МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование кафедры)
02.03.03 Математическое обеспечение и администрирование информационных систем
(код и наименование направления подготовки, специальности)
Технология программирования
(направленность (профиль)/специализация)

БАКАЛАВРСКАЯ РАБОТА

на тему **Разработка подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении**

Студент	Н.В. Иванов	
	(И.О. Фамилия)	(личная подпись)
Руководитель	А.Б. Кузьмичев	
	(И.О. Фамилия)	(личная подпись)
Консультанты	А.В. Москалюк	
	(И.О. Фамилия)	(личная подпись)

Допустить к защите

Заведующий кафедрой к.т.н., доцент, А.В. Очеповский_____
(ученая степень, звание, И.О. Фамилия) (личная подпись)

«_____»_____20_____г.

Тольятти 2018

Аннотация

Работа состоит из трех разделов в которых представлены анализ, проектирование и разработка подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении.

Объём пояснительной записки - 50 страниц, на которых размещены 12 рисунков и 11 таблиц. При написании работы использовалось 23 источника.

РАЗРАБОТКА, МОБИЛЬНОЕ ПРИЛОЖЕНИЕ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ИНФОРМАЦИОННЫЕ СИСТЕМЫ.

Объектом исследования являются системы защиты персональных данных в лечебно-профилактических учреждениях.

Предметом данной работы является подсистема защиты персональных данных в системе публикации контента лечебно-профилактического учреждения. В ходе работы были выполнены задачи: анализ системы публикации контента в медицинском учреждении, проектирование подсистемы защиты персональных данных.

Актуальность выпускной квалификационной работы определяется растущей информатизацией в медицинской области и автоматизацией деятельности за счет использования сетей передачи данных, которые объединяют медицинские и профилактические учреждения и интерес государственных структур к обеспечению защиты данных пациентов.

Целью работы является разработка подсистемы защиты персональных данных в системе публикации контента медицинского учреждения, путем создания проектного решения.

Для выполнения данной цели были поставлены следующие задачи:

- провести исследование порядка обработки персональных данных в системе публикации контента в медицинском учреждении;
- составление расчетов вероятности угроз;
- проведение обоснования выбора средств защиты информации для создания подсистемы защиты персональных данных;

– конструирование подсистемы защиты персональных данных в соответствии модели вероятностных угроз.

По итогу проделанной работы разработана подсистема защиты персональных данных в системе публикации контента в медицинском учреждении.

Abstract

The work consists of three sections in which analysis, design and development of a subsystem for the protection of personal data in the content publishing system in a medical institution are presented.

The paper consists of 50 pages, with 12 figures and 11 tables. While writing the thesis 23 reference sources were used.

Keywords: development, mobile application, personal data, information security, information systems.

The subject of the study are personal data protection systems in medical and preventive institutions.

The subject of this work is a subsystem for the protection of personal data in the publication system of the content of the treatment and prevention institution. In the course of the work the following tasks were accomplished: analysis of the content publishing system in a medical institution, design of a personal data protection subsystem.

The urgency of graduation work is determined by the growing informatization in the medical field and automation of activities through the use of data transmission networks that combine medical and preventive facilities and the interest of state structures to ensure the protection of these patients.

The aim of the work is to develop a subsystem for the protection of personal data in the publication system of the content of a medical institution, by creating a design solution.

To achieve this goal, the following tasks were set:

- conduct a study of the procedure for processing personal data in the content publishing system in a medical institution;
- compilation of a probability model for threats;
- carrying out of a substantiation of a choice of means of protection of the information for creation of a subsystem of protection of the personal data;

– the construction of a personal data protection subsystem in accordance with the model of probabilistic threats.

As a result of the work done, a subsystem for protecting personal data in the content publishing system in a medical institution was developed.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В медицинских лечебных учреждениях на сегодняшний день все больше внедряются информационные системы для **решения задач автоматизации административных процессов, хранения результатов обследовании**, анализов, а также других данных в цифровом виде для последующего поиска и обработки. Данный факт обуславливает потребность медицинских учреждений в обработки персональных данных пациентов, что и стало темой исследований данной бакалаврской работы.

Актуальность выпускной квалификационной работы определяется растущей информатизацией в медицинской области и автоматизацией деятельности за счет использования сетей передачи данных, которые объединяют медицинские и профилактические учреждения и интерес государственных структур к обеспечению защиты данных пациентов.

Цель выпускной квалификационной работы заключается в разработке подсистемы защиты персональных данных в системе публикации контента медицинского учреждения, путем создания проектного решения.

Объектом исследования является процесс представления данных в системе защиты данных в системе публикации контента типового лечебно-профилактического учреждения.

Предметом