

1.3. СУБД для информационных систем

Выбор системы управления баз данных (СУБД) является одним из важных этапов при разработке приложений, обеспечивающих работу со структурированными данными. Выбранный программный продукт должен удовлетворять как текущим, так и будущим потребностям предприятия,

при этом следует учитывать финансовые затраты на приобретение необходимого оборудования, самой системы, разработку необходимого программного обеспечения на ее основе, а также обучение персонала. На сегодняшний день существует большое количество вариаций систем управления базами данных, различающихся архитектурой, размером, применимостью, количеством пользователей и возможностью одновременной работы с БД. Среди корпоративных СУБД наиболее популярны, следующие, применяющиеся в крупных компаниях с достаточно большим количеством пользователей: Oracle, MS SQL Server, DB2, MySQL, PostgreSQL.

Oracle Database [12]. Это объектно-реляционная система, поддерживающая некоторые технологии, реализующие объектно-ориентированный подход, то есть обеспечивающие управление созданием и использованием баз данных. Ключевыми возможностями являются: Real Application Cluster (обеспечивает работу одного экземпляра базы данных на нескольких узлах grid, позволяя управлять нагрузкой и гибко масштабировать систему в случае необходимости), Automatic Storage Management (позволяет автоматически распределять данные между имеющимися ресурсами систем хранения данных), Real Application Testing (позволяет значительно снизить затраты на проведение плановых изменений в конфигурации) и другие. Хорошо подходит для больших систем.

PostgreSQL [5]. Это объектно-реляционная система управления базами данных (СУБД), которая имеет традиционные возможности коммерческих СУБД с расширениями, которые есть в СУБД нового поколения. PostgreSQL – это свободное и полностью открытое программное обеспечение. Сильными сторонами PostgreSQL считаются: высокопроизводительные и надежные механизмы транзакций и репликации, расширяемая система встроенных языков программирования. В стандартной поставке поддерживаются PL/pgSQL, PL/Perl, PL/Python и PL/Tcl, наследование, легкая расширяемость.

MySQL [23]. Это одна из самых популярных и самых распространен-

ных СУБД (система управления базами данных) в интернете. Она не предназначена для работы с большими объемами информации, но ее применение идеально для интернет-сайтов и веб-приложений, как небольших, так и достаточно крупных. MySQL отличатся хорошей скоростью работы, надежностью, гибкостью. Работа с ней, как правило, не вызывает больших трудностей. Поддержка сервера MySQL автоматически включается в поставку такого языка, как PHP.

1.4. Вывод

После анализа существующих проектов было решено реализовывать собственную систему по следующим причинам:

- специфичный алгоритм работы отдела информационной безопасности ГБУЗ «Челябинский областной медицинский информационно-аналитический центр»;
- неполный функционал существующих решений, их высокая стоимость и необходимость доработки.

Для реализации веб-приложения была выбрана платформа Django [11, 21] с использованием в качестве хранилища базы данных MySQL, поскольку данный подход базируется на свободно-распространяемых продуктах и хорошо подходит для реализации веб-систем с небольшим объемом хранимых данных.

2. АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

2.1. Термины и определения

СКЗИ, криптосредство – средство криптографической защиты информации.

ВСПД – VPN, построенный между УЗ ЧО, с использованием СКЗИ ViPNet [8] для обеспечения защиты передаваемой информации.

УКЦ – Удостоверяющий и ключевой центр.

Дистрибутив ключей – файл с расширением *.dst, создаваемый в программе «ViPNet Удостоверяющий и ключевой центр» или «ViPNet Manager» для каждого пользователя сетевого узла ViPNet. В этом файле помещены адресные справочники, ключевая информация и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Связь (доступ к ресурсу) – связь между сетевыми узлами ViPNet своей сети и доверенной сети, определяющая возможность обмена защищенными IP-пакетами.

2.2. Описание бизнес-процессов

ГБУЗ «Челябинский областной медицинский информационно-аналитический центр» занимается обслуживанием защищенной сети передачи данных, используемой медицинскими организациями Челябинской области для доступа к различным информационным сервисам. Процесс подключения к сети можно условно разделить на несколько этапов.

1. Между ГБУЗ «Челябинский областной медицинский информационно-аналитический центр» и организацией, желающей подключиться к ВСПД должен быть заключен договор присоединения к регламенту работы Удостоверяющего и ключевого центра ГБУЗ «Челябинский областной медицинский информационно-аналитический центр» (приложение 1). Вся дальнейшая работа по изготовлению дистрибутивов ключей ведется на основании этого договора. Договор заключается до прекращения деятельно-

сти УКЦ или до расторжения Администратором УКЦ или по соглашению сторон.

2. Назначенный приказом в учреждении пользователь средства криптографической защиты информации должен предоставить в ГБУЗ «Челябинский областной медицинский информационно-аналитический центр» для регистрации лично или через представителя следующий набор документов: согласие на обработку персональных данных (приложение 2), оригинал и копию паспорта гражданина Российской Федерации (копия заверяется пользователем средства криптографической защиты информации), оригинал и копию страхового свидетельства обязательного пенсионного страхования (копия заверяется пользователем средства криптографической защиты информации), оригинал справки с места работы (приложение 3).

При обращении через представителя представитель пользователя предоставляет согласие на обработку своих персональных данных, оригинал и копию паспорта гражданина Российской Федерации (копия заверяется представителем пользователя средства криптографической защиты информации), оригинал справки с места работы, а также документы, необходимые для регистрации пользователя средства криптографической защиты информации на основании полученной от пользователя средства криптографической защиты информации Доверенности на совершение юридически значимых действий в Удостоверяющем и ключевом центре (приложение 4).

3. Пользователь средства криптографической защиты информации для получения дистрибутива ключей для подключения к ведомственной сети передачи данных Министерства здравоохранения Челябинской области предоставляет в Удостоверяющий и ключевой центр оригинал заявления на изготовление дистрибутива ключей для подключения к ведомственной сети передачи данных Министерства здравоохранения Челябинской области (приложения 5, 6), а также копию приказа «О назначении пользователя средства криптографической защиты информации» (копия

заверяется руководителем учреждения) (приложение 7).

4. ГБУЗ «Челябинский областной медицинский информационно-аналитический центр» осуществляет проверку указанных сведений. Проверка полномочий руководителя учреждения осуществляется с использованием официальных ресурсов Федеральной налоговой службы Российской Федерации http://egrul.nalog.ru/ и https://service.nalog.ru/uwsfind.do путем запроса выписки из Единого государственного реестра юридических лиц, а также изучения сведений о юридических лицах, в отношении которых представлены документы для государственной регистрации, в том числе для государственной регистрации изменений, вносимых в учредительные документы юридического лица, и внесения изменений в сведения о юридическом лице, содержащиеся в Едином государственном реестре юридических лиц.

Проверка паспорта гражданина Российской Федерации осуществляется с использованием официального ресурса Федеральной миграционной службы Российской Федерации http://services.fms.gov.ru/info-service.htm?sid=2000 путем запроса информации о действительности паспорта.

5. По результатам проведения проверки достоверности указанных в предоставленных для идентификации и получения дистрибутива ключей для подключения к ведомственной сети передачи данных Министерства здравоохранения Челябинской области сведениях должностным лицом Удостоверяющего и ключевого центра выносится решение о выдаче дистрибутива ключей или отказе в выдаче дистрибутива ключей.

В настоящий момент все вышеуказанные действия осуществляются вручную, информация хранится на бумажных носителях, что не дает возможности быстрого поиска необходимой информации.

Диаграмма деятельности по изготовлению дистрибутива ключей представлена на рис. 3.

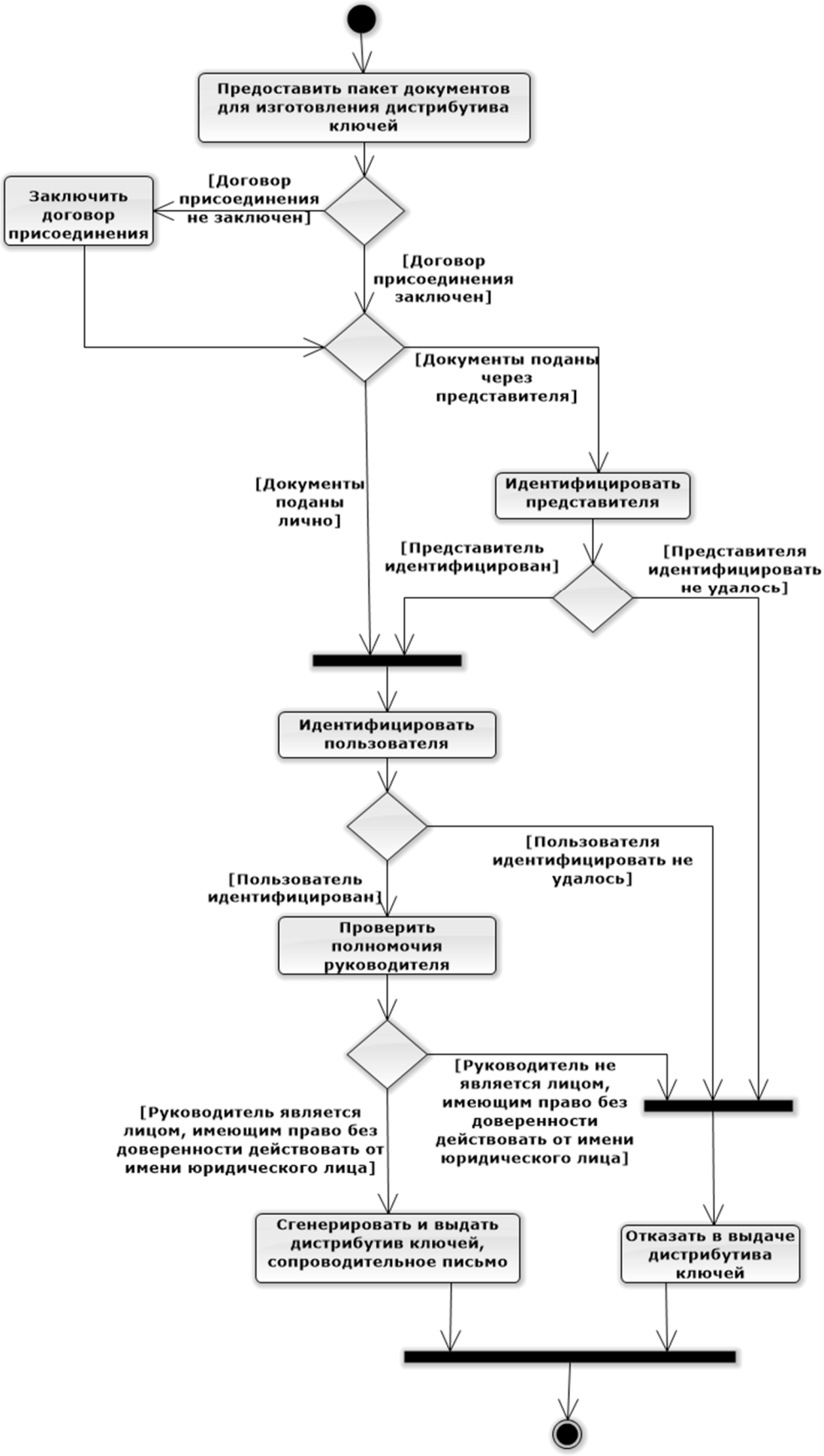

Рис. 3. Диаграмма деятельности по изготовлению дистрибутива ключей

2.3. Требования к системе

2.3.1. Функциональные требования

Система должна обеспечивать аутентификацию и авторизацию пользователя по логину и паролю.

Система должна предоставлять возможность добавления и дистрибутива ключей редактирования договора присоединения к Регламенту работы Удостоверяющего и ключевого центра ГБУЗ «ЧОМИАЦ» любому сотруднику отдела информационной безопасности.

Система должна запрашивать следующие данные для добавления нового договора присоединения: номер и дата регистрации, файл со скан-копией договора присоединения, полное и краткое название организации, с которой заключен договор, ее ИНН, ОГРН, почтовый адрес (индекс, район, населенный пункт, улица, дом), скан-копия свидетельства о постановке на учет юридического лица в налоговом органе по месту нахождения на территории Российской Федерации, выписку из Единого государственного реестра юридических лиц на текущую дату (необязательно).

После регистрации пользователь должен быть переадресован на страницу просмотра информации о зарегистрированном договоре присоединения.

В случае, когда выписка из ЕГРЮЛ не представлена при регистрации, на странице просмотра информации о договоре присоединения в отдельном фрейме должна быть отображена форма сведений о государственной регистрации юридических лиц, индивидуальных предпринимателей, крестьянских (фермерских) хозяйств с сайта ФНС, в которую пользователь вносит данные и получает файл с выпиской из ЕГРЮЛ. Эту выписку система должна сохранить в базе данных.

Система должна осуществлять разбор выписки из ЕГРЮЛ (файл в формате *.pdf) с целью установления текущего лица, имеющего право без доверенности действовать от имени юридического лица.

На странице просмотра информации о договоре присоединения

должны отображаться значения всех полей из формы регистрации.

Система должна хранить и отображать архив старых выписок из ЕГРЮЛ на странице просмотра информации о договоре присоединения.

Система должна хранить и отображать архив старых сведений о регистрации юридических лиц из ЕГРЮЛ на странице просмотра информации о договоре присоединения.

На странице просмотра информации о договоре присоединения должен отображаться список всех заявлений от этого учреждения и сопроводительных писем, выданных этому учреждению.

На странице просмотра списка всех договоров каждый договор должен быть представлен гиперссылкой на соответствующую страницу просмотра договора с текстом следующего содержания: «Договор №_ от __.__.____ г. с <краткое наименование организации>».

Система должна предоставлять возможность регистрации физического лица любому сотруднику отдела информационной безопасности.

При регистрации физического лица система должна запрашивать разную информацию в зависимости от того, является ли лицо пользователем средства криптографической защиты информации или представителем пользователя. Если лицо является пользователем, то предоставляет ли оно документы лично, или через представителя.

При регистрации пользователя средства криптографической защиты информации, подающего документы лично, система должна запрашивать следующую информацию: ФИО, фамилия в родительном падеже, инициалы, пол, должность, адрес электронной почты, телефон, номер страхового номера индивидуального лицевого счета и его скан-копия; серия и номер паспорта, дата, место выдачи, место регистрации, скан-копия первого разворота паспорта и разворота с местом регистрации; дата оформления согласия на обработку персональных данных и его скан-копия.

При регистрации пользователя средства криптографической защиты информации, подающего документы через представителя, система должна

запрашивать следующую информацию: ФИО, фамилия в родительном падеже, инициалы, пол, должность, адрес электронной почты, телефон, номер страхового номера индивидуального лицевого счета и его скан-копия; серия и номер паспорта, дата, место выдачи, место регистрации, скан-копия первого разворота паспорта и разворота с местом регистрации; дата оформления согласия на обработку персональных данных и его скан-копия, дата выдачи доверенности на совершение юридически значимых действий в УКЦ ГБУЗ «ЧОМИАЦ», учреждение, представитель (выбор из списка уже зарегистрированных или регистрация нового), скан-копия доверенности.

При регистрации представителя пользователя средства криптографической защиты информации система должна запрашивать следующую информацию: ФИО, фамилия в родительном падеже, инициалы, должность, серия и номер паспорта, дата, место выдачи, место регистрации, скан-копия первого разворота паспорта и разворота с местом регистрации; дата оформления согласия на обработку персональных данных и его скан-копия.

На странице просмотра информации о физическом лице должны отображаться значения всех полей из соответствующей формы регистрации.

На странице просмотра информации о пользователе средства криптографической защиты информации должен отображаться список всех заявлений, выданных сопроводительных писем и дистрибутивов ключей, связанных с этим пользователем.

Каждый день система должна проверять паспорта зарегистрированных физических лиц на наличие в списке недействительных (утраченных (похищенных), оформленных на утраченных (похищенных) бланках паспорта гражданина Российской Федерации, выданных в нарушение установленного порядка, а также признанных недействительными) паспортов граждан Российской Федерации, удостоверяющих личность гражданина

Российской Федерации на территории Российской Федерации.

Система должна предоставлять возможность регистрации заявлений любому сотруднику отдела информационной безопасности.

При добавлении заявления на изготовление или изменение дистрибутива ключей для подключения к ведомственной сети передачи данных Министерства здравоохранения Челябинской области система должна запрашивать следующую информацию: учреждение, с которым заключен договор присоединения, пользователь средства криптографической защиты информации, тип средства криптографической защиты информации (ViPNet Client / ViPNet Coordinator Windows / ViPNet Coordinator Linux / ViPNet Coordinator HW100A / ViPNet Coordinator HW100B / ViPNet Coordinator HW100C / ViPNet Coordinator HW1000), номер, адрес расположения, скан-копия приказа о назначении пользователя средства криптографической защиты информации, перечень информационных систем, к которым предоставляется доступ (медицинская информационная система, система бухгалтерского учета, система кадрового учета, регистр онкологических больных, медицинское освидетельствование иностранных граждан, паспорт ЛПУ, льготное лекарственное обеспечение граждан, журнал госпитализации в ГБУЗ «ЧОКБ», сервисы ТФОМС), скан-копия заявления.

После заполнения полей регистрации система должна проверить актуальность справки пользователя (не более 3 дней) и его паспортных данных, соответствие организации и пользователя, указанных в справке, данным, полученным при регистрации, актуальность доверенности, если пользователь подает документы через представителя (не более 3 месяцев), соответствие организации, указанной в доверенности, данным, полученным при регистрации, актуальность справки представителя и его паспортных данных.

После добавлении заявления на изготовление дистрибутива ключей и проведения соответствующих работ в Удостоверяющем и ключевом центре ГБУЗ «ЧОМИАЦ» пользователю должна быть предоставлена возмож-

ность формирования сопроводительного письма (приложение 8) к выдаваемому дистрибутиву, а именно: автоматически подставлять данные организации и пользователя, тип средства криптографической защиты информации, формировать номер выданного дистрибутива ключей, генерировать фразу для информирования УКЦ ГБУЗ «ЧОМИАЦ» о компрометации ключей.

Система должна предоставлять пользователю средства криптографической защиты информации автоматически формировать заявление, заполнив следующие поля: организация, ИНН, ОГРН, тип заявления, реквизиты договора присоединения, реквизиты средства криптографической защиты информации, реквизиты приказа о назначении пользователя средства криптографической защиты информации, данные пользователя. Система формирует и выдает пользователю pdf-файл с заявлением, на котором находится QR-код, содержащий введенную информацию в формате JSON. Никакие данные на сервере не сохраняются.

Система должна предоставлять возможность сканирования QR-кода из заявления и автоматического заполнения полей заявления.

2.3.2. Нефункциональные требования

Система должна быть реализована в виде веб-приложения.

Веб-приложение должно корректно работать и отображаться в браузерах Chrome версии 45 и выше, Mozilla Firefox версии 40 и выше, Microsoft Edge версии 20 и выше, Opera версии 12 и выше.

2.3.3. Варианты использования системы

В результате анализа требований заказчика было определено 3 актера, взаимодействующих с системой автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ».

Пользователь СКЗИ – пользователь системы со стороны медицинской организации, который может формировать заявление на изготовление или внесение изменений в дистрибутив ключей.

Сотрудник отдела информационной безопасности – пользователь

системы со стороны ГБУЗ «ЧОМИАЦ», который может осуществлять добавление договоров присоединения к регламенту работы удостоверяющего и ключевого центра, заявлений, регистрацию физических лиц: пользователей и представителей.

Администратор – администратор системы, который может добавлять и редактировать (удалять, изменять) пользователей системы – сотрудников отдела информационной безопасности.

Диаграмма вариантов использования системы представлена на рис. 4.

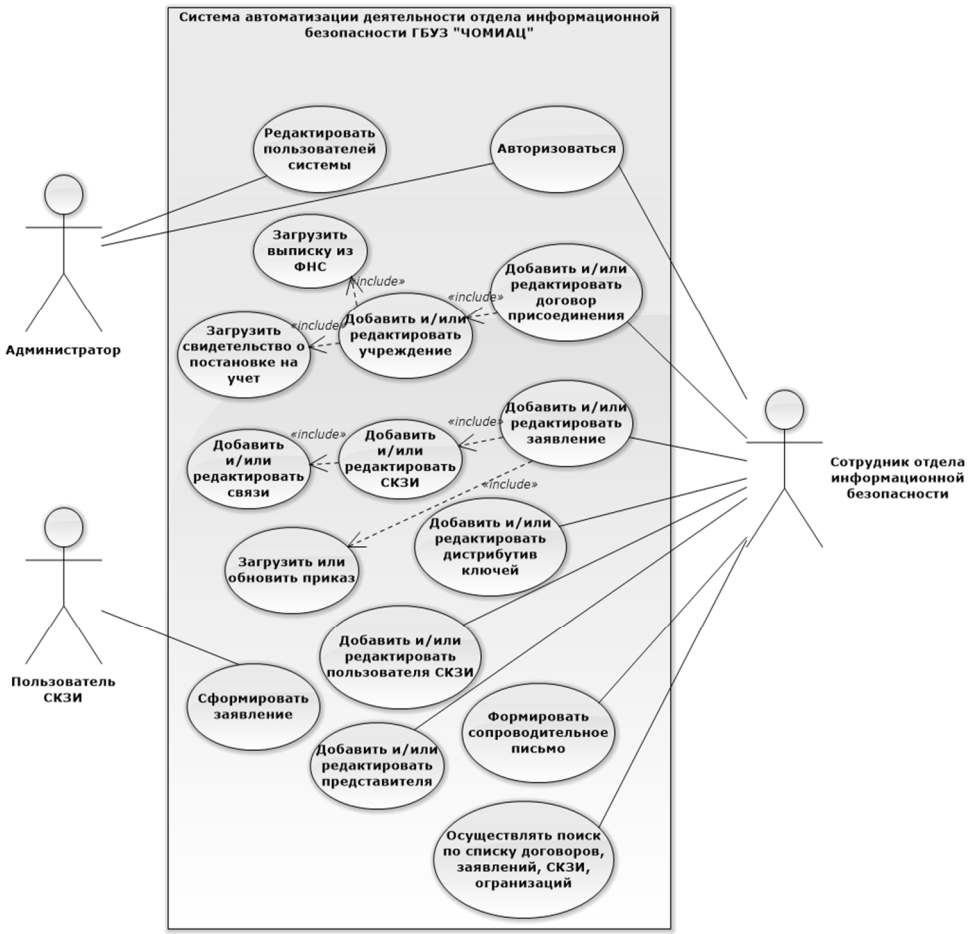

Рис. 4. Диаграмма вариантов использования системы

2.3.4. Детализация прецедентов

1. *Авторизоваться.* Администратор системы либо сотрудник отдела информационной безопасности должен пройти процедуру авторизации до того, как получит доступ к системе. Авторизация производится на основе

введенных логина и пароля.

2. *Редактировать пользователей системы.* Администратор системы может добавлять и редактировать (удалять, изменять) пользователей системы – сотрудников отдела информационной безопасности.

3. *Добавить и/или редактировать договор присоединения.* Сотрудник отдела информационной безопасности при заключении договора присоединения вносит информацию о нем в систему. При изменении этой информации сотрудник может внести изменения в карточку договора в системе.

4. *Добавить и/или редактировать учреждение.* В рамках процедуры добавления договора присоединения сотруднику отдела информационной безопасности необходимо указать сведения об учреждении, с которым этот договор заключается. При изменении реквизитов учреждения можно внести изменения в карточку организации.

5. *Загрузить выписку из ФНС.* При каждом обращении в ГБУЗ «ЧОМИАЦ» необходимо проверить полномочия руководителя учреждения, с помощью выписки из ЕГРЮЛ. Файл с выпиской сотрудник отдела информационной безопасности прикрепляет к карточке документа.

6. *Загрузить свидетельство о постановке на учет.* При добавлении учреждения сотрудник отдела информационной безопасности прикрепляет скан-копию свидетельства о постановке на учет в налоговом органе. При изменении реквизитов учреждения (название, адрес и т.п.), сотрудник прикрепляет новый документ.

7. *Добавить и/или редактировать заявление.* Сотрудник отдела информационной безопасности вносит информацию о заявлении в систему. Это можно сделать двумя способами: считывание QR-кода или добавление вручную путем заполнения формы.

8. *Добавить и/или редактировать СКЗИ.* Сотрудник отдела информационной безопасности при получении нового приказа, должен добавить соответствующее СКЗИ в систему, заполнив форму.

9. *Добавить и/или редактировать связи.* При обращении с заявлением организация указывает информационные системы, с которыми ей нужны связи. Эту информацию сотрудник вносит в систему автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ».

10. *Загрузить или обновить приказ.* Пользователь криптосредства назначается приказом, подписанным руководителем учреждения. Сотрудник отдела информационной безопасности добавляет данные о приказе в систему.

11. *Добавить и/или редактировать дистрибутив ключей.* На основании заявления пользователю выдается дистрибутив ключевой информации. Сотрудник отражает это в системе.

12. *Добавить и/или редактировать пользователя СКЗИ.* Сотрудник отдела информационной безопасности вносит данные о пользователе в систему. При этом система проверяет актуальность паспортных данных пользователя.

13. *Добавить и/или редактировать представителя.* При обращении в ГБУЗ «ЧОМИАЦ» через представителя, сотрудник отдела информационной безопасности вносит данные о представителе в систему. При этом системы проверяет актуальность паспортных данных представителя.

14. *Осуществлять поиск по списку договоров, заявлений, СКЗИ, организаций.* Сотрудник отдела информационной безопасности для быстрого доступа к конкретному договору может воспользоваться поиском по номеру, дате заключения или организации. Для поиска заявлений может использоваться дата, ФИО, организация. Для поиска по СКЗИ – учетный номер, тип, адрес установки. Для поиска организации – название, ИНН, ОГРН, адрес.

15. *Формировать сопроводительное письмо*. Сотрудник отдела информационной безопасности генерирует сопроводительное письмо на каждое заявление, поданное пользователем криптосредства.

16. *Сформировать заявление.* Пользователь СКЗИ перед обращени-

ем в ГБУЗ «ЧОМИАЦ» может сформировать заявление, заполнив специальную форму, и распечатать его. При этом на заявление наносится QR-код, содержащий основную информацию этого заявления, для дальнейшей возможности его считывания при добавлении нового заявления.

2.4. Вывод

Таким образом, система автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ» должна быть ориентирована на удобство использования сотрудниками отдела информационной безопасности. Система рассчитана на предоставление пользователям возможности работы с документами, формирования сопроводительных писем и генерации заявлений в формате *.pdf.

3. ПРОЕКТИРОВАНИЕ

3.1. Паттерн проектирования. Особенности MVC в Django

Для разработки приложения использовалась концепция Model-View-Controller (MVC, модель-представление-контроллер), что позволило отделить бизнес-логику (модели) от ее визуализации (представления, вида). За счет такого разделения повышается возможность повторного использования.

Модель приложения, пользовательский интерфейс и взаимодействие с пользователем разделяются на три отдельных компонента таким образом, чтобы модификация одного из компонентов оказывала минимальное воздействие на остальные.

Django следует модели MVC достаточно близко, т.е. может быть назван MVC-совместимой средой разработки. Но часть контроллера в Django – это часть, которая выбирает представление в зависимости от пользовательского ввода, обрабатывается самой средой разработки, следуя созданной схемой URL, и вызывает соответствующую функцию Python для указанного URL. Поэтому на Django ссылаются как на MTV-ориентированную среду разработки:

- «M» определено для «Модели» (Model), слоя доступа к данным. Этот слой знает все о данных: как получить к ним доступ, как проверить их, как с ними работать и как данные связаны между собой;
- «T» определено для «Шаблона» (Template), слоя представления данных. Этот слой принимает решения относительно представления данных: как и что должно отображаться на странице или в другом типе документа;
- «V» определено для «Представления» (View), слоя бизнес-логики. Этот слой содержит логику, информацию о том, как получать доступ к моделям и применять соответствующий шаблон. Можно рассматривать его как мост между моделями и шаблонами.

3.2. Компоненты системы

Диаграмма компонентов системы автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ» представлена на рис. 5. Система состоит из базы данных, интерфейса пользователя и 5 модулей: модуль договоров, модуль СКЗИ, модуль пользователей и представителей, модуль генерации заявлений, модуль проверки паспортов.

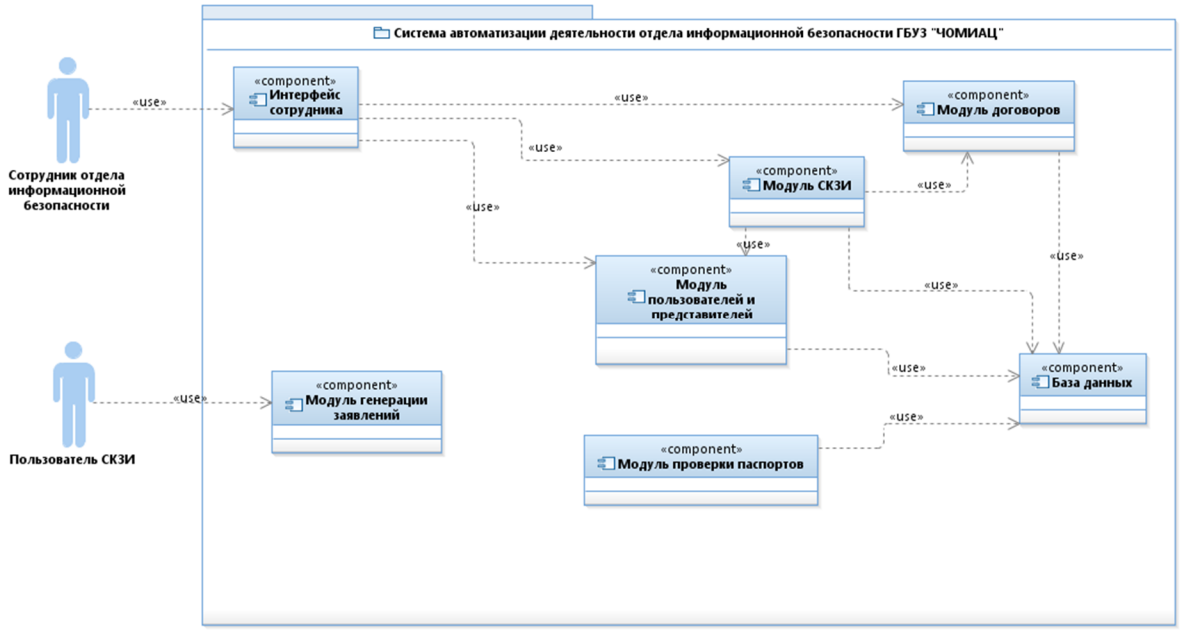

Рис. 5. Диаграмма компонентов

Рассмотрим основные компоненты более подробно.

Интерфейс сотрудника – пользовательский интерфейс, с помощью которого можно осуществлять работу с заявлениями, криптосредствами, пользователями и представителями пользователей, зарегистрированными в системе.

Модуль договоров – подсистема, в рамках которой ведется работа с договорами и учреждениями, с которыми договоры заключены. Предоставляется возможность их создания и изменения, поиска по списку договоров.

Модуль СКЗИ – подсистема, в рамках которой ведется работа с СКЗИ и связями, заявлениями, приказами и сопроводительными письмами

(создание, изменение, просмотр, удаление). Осуществляется сканирование QR-кода из заявления и заполнение полей заявления автоматически, генерация сопроводительных писем.

Модуль пользователей и представителей – подсистема, в рамках которой ведется работа с пользователями средств криптографической защиты информации и представителями пользователей (создание, изменение, просмотр, удаление).

Модуль генерации заявлений – подсистема, осуществляющая генерацию PDF-файла заявления из формы, заполненной пользователем средства криптографической защиты информации.

3.3. Концептуальная схема БД

Концептуальная схема базы данных (универсальное представление структуры данных в рамках предметной области, независимое от конечной реализации базы данных и аппаратной платформы), представлена на рис. 6.

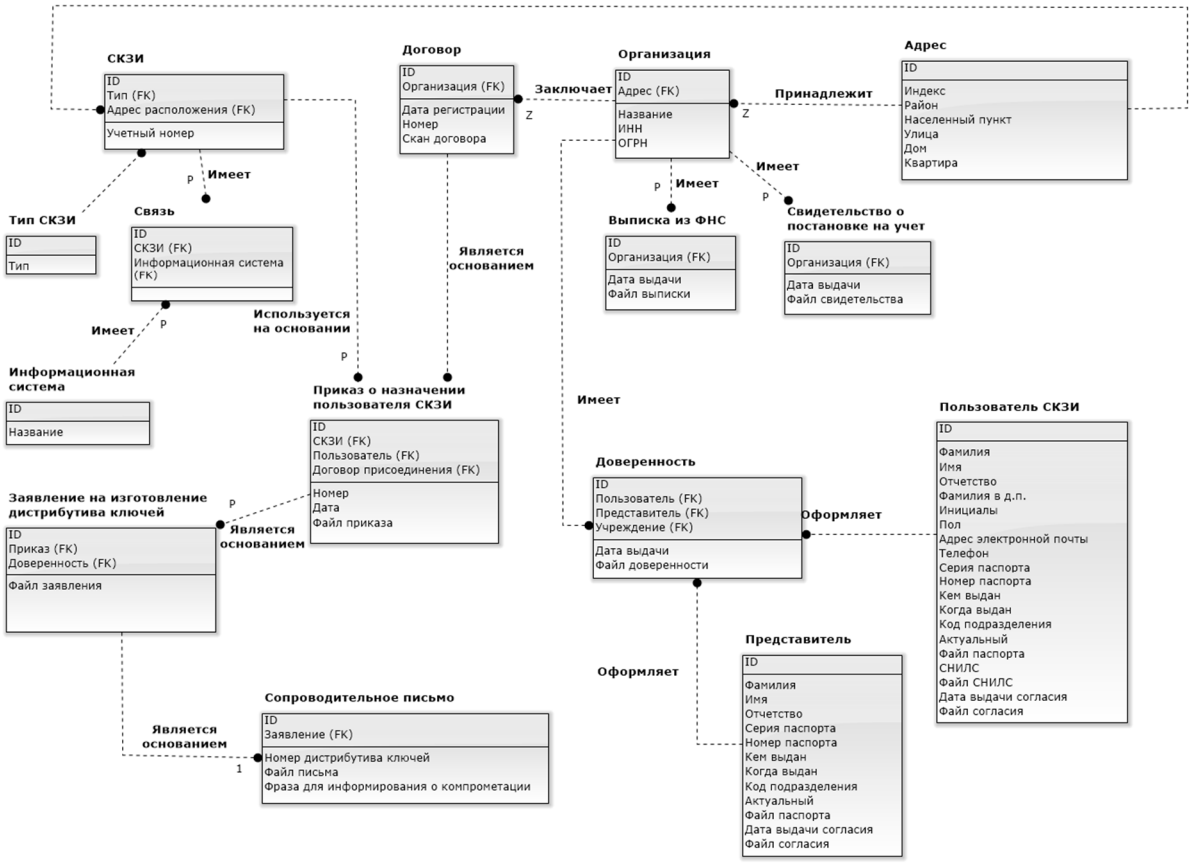

Рис. 6. Концептуальная схема БД

3.4. Вывод

В соответствии с требованиями была спроектирована система автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ». Шаблоном проектирования выбран шаблон MVC. Функционал системы разделен на 5 модулей: модуль договоров, модуль СКЗИ, модуль пользователей и представителей, модуль генерации заявлений, модуль проверки паспортов. Была спроектирована концептуальная схема базы данных, что позволило получить представление структуры данных предметной области, независимое от конечной реализации базы данных и аппаратной платформы.

4. РЕАЛИЗАЦИЯ

На основании выполненного в главе 3 проектирования произведена реализация системы. Для реализации системы был использован язык программирования Python (фреймворк Django) и база данных MySQL.

4.1. Модели в системе

Модель содержит основные поля хранимых данных и описывает их поведение. Как правило, каждая модель является представлением одной из таблиц базы данных. Кроме того, фреймворк Django позволяет разработчику обращаться к ней без выполнения запросов на языке SQL.

В системе были созданы следующие модели:

- модуль договоров:
  - модель договора (Contract);
  - модель организации (Organization);
  - модель адреса (Address);
  - модель выписки из налоговой (Extract);
  - модель свидетельства о постановке на учет (Certificate);
- модуль пользователей и представителей:
  - модель пользователя СКЗИ (Cdpt_user);
  - модель представителя пользователя (Representative);
  - модель доверенности (Attorney);
- модуль криптосредств:
  - модель СКЗИ (Cdpt);
  - модель типа СКЗИ (Cdpt_type);
  - модель информационной системы (InfSystem);
  - модель связи (Relation);
  - модель приказа (Statement);
  - модель заявления (Order);
  - модель сопроводительного письма (Letter);
  - модель дистрибутива ключей (Distrib).

4.2. Реализация представлений

Для реализации представлений в Django существуют так называемые представления-классы (Class-based views, CBV), которые облегчают работу с базовыми функциями создания, чтения, обновления и удаления данных:

- *CreateView* для создания экземпляра модели;
- *UpdateView* для обновления существующего экземпляра модели;
- *DeleteView* для удаления существующего экземпляра модели;
- *DetailView* для просмотра информации о конкретном экземпляре модели.
- *ListView* для просмотра списка экземпляров модели. Выборка может осуществляться по полям модели с использованием фильтров, также могут быть выбраны все экземпляры.

Для просмотра детальной информации об экземпляре модели необходимо отображать данные связанных с ним моделей. Для этого в класс *DetailView* существует метод *get_context_data()*, который возвращает данные контекста для отображения на веб-странице. В него можно добавлять любые данные. Пример переопределения метода *get_context_data()* представлен на рис. 7.

```
def get_context_data(self, **kwargs):
    context = super(UserDetail, self).get_context_data(**kwargs)
    context['attorneys'] = Attorney.objects.filter(Q(principal_id =
self.object.id))
    return context
```

Рис. 7. Листинг метода получения контекста

В связи с тем, что многие модели связаны друг с другом, удобнее реализовать их создание и редактирование вместе, то есть отображать на одной странице поля всех связанных форм. Например, для добавления договора присоединения помимо полей модели договора, доступны поля модели организации и адреса. Это существенно упрощает и ускоряет добавление и изменение данных, т.к. не приходится сначала добавлять адрес, потом организацию с выбором ранее добавленного адреса, а только потом

договор с выбором организации.

В таком случае работу с формами можно разделить на 3 типа.

1. *Первоначальный GET* (отображение пустой или предварительно заполненной формы). Для этого необходимо в методе *get()* добавить нужные формы в данные контекста.

2. *POST с неверными данными* (повторное отображение формы с ошибками). Для этого в методе *form_invalid()* необходимо также указать нужные формы в данных контекста. Ошибки автоматически отобразятся для всех указанных в контексте форм.

3. *POST с верными данными* (обработка данных, сохранение, перенаправление на другую страницу). Для этого в методе *form_valid()* необходимо описать порядок сохранения данных, например сначала сохранить адрес и его использовать для заполнения поля «адрес» в модели «организация», при загрузке нового паспорта установить значение актуальности равное «1» и т.п.

4.3. Генерация заявления

Для ускорения регистрации заявлений на изготовление дистрибутива ключей, уменьшения количества ошибок при заполнении заявлений пользователями средств криптографической защиты информации принято решение разработать сервис для генерации заявлений с помощью заполнения веб-формы. На основании введенных данных система заполняет шаблон и вносит в него QR-код, содержащий введенные данные в формате JSON. Валидация происходит с помощью модуля *jsonschema* [4], который проверяет соответствие представленных JSON данных с помощью JSON Schema (приложение 9).

Для генерации QR-кода был использован модуль *python-qrcode* [6], предоставляющий возможность простого создания изображения QR-кода, используя всего один метод *make()*. PDF-документ генерируется из HTML с использованием модуля *Weasyprint* [9].

4.4. Реализация интерфейса. Bootstrap

При реализации интерфейса системы для повышения удобства его использования принято решение использовать фреймворк Bootstrap 3 [15]. Он поддерживается всеми требуемыми браузерами, что обеспечит одинаковое отображение системы в любом из них. Фреймворк содержит реализованные CSS-классы для удобного отображения списка элементов (*list-group* и *list-group-item*), предоставляет возможность группировки данных с помощью текстовых панелей (*panel*) и др.

Для быстрого поиска по списку документов был реализован фильтр, позволяющий скрыть элементы, неудовлетворяющие запросу. Реализация фильтра была осуществлена на языке JavaScript с использованием JQuery [3]. Код скрипта приведен на рис. 8.

```
<script type="text/javascript">
var $elements = $('.list-group-item');

$('#filter').on('keyup', function() {
  var val = this.value.toLowerCase();

  $elements.show().filter(function(){
    var panelTitleText = $(this).text().toLowerCase();
    return panelTitleText.indexOf(val) < 0;
  }).hide();
});
</script>
```

Рис. 8. Реализация фильтра элементов списка

4.5. Реализация автоматической проверки паспортов

В связи с тем, что при каждом обращении пользователя или представителя пользователя в ГБУЗ «ЧОМИАЦ» производится его идентификация [19], необходимо знать, паспорта каких физических лиц являются недействительными, чтобы оперативно заменить скан-копию в системе, если пользователь предоставил оригинал нового паспорта, или отказать в выдаче дистрибутива ключей, если предоставленный оригинал паспорта также недействителен.

На сайте Федеральной миграционной службы Российской Федерации

представлен список недействительных (утраченных (похищенных), оформленных на утраченных (похищенных) бланках паспорта гражданина Российской Федерации, выданных в нарушение установленного порядка, а также признанных недействительными) паспортов граждан Российской Федерации, удостоверяющих личность гражданина Российской Федерации на территории Российской Федерации [17] в файле формата *.csv.

Ежедневно в 00.00 с помощью программы-демона *cron* [2] запускается скрипт Python, который скачивает файл с сайта ФМС, разархивирует его, и проверяет все паспорта в системе на наличие в этом файле. Если паспорт присутствует в файле, то значение поля *actual* становится равным 0. Диаграмма деятельности по проверке паспорта представлена на рис. 9.

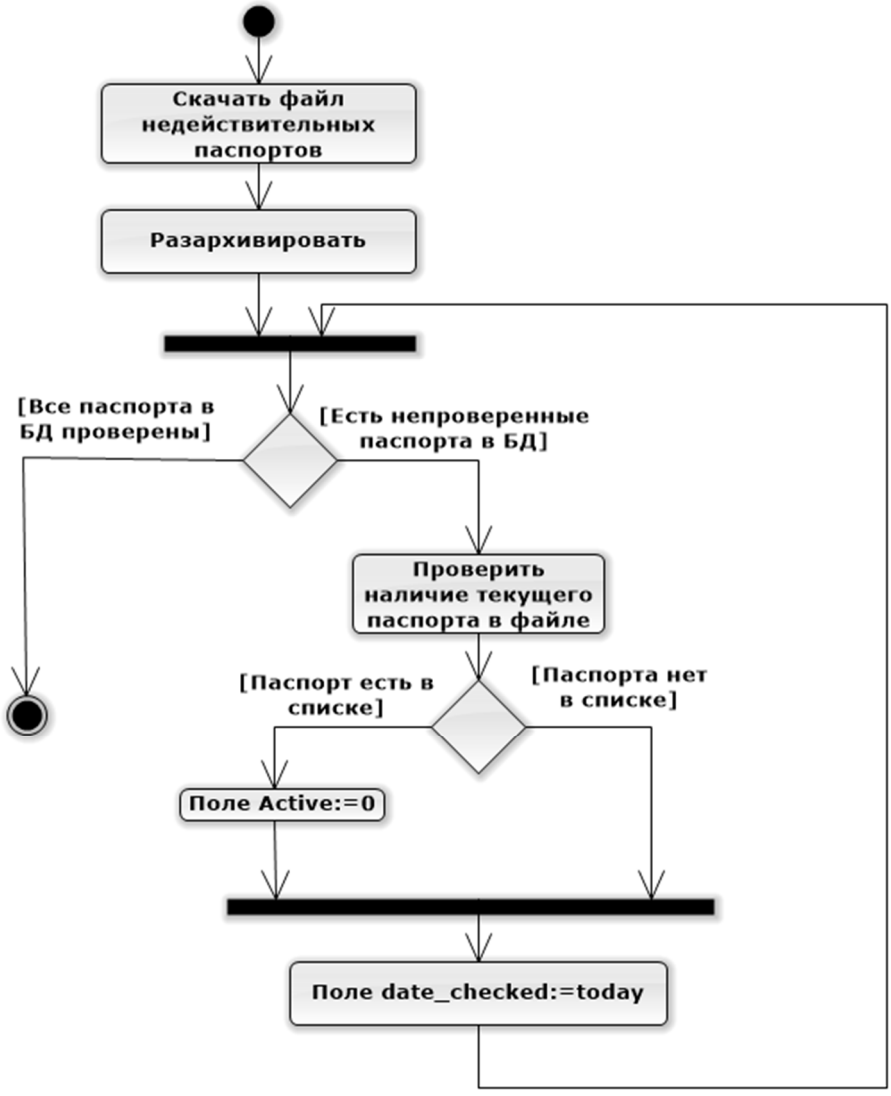

Рис. 9. Диаграмма деятельности по проверке паспортов

4.6. Вывод

На основе выполненного проектирования была реализована система, предоставляющая пользователям удобный инструмент для работы с документами, генератор сопроводительных писем и заявлений в формате PDF. Информация хранится в СУБД MySQL. Выполнена реализация модулей договоров, СКЗИ, пользователей и представителей, генерации заявлений, проверки паспортов и пользовательского интерфейса с использованием фреймворка Django и языка программирования Python.

5. ТЕСТИРОВАНИЕ

Для тестирования веб-приложения были использованы следующие методы:

- функциональное тестирование;
- юзабилити-тестирование;
- тестирование пользовательского интерфейса.

Для тестирования был использован тестовый набор данных, представленный в приложении 10.

5.1. Функциональное тестирование

Функциональное тестирование – один из ключевых видов тестирования, задача которого установить соответствие разработанного программного обеспечения исходным функциональным требованиям заказчика. То есть проведение функционального тестирования позволяет проверить способность информационной системы в определенных условиях решать задачи, нужные пользователям.

Функциональное тестирование проводилось с помощью библиотеки WebTest [14], которая предоставляет класс-наследник от базового класса django.test.TestCase [13], но предоставляет такие возможности, как переход по ссылкам, отправка форм, загрузка файла, парсинг ответа сервера и т.д. Пример класса для проверки авторизации представлен на рис. 10. Полная спецификация тестовых случаев доступна в приложении 11.

```
class AuthTest(WebTest):
    fixtures = ['users.json']
    def testLogoutAndLogin(self):
        page = self.app.get('/', user='test-user')
        page = page.click(u'Выйти').follow()
        assert u'Выйти' not in page
        login_form = page.click(u'Войти', index= 0).form
        login_form['email'] = 'example@example.com'
        login_form['password'] = '123'
        result_page = login_form.submit().follow()
        assert u'Войти' not in result_page
        assert u'Выйти' in result_page
```

Рис. 10. Класс для проверки авторизации

5.2. Юзабилити-тестирование

Юзабилити-тестирование – тестирование, выполняемое с целью определения, удобна ли веб-страница или пользовательский интерфейс для его предполагаемого применения. Для этого теста были привлечены 4 сотрудника отдела информационной безопасности ГБУЗ «ЧОМИАЦ». Тестировщикам было предложено решить следующие задачи:

- авторизоваться в системе;
- осуществить поиск по договорам присоединения;
- добавить или изменить существующий договор присоединения;
- прикрепить новую выписку из ФНС;
- осуществить поиск по пользователям;
- добавить или редактировать пользователя;
- добавить заявление вручную и с помощью QR-кода;
- сгенерировать сопроводительное письмо к заявлению;
- добавить или изменить СКЗИ и связи;
- сгенерировать заявление из формы.

Все задачи были решены всеми тестировщиками без каких-либо затруднений. Недостатков не выявлено. Тест пройден успешно.

5.3. Тестирование пользовательского интерфейса

Интерфейс был протестирован в браузерах Microsoft Edge, Mozilla Firefox, Opera, Google Chrome. В ходе тестирования не возникло никаких проблем с версткой. Интерфейс во всех браузерах был идентичным. Тест пройден успешно.

5.4. Вывод

Для тестирования системы автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ» применялось функциональное тестирование, юзабилити-тестирование и тестирование пользовательского интерфейса. Для тестирования был разработан набор тестовых данных. Тестирование не выявило недостатков в системе.

ЗАКЛЮЧЕНИЕ

Данная работа посвящена разработке системы автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ». В ходе проделанной работы мной были решены следующие задачи:

- изучены требования Регламента работы Удостоверяющего и ключевого центра ГБУЗ «ЧОМИАЦ»;
- изучены существующие подходы, применяющиеся при построении информационных систем, а частности веб-приложений, был выбран наиболее оптимальный из них;
- на основе выбранной технологии реализована система автоматизации деятельности отдела информационной безопасности ГБУЗ «ЧОМИАЦ». В процессе работы были изучены возможности работы с фреймворком Django, языком программирования Python, системой управления базами данных MySQL;
- произведено тестирование системы с использованием тестового набора пользовательских данных. Система успешно прошла предложенные тесты.

Разработанное веб-приложение внедрено в промышленную эксплуатацию ГБУЗ «ЧОМИАЦ» и используется для выдачи и учета средств криптографической защиты информации, генерации заявлений и сопроводительных писем.

СПИСОК ЛИТЕРАТУРЫ

1. About Node.js. [Электронный ресурс] URL: https://nodejs.org/en/about/ (дата обращения: 25.02.2016).
2. Cron. Русскоязычная документация по Ubuntu. [Электронный ресурс] URL: http://help.ubuntu.ru/wiki/cron (дата обращения: 05.04.2016).
3. JQuery API Documentation. [Электронный ресурс] URL: http://api.jquery.com/ (дата обращения: 02.04.2016).
4. JSONSchema Documentation. [Электронный ресурс] URL: https://pypi.python.org/pypi/jsonschema (дата обращения: 02.04.2016).
5. PostgreSQL: The world’s most advanced open source database. [Электронный ресурс] URL: http://www.postgresql.org/ (дата обращения: 28.03.2016).
6. Pure python QR Code generator. [Электронный ресурс] URL: https://pypi.python.org/pypi/qrcode (дата обращения: 02.04.2016).
7. TIOBE Software: Tiobe Index. [Электронный ресурс] URL: http://www.tiobe.com/tiobe_index (дата обращения: 01.05.2016).
8. ViPNet Custom. [Электронный ресурс] URL: https://infotecs.ru/products/line/custom.php (дата обращения: 21.03.2016).
9. WeasyPrint Documentation. [Электронный ресурс] URL: http://weasyprint.readthedocs.io/en/latest/ (дата обращения: 02.04.2016).
10. 1С Предприятие 8. [Электронный ресурс] URL: http://v8.1c.ru/overview/ (дата обращения: 21.03.2016).
11. Головатый А., Каплан-Мосс Дж. Django. Подробное руководство. – СПб.: Символ-Плюс, 2010. – 560 с.
12. Гринвальд Р., Стаковьяк Р., Додж Г. Oracle для профессионалов. – М.: Диалектика, 2007. – 783 с.
13. Документация Django. [Электронный ресурс] URL: https://www.djangoproject.com/ (дата обращения: 11.05.2016).
14. Документация Django WebTest. [Электронный ресурс] URL: https://pypi.python.org/pypi/django-webtest (дата обращения: 02.04.2016).

15. Документация Twitter Bootstrap. [Электронный ресурс] URL: http://getbootstrap.com/ (дата обращения: 11.05.2016).

16. Костарев А. PHP 5. – СПб.: BHV-Петербург, 2008. – 1104 с.

17. Проверка по списку недействительных российских паспортов. [Электронный ресурс] URL: http://services.fms.gov.ru/info-service.htm?sid=2000 (дата обращения: 02.03.2016).

18. Программный комплекс: «Аристотель». [Электронный ресурс] URL: http://www.aristotel.biz/content/about.html (дата обращения: 22.03.2016).

19. Регламент работы Удостоверяющего и ключевого центра ГБУЗ «Челябинский областной медицинский информационно-аналитический центр». [Электронный ресурс] URL: http://www.miac74.ru/upload/medialibrary/fbd/fbd94d18ee63f57b26e9a10c9d6730ab.pdf (дата обращения: 04.02.2016).

20. Тейт Б., Хиббс К. Ruby on Rails. Быстрая веб-разработка. – СПб.: BHV-Петербург, 2008. – 224 с.

21. Чан У., Биссекс П., Форсье Д. Django. Разработка веб-приложений на Python. – СПб.: Символ-Плюс, 2009. – 456 с.

22. Чедвик Д., Снайдер Т., Панда Х. ASP.NET MVC 4: разработка реальных веб-приложений с помощью ASP.NET MVC. – М.: Вильямс, 2013. – 432 с.

23. Шелдон Р., Мойе Д. MySQL 5: базовый курс. – М.: Диалектика, 2007. – 880 с.

ПРИЛОЖЕНИЯ

Приложение 1

Договор присоединения

ДОГОВОР ПРИСОЕДИНЕНИЯ №12345
к Регламенту работы удостоверяющего и ключевого центра
государственного бюджетного учреждения здравоохранения
«Челябинский областной медицинский информационно-аналитический центр»

г. Челябинск 29 декабря 2014 г.

Государственное бюджетное учреждение здравоохранения «Челябинский областной медицинский информационно-аналитический центр», в лице начальника отдела информационной безопасности Староверова Артёма Сергеевича, действующего на основании приказа от 30 апреля 2015 г. № 36 о/д, именуемое в дальнейшем «Администратор УКЦ», с одной стороны, и муниципальное бюджетное учреждение здравоохранения «Городская клиническая больница №12», в лице главного врача Петрова Ивана Павловича, действующего на основании Устава, именуемое в дальнейшем «Пользователь УКЦ», с другой стороны, вместе именуемые «Стороны», а по отдельности – «Сторона», заключили настоящий договор присоединения к Регламенту работы удостоверяющего и ключевого центра государственного бюджетного учреждения здравоохранения «Челябинский областной медицинский информационно-аналитический центр» о нижеследующем.

1. Предмет договора

1.1. Настоящий договор является договором присоединения Пользователя УКЦ к Регламенту работы удостоверяющего и ключевого центра государственного бюджетного учреждения здравоохранения «Челябинский областной медицинский информационно-аналитический центр» (далее – Регламент) в порядке ст. 428 Гражданского кодекса Российской Федерации.

2. Права, обязанности и ответственность Сторон

2.1. Права, обязанности и ответственность Сторон определяются Регламентом и настоящим договором.

2.2. Обязанности Пользователя УКЦ:

2.2.1. в момент заключения настоящего договора предоставить Администратору УКЦ заверенную копию свидетельства о постановке на учет юридического лица в налоговом органе по месту нахождения на территории Российской Федерации, копию свидетельства о государственной регистрации юридического лица, копии свидетельств о внесении записи в Единый государственный реестр юридических лиц о регистрации изменений, вносимых в учредительные документы юридического лица, при этом все предоставляемые копии свидетельств заверяются руководителем Пользователя УКЦ;

2.2.2. своевременно (не позднее одного рабочего дня с момента принятия решения об внесении изменений) информировать Администратора УКЦ об изменении реквизитов Пользователя УКЦ, пользователей средств криптографической защиты информации (в том числе о расторжении трудовых договоров с пользователями средств криптографической защиты информации);

2.2.3. принимать все вносимые в Регламент изменения с момента их вступления в силу.

2.3. Права Администратора УКЦ:

2.3.1. приостанавливать исполнение настоящего договора и Регламента в случае выявления нарушений со стороны Пользователя УКЦ до момента устранения таких нарушений;
2.3.2. вносить изменения в Регламент без дополнительного уведомления Пользователя УКЦ.

3. Порядок разрешения споров

3.1. Разногласия, возникающие между Сторонами при заключении, изменении и расторжении настоящего договора рассматриваются в установленном действующим Законодательством порядке.
3.2. Все споры между Сторонами, по которым не было достигнуто соглашение, разрешаются в Арбитражном суде Челябинской области.

4. Дополнительные условия

4.1. Настоящий договор вступает в силу с момента подписания его Сторонами и действует до выполнения одного из следующих условий: прекращение деятельности Удостоверяющего и ключевого центра государственного бюджетного учреждения здравоохранения «Челябинский областной медицинский информационно-аналитический центр», расторжение Администратором УКЦ в одностороннем порядке, расторжение по соглашению Сторон, иные предусмотренные законодательством Российской Федерации условия.
4.2. Отношения Сторон, не урегулированные настоящим договором, регулируются действующим Законодательством.
4.3. Условия настоящего договора могут быть изменены по взаимному согласию Сторон с обязательным составлением письменного документа, являющегося неотъемлемой частью настоящего договора.
4.4. Настоящий договор составлен в двух экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой Стороны.

Реквизиты и подписи сторон

Администратор УКЦ:	*Пользователь УКЦ:*
Государственное бюджетное учреждение здравоохранения «Челябинский областной медицинский информационно-аналитический центр» Юридический адрес: г. Челябинск, ул. Кузнецова, 2А. Почтовый адрес: 454087, г. Челябинск, ул. Кузнецова, 2А. ИНН 7453141034, КПП 745301001, ОГРН 1057424502673. Телефон: +7 (351) 200-61-61. Факс: +7 (351) 200-61-61 (доб. 9).	Муниципальное бюджетное учреждение здравоохранения «Городская клиническая больница №12» Юридический адрес: Аргаяшский р-н, с. Кузнецкое, ул. Пионерская, д. 32. Почтовый адрес: 456123, Аргаяшский р-н, с. Кузнецкое, ул. Пионерская, д. 32. ИНН 7453123456, КПП 745301001, ОГРН 1057453654321. Телефон: +7 (351-12) 3-45-67. Факс: +7 (351-12) 3-45-68.
_____ / А.С. Староверов	_____ / И.П. Петров
	Место печати

Приложение 2

Согласие субъекта

Согласие на обработку персональных данных

Город Челябинск,
Двадцать девятое декабря две тысячи четырнадцатого года.

Субъект персональных данных Сидорова Мария Николаевна (паспорт гражданина РФ серии 7500 номер 123456 выдан 20 марта 2008 г. Отделением УФМС России по Челябинской области в Аргаяшском районе, код подразделения 740-000), зарегистрированный по адресу: Аргаяшский р-н, село Кузнецкое, ул. Школьная, д. 11, кв. 22, в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» дает свое согласие Удостоверяющему и ключевому центру ГБУЗ «Челябинский областной медицинский информационно-аналитический центр», расположенному по адресу: г. Челябинск, ул. Кузнецова, д. 2А, на обработку своих персональных данных (фамилия, имя, отчество, пол, дата и место рождения, серия, номер, дата и место выдачи паспорта гражданина Российской Федерации, место жительства, место работы и должность, страховой номер индивидуального номера лицевого счета, адрес электронной почты, номер телефона) для осуществления действий, предусмотренных Регламентом работы Удостоверяющего и ключевого центра ГБУЗ «Челябинский областной медицинский информационно-аналитический центр».

Субъект персональных данных предоставляет право Удостоверяющему и ключевому центру ГБУЗ «Челябинский областной медицинский информационно-аналитический центр» осуществлять с использованием средств автоматизации или без использования таких средств следующие действия с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Настоящее согласие дано субъектом до прекращения деятельности Удостоверяющего и ключевого центра ГБУЗ «Челябинский областной медицинский информационно-аналитический центр». Настоящее согласие может быть отозвано в порядке, установленном Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных». В случае отзыва настоящего согласия, Удостоверяющий и ключевой центр ГБУЗ «Челябинский областной медицинский информационно-аналитический центр» вправе не прекращать обработку персональных данных субъекта до истечения сроков, установленных законодательством Российской Федерации.

Субъект персональных данных М.Н. Сидорова

Подпись субъекта персональных данных удостоверяю:

Результаты проведения внутренней проверки Удостоверяющего и ключевого центра достоверности указанных сведений:

Паспорт гражданина РФ субъекта: ___.___.20___ г. _____ *Подпись сотрудника Удостоверяющего центра*

Отметка о принятии в работу Удостоверяющего и ключевого центра:

Приложение 3

Справка с места работы

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ «ГОРОДСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА №12»

Справка

Дана старшей медицинской сестре хирургического отделения Сидоровой Марии Николаевне (паспорт гражданина РФ серии 7500 номер 123456 выдан 20 марта 2008 г. Отделением УФМС России по Челябинской области в Аргаяшском районе, код подразделения 740-000) в том, что она действительно работает в МБУЗ «Городская клиническая больница №12» с 01 марта 1995 г. по настоящее время.

Справка действительна в течение трех рабочих дней и дана для предъявления в Удостоверяющий и ключевой центр ГБУЗ «Челябинский областной медицинский информационно-аналитический центр».

Главный врач МБУЗ «ГКБ №12» И.П. Петров

Место печати «29» декабря 2014 г.

Приложение 4

Доверенность

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ «ГОРОДСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА №12»

Доверенность
на совершение юридически значимых действий в Удостоверяющем и ключевом центре
ГБУЗ «Челябинский областной медицинский информационно-аналитический центр»

Село Кузнецкое Аргаяшского района,
Двадцать девятое декабря две тысячи четырнадцатого года.

Я, старшая медицинская сестра хирургического отделения Сидорова Мария Николаевна (паспорт гражданина РФ серии 7500 номер 123456 выдан 20 марта 2008 г. Отделением УФМС России по Челябинской области в Аргаяшском районе, код подразделения 740-000), доверяю водителю службы скорой медицинской помощи Иванову Михаилу Степановичу (паспорт гражданина РФ серии 7500 номер 654321 выдан 20 декабря 2009 г. Отделением УФМС России по Челябинской области в Аргаяшском районе, код подразделения 740-000) совершать от моего имени следующие действия:

1. давать Удостоверяющему и ключевому центру ГБУЗ «Челябинский областной медицинский информационно-аналитический центр» согласие на обработку моих персональных данных;
2. передавать в Удостоверяющий и ключевой центр ГБУЗ «Челябинский областной медицинский информационно-аналитический центр» документы, предусмотренные Регламентом работы Удостоверяющего и ключевого центра ГБУЗ «Челябинский областной медицинский информационно-аналитический центр», в том числе заявления на изготовление дистрибутивов ключей для подключения к ведомственной сети передачи данных Министерства здравоохранения Челябинской области и сертификатов ключей проверки электронной подписи;
3. получать в Удостоверяющем и ключевом центре ГБУЗ «Челябинский областной медицинский информационно-аналитический центр» дистрибутивы ключей для подключения к ведомственной сети передачи данных Министерства здравоохранения Челябинской области и сертификаты ключей проверки электронной подписи;
4. расписываться в учетных документах Удостоверяющего и ключевого центра ГБУЗ «Челябинский областной медицинский информационно-аналитический центр», заполняемых при совершении определенных настоящей доверенностью действий, в том числе сертификатах ключа проверки электронной подписи.

Настоящая доверенность выдана сроком на три месяца без права передоверия.

Собственноручную подпись М.С. Иванова _____ удостоверяю:

Старшая медицинская сестра хирургического отделения М.Н. Сидорова
Главный врач МБУЗ «ГКБ №12» И.П. Петров
Место печати «29» декабря 2014 г.

Результаты проведения внутренней проверки Удостоверяющего и ключевого центра достоверности указанных сведений:

<table>
<tr><td colspan="2">Полномочия руководителя:

___.___.20___ г.
_____
Подпись сотрудника Удостоверяющего центра</td></tr>
<tr><td>Полномочия доверителя:

___.___.20___ г.
_____
Подпись сотрудника Удостоверяющего центра</td><td>Полномочия доверенного:

___.___.20___ г.
_____
Подпись сотрудника Удостоверяющего центра</td></tr>
<tr><td>Паспорт гражданина РФ доверителя:

___.___.20___ г.
_____
Подпись сотрудника Удостоверяющего центра</td><td>Паспорт гражданина РФ доверенного:

___.___.20___ г.
_____
Подпись сотрудника Удостоверяющего центра</td></tr>
<tr><td>Согласие на обработку персональных данных доверителя:
___.___.20___ г.
_____
Подпись сотрудника Удостоверяющего центра</td><td>Согласие на обработку персональных данных доверенного:
___.___.20___ г.
_____
Подпись сотрудника Удостоверяющего центра</td></tr>
</table>

Отметка о принятии в работу Удостоверяющего и ключевого центра:

Приложение 5

Заявление на изготовление дистрибутива ключей Coordinator

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ «ГОРОДСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА №12»

В Удостоверяющий и ключевой центр
ГБУЗ «Челябинский областной медицинский информационно-аналитический центр»

Заявление
на изготовление дистрибутива ключей для подключения к ведомственной сети передачи данных Министерства здравоохранения Челябинской области

В рамках исполнения договора присоединения к Регламенту работы удостоверяющего и ключевого центра государственного бюджетного учреждения здравоохранения «Челябинский областной медицинский информационно-аналитический центр» от 29 декабря 2014 г. №12345 муниципальное бюджетное учреждение здравоохранения «Городская клиническая больница №12» (ИНН 7453123456, ОГРН 1057453654321) просит Вас изготовить дистрибутив ключей для подключения к ведомственной сети передачи данных Министерства здравоохранения Челябинской области средства криптографической защиты информации ViPNet Coordinator (учетный номер: 585Б-123456) по адресу: Аргаяшский р-н, с. Кузнецкое, ул. Пионерская, д. 32.

Средство криптографической защиты информации будет использоваться для доступа к следующим информационным системам: медицинская информационная система, система бухгалтерского учета.

Пользователем средства криптографической защиты информации приказом от 29 декабря 2014 г. № 123 назначена старшая медицинская сестра хирургического отделения Сидорова Мария Николаевна (страховой номер индивидуального номера лицевого счета 123-456-789 00, электронная почта: sidorovamn@mail.ru, номер телефона: +7 (912) 345-67-89).

С «Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденными руководством 8 Центра Федеральной службы безопасности Российской Федерации 21 февраля 2008 г. № 149/6/6-622, приказом Федерального агентства Правительственной связи и информации от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», Регламентом работы Удостоверяющего и ключевого центра ГБУЗ «Челябинский областной медицинский информационно-аналитический центр» М.Н. Сидорова ознакомлена.

Копия приказа от 29 декабря 2014 г. № 123 «О назначении пользователя средства криптографической защиты информации» прилагается.

Старшая медицинская сестра хирургического отделения М.Н. Сидорова
Главный врач МБУЗ «ГКБ №12» И.П. Петров
Место печати «29» декабря 2014 г.

Результаты проведения внутренней проверки Удостоверяющего и ключевого центра достоверности указанных сведений:

Договор присоединения: ___.___.20___ г. _____ *Подпись сотрудника Удостоверяющего центра*	Согласие на обработку персональных данных пользователя: ___.___.20___ г. _____ *Подпись сотрудника Удостоверяющего центра*
Полномочия руководителя: ___.___.20___ г. _____ *Подпись сотрудника Удостоверяющего центра*	Полномочия пользователя: ___.___.20___ г. _____ *Подпись сотрудника Удостоверяющего центра*
Ознакомление пользователя с приказом: ___.___.20___ г. _____ *Подпись сотрудника Удостоверяющего центра*	

Отметка о принятии в работу Удостоверяющего и ключевого центра:

Приложение 6

Заявление на изготовление дистрибутива ключей Client

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ «ГОРОДСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА №12»

В Удостоверяющий центр
ГБУЗ «Челябинский областной медицинский информационно-аналитический центр»

Заявление
на изготовление дистрибутива ключей для подключения к ведомственной сети передачи данных Министерства здравоохранения Челябинской области

В рамках исполнения договора присоединения к Регламенту работы удостоверяющего и ключевого центра государственного бюджетного учреждения здравоохранения «Челябинский областной медицинский информационно-аналитический центр» от 29 декабря 2014 г. №12345 муниципальное бюджетное учреждение здравоохранения «Городская клиническая больница №12» (ИНН 7453123456, ОГРН 1057453654321) просит Вас изготовить дистрибутив ключей для подключения к ведомственной сети передачи данных Министерства здравоохранения Челябинской области средства криптографической защиты информации ViPNet Client (учетный номер: 585Б-123456) по адресу: Аргаяшский р-н, с. Кузнецкое, ул. Пионерская, д. 32.

Средство криптографической защиты информации будет использоваться для работы с сертификатом открытого ключа подписи, а также доступа к следующим информационным системам: медицинская информационная система, система бухгалтерского учета.

Пользователем средства криптографической защиты информации приказом от 29 декабря 2014 г. № 123 назначена старшая медицинская сестра хирургического отделения Сидорова Мария Николаевна (страховой номер индивидуального номера лицевого счета 123-456-789 00, электронная почта: sidorovamn@mail.ru, номер телефона: +7 (912) 345-67-89).

С «Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденными руководством 8 Центра Федеральной службы безопасности Российской Федерации 21 февраля 2008 г. № 149/6/6-622, приказом Федерального агентства Правительственной связи и информации от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», Федеральным законом от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи», Регламентом работы Удостоверяющего и ключевого центра ГБУЗ «Челябинский областной медицинский информационно-аналитический центр» М.Н. Сидорова ознакомлена.

Копия приказа от 29 декабря 2014 г. № 123 «О назначении пользователя средства криптографической защиты информации» прилагается.

Старшая медицинская сестра хирургического отделения М.Н. Сидорова
Главный врач МБУЗ «ГКБ №12» И.П. Петров
Место печати «29» декабря 2014 г.

Результаты проведения внутренней проверки Удостоверяющего и ключевого центра достоверности указанных сведений:

Договор присоединения: ___.___.20___ г. _____ *Подпись сотрудника Удостоверяющего центра*	Согласие на обработку персональных данных пользователя: ___.___.20___ г. _____ *Подпись сотрудника Удостоверяющего центра*
Полномочия руководителя: ___.___.20___ г. _____ *Подпись сотрудника Удостоверяющего центра*	Полномочия пользователя: ___.___.20___ г. _____ *Подпись сотрудника Удостоверяющего центра*
Ознакомление пользователя с приказом: ___.___.20___ г. _____ *Подпись сотрудника Удостоверяющего центра*	

Отметка о принятии в работу Удостоверяющего и ключевого центра:

Приложение 7

Приказ на подключение Coordinator

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ «ГОРОДСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА №12»

Приказ

29 декабря 2014 г. № 123

О назначении пользователя средства криптографической защиты информации ViPNet Coordinator

Для организации функционирования средства криптографической защиты информации ViPNet Coordinator (учетный номер: 585Б-123456) в рамках исполнения договора присоединения к Регламенту работы удостоверяющего и ключевого центра государственного бюджетного учреждения здравоохранения «Челябинский областной медицинский информационно-аналитический центр» от 29 декабря 2014 г. №12345

ПРИКАЗЫВАЮ:

1. Назначить пользователем средства криптографической защиты информации старшую медицинскую сестру хирургического отделения Сидорову Марию Николаевну.
2. М.Н. Сидоровой ознакомиться со следующими документами и неукоснительно соблюдать их при работе со средством криптографической защиты информации:
   а. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные руководством 8 Центра Федеральной службы безопасности Российской Федерации 21 февраля 2008 г. № 149/6/6-622;
   б. приказ Федерального агентства Правительственной связи и информации от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
   в. Регламент работы Удостоверяющего и ключевого центра ГБУЗ «Челябинский областной медицинский информационно-аналитический центр».
3. Контроль исполнения приказа оставляю за собой.

Главный врач МБУЗ «ГКБ №12» И.П. Петров

С приказом ознакомлена:

Старшая медицинская сестра хирургического отделения М.Н. Сидорова

Приложение 8

JSON Schema заявления

```
{"$schema":"http://json-schema.org/draft-03/schema#",
    "id": "statement",
    "type": "object",
    "additionalProperties": false,
    "properties": {
        "contract": {
      "type": "object",
      "properties": {
        "organization": {
          "type": "object",
          "properties": {
            "full": {
              "type": "string",
              "required": true
            },
            "name": {
              "type": "string",
              "required": true
            },
            "inn": {
              "type": "integer",
              "required": true
            },
            "ogrn": {
              "type": "integer",
              "required": true
            }
          }
        },
        "number": {
          "type": "integer",
          "required": true
        },
        "date": {
            "type": "string",
            "pattern":"^[0-9]{4}-[0-9]{2}-[0-9]{2}",
            "required": true
          }
      }
        },
    "cdpt": {
      "type": "object",
      "properties": {
        "type_cdpt": {
          "type": "integer",
          "required": true
        },
        "number": {
          "type": "string",
          "required": true
        },
        "address": {
          "type": "object",
          "properties": {
              "district": {
                "type": "string"
              },
              "locality": {
                "type": "string",
```

```
                    "required": true
                  },
                  "street": {
                    "type": "string",
                    "required": true
                  },
                  "house": {
                    "type": "string",
                    "required": true
                  }
                }
            },
            "systems": {
              "type": "array",
              "items": {
                "type": "string"
              },
              "required": true
            }
          }
      },
      "user": {
        "type": "object",
          "properties": {
          "surname": {
            "type": "string",
            "required": true
          },
          "name": {
            "type": "string",
            "required": true
          },
            "patronymic": {
            "type": "string",
            "required": true
          },
          "post": {
            "type": "string",
            "required": true
          },
            "snils": {
            "type": "string",
            "required": true
          },
          "email": {
            "type": "string",
            "required": true
            },
          "phone": {
            "type": "string",
            "required": true
            },
          "order_date": {
            "type": "string",
            "pattern": "^[0-9]{4}-[0-9]{2}-[0-9]{2}",
            "required": true
          },
          "order_number": {
            "type": "string",
            "required": true
            },
        }
  }}}
```

Приложение 9

Сопроводительное письмо

МБУЗ Детский санаторий №2
123456, г. Челябинск,
ул Ленина, 1

Бухгалтеру
А.А. Ивановой

Уважаемая Анна Анатольевна!

Удостоверяющий и ключевой центр ГБУЗ «Челябинский областной медицинский информационно-аналитический центр» направляет в Ваш адрес дистрибутив ключей для подключения к ведомственной сети передачи данных Министерства здравоохранения Челябинской области средства криптографической защиты информации ViPNet Client № 1464-КЛ-1-1.

В случае компрометации ключей используйте следующую фразу для информирования Удостоверяющего и ключевого центра ГБУЗ «Челябинский областной медицинский информационно-аналитический центр»:

черновой герцог точит курильщика

Заместитель директора
по информационным технологиям
и информационной безопасности А.С. Староверов

Приложение 10

Набор тестовых данных

```
[
  {
    "model": "ib.User",
    "pk": 1,
    "fields": {
  “login”: “admin”,
      “password”: “123”,
  “role”: “admin”
    }
  },
  {
    "model": "ib.User",
    "pk": 2,
    "fields": {
      “login”: “user”,
      “password”: “123”,
  “role”: “user”
    }
  },
  {
    "model": "ib.Organization",
    "pk": 1,
    "fields": {
      “name”: “ЧОМИАЦ”,
      “inn”: “1231231231”,
  “orgn”: “1234567890123”,
  “address”: “1”
    }
  },
  {
    "model": "ib.Address",
    "pk": 1,
    "fields": {
      “locality”: “г. Челябинск”,
  “street”: “ул. Ленина”,
  “house”: “1”
    }
  },
  {
    "model": "ib.Contract",
    "pk": 1,
    "fields": {
      “date_register”: “2016-01-01”,
      “number”: “123”,
  “organization”: “1”,
  “scan_contract”: “/contracts/1.png”
    }
  },
  {
    "model": "ib.Extract",
    "pk": 1,
    "fields": {
      “file”: “/extracts/1.png”,
  “organization”: “1”
    }
  },
  {
    "model": "ib.Certificate",
    "pk": 1,
```

```
    "fields": {
      “file”: “/certificates/1.png”,
   “organization”: “1”
    }
   },
   {
    "model": "people.cdpt_User",
    "pk": 1,
    "fields": {
      “surname”: “Иванов”,
   “name”: “Иван”,
   “patronymic”: “Иванович”,
   “inirials”: “И.И.”,
   “sex”: “0”,
   “email”: “example@example.com”,
   “phone”: “81234567891”,
   “passport_series”: “1123”,
   “passport_number”: “112354”,
   “passport_issued_date ”: “2016-01-10”,
   “passport_issued_by ”: “ОУФМС России по Челябинской области в Центральном
районе города Челябинска”,
   “passport_code”: “123-012”,
   “passport_actual”: “1”,
   “passport_file ”: “/passports/1.png”,
   “snils_number ”: “123-123-123 00”,
   “snils_file ”: “/snils/1.png”,
   “agreement_date”: “2016-01-01”,
   “agreement_file ”: “/agreements/1.png”
    }
   },
   {
    "model": "people.Representative",
    "pk": 1,
    "fields": {
      “surname”: “Петров”,
   “name”: “Иван”,
   “patronymic”: “Иванович”,
   “inirials”: “И.И.”,
   “sex”: “0”,
   “email”: “example1@example.com”,
   “phone”: “81212112121”,
   “passport_series”: “1113”,
   “passport_number”: “100121”,
   “passport_issued_date ”: “2016-01-10”,
   “passport_issued_by ”: “ОУФМС России по Челябинской области в Центральном
районе города Челябинска”,
   “passport_code”: “123-012”,
   “passport_actual”: “1”,
   “passport_file ”: “/passports/2.png”,
   “agreement_date”: “2016-01-01”,
   “agreement_file ”: “/agreements/2.png”
    }
   },
   {
    "model": "cdpt.Order",
    "pk": 1,
    "fields": {
      “contract”: “1”,
   “cdpt”: “1”,
   “user”: “1”,
   “number”: “123”,
   “date_register”: “2016-01-02”,
   “order_file”: “/orders/1.pdf”
```

```
  }
},
{
  "model": "cdpt.Cdpt",
  "pk": 1,
  "fields": {
    “type”: “1”,
“address”: “1”,
“number”: “КЛ-123-123”
}
},
{
  "model": "cdpt.Cdpt_type",
  "pk": 1,
  "fields": {
    “type”: “ViPNet Coordinator HW1000”
  }
},
{
  "model": "cdpt.Cdpt_type",
  "pk": 2,
  "fields": {
    “type”: “ViPNet Coordinator HW100A”
  }
},
{
  "model": "cdpt.Cdpt_type",
  "pk": 3,
  "fields": {
    “type”: “ViPNet Coordinator HW100B”
  }
},
{
  "model": "cdpt.Cdpt_type",
  "pk": 4,
  "fields": {
    “type”: “ViPNet Client”
  }
},
{
  "model": "cdpt.Relation",
  "pk": 1,
  "fields": {
    “cdpt”: “1”,
“is”: “1”
  }
},
{
  "model": "cdpt.InfSystem",
  "pk": 1,
  "fields": {
    “name”: “Медицинская информационная система”
  }
},
{
  "model": "cdpt.Statement",
  "pk": 1,
  "fields": {
    “order”: “1”,
“attorney”: None,
“statement_file”: “statements/1.png”
  }
},
```

```
  {
    "model": "cdpt.CoverLetter",
    "pk": 1,
    "fields": {
      “number_distr”: “КЛ123-13-1”,
      “statement”: “1”,
      “file_letter”: “/letters/1.pdf”,
  “phrase”: “черновой герцог точит курильщика”
    }
  },
]
```

Приложение 11

Спецификация тестовых случаев

Название:	Тест аутентификации и авторизации	
Функция:	Проверить корректность введенного логина и пароля	
Действие	**Ожидаемый результат**	**Результат теста**
Предусловие:		
Зайти на страницу приложения	Отобразилась главная страница системы с приглашением ввести логин и пароль для дальнейшей работы	Пройден
Шаги теста:		
Ввести учетные данные	Поля заполнены	Пройден
Нажать кнопку войти	Логин/пароль проверены, выдано сообщение об ошибке или произошла переадресация на главную страницу системы и в правом верхнем углу появилась информация о пользователе	Пройден

Название:	Тест добавления договора присоединения	
Функция:	Добавить договор присоединения в систему	
Действие	**Ожидаемый результат**	**Результат теста**
Предусловие:		
Авторизоваться в системе. Перейти на страницу Договоры	Отобразилась страница Договоры со списком всех договоров, фильтром и кнопкой Новый договор	Пройден
Шаги теста:		
Нажать кнопку Новый договор	Произошла переадресация на страницу с формой введения данных нового договора	Пройден
Ввести данные	Поля заполнены	Пройден
Нажать кнопку Добавить	Новый договор внесен в базу данных. Произошла переадресация на страницу просмотра договоров	Пройден

Название:	Тест добавления пользователя	
Функция:	Добавить пользователя криптосредства	
Действие	**Ожидаемый результат**	**Результат теста**
Предусловие:		
Авторизоваться в системе. Перейти на страницу Пользователи	Отобразилась страница Пользователи со списком всех пользователей, фильтром и кнопкой Новый пользователь	Пройден
Шаги теста:		
Нажать кнопку Новый пользователь	Произошла переадресация на страницу с формой введения данных нового пользователя	Пройден
Ввести данные	Поля заполнены	Пройден
Нажать кнопку Добавить	Новый пользователь внесен в базу данных. Произошла переадресация на страницу просмотра пользователей	Пройден

Название:	Тест добавления представителя пользователя	
Функция:	Добавить представителя пользователя	
Действие	**Ожидаемый результат**	**Результат теста**
Предусловие:		
Авторизоваться в системе. Перейти на страницу Представители	Отобразилась страница Представители со списком всех представителей, фильтром и кнопкой Новый представитель	Пройден
Шаги теста:		
Нажать кнопку Новый представитель	Произошла переадресация на страницу с формой введения данных нового представителя	Пройден
Ввести данные	Поля заполнены	Пройден
Нажать кнопку Добавить	Новый представитель внесен в базу данных. Произошла переадресация на страницу просмотра представителей	Пройден

Название:	Тест добавления СКЗИ	
Функция:	Добавить СКЗИ	
Действие	**Ожидаемый результат**	**Результат теста**
Предусловие:		
Авторизоваться в системе. Перейти на страницу СКЗИ	Отобразилась страница СКЗИ со списком всех представителей, фильтром и кнопкой Новое СКЗИ	Пройден
Шаги теста:		
Нажать кнопку Новое СКЗИ	Произошла переадресация на страницу с формой введения данных нового СКЗИ	Пройден
Ввести данные	Поля заполнены	Пройден
Нажать кнопку Добавить	Новое СКЗИ внесен в базу данных. Произошла переадресация на страницу просмотра СКЗИ	Пройден

Название:	Тест добавления пользователя в систему	
Функция:	Добавить пользователя в систему	
Действие	**Ожидаемый результат**	**Результат теста**
Предусловие:		
Авторизоваться с учетной записью Администратора. Перейти на страницу Пользователи системы.	Отобразилась страница Пользователи системы со списком всех пользователей, фильтром и кнопкой Новый пользователь	Пройден
Шаги теста:		
Нажать кнопку Новый пользователь	Произошла переадресация на страницу с формой введения данных нового пользователя	Пройден
Ввести данные	Поля заполнены	Пройден
Нажать кнопку Добавить	Новый пользователь внесен в базу данных. Произошла переадресация на страницу просмотра пользователей	Пройден

Название:	Тест добавления заявления с помощью QR-кода	
Функция:	Распознать QR-код с заявления и заполнить поля	
Действие	**Ожидаемый результат**	**Результат теста**
Предусловие:		
Авторизоваться в системе. Перейти на страницу заявлений	Отобразилась страница со списком заявлений, фильтром и кнопкой Новое заявление	Пройден.
Шаги теста:		
Нажатие кнопки Новое заявление	Произошла переадресация на страницу с формой введения данных нового пользователя	Пройден.
Сканирование QR-кода	Поля заполнены	Пройден.
Нажатие кнопки Зарегистрировать	Новое заявление внесено в базу данных. Произошла переадресация на страницу просмотра заявлений.	Пройден.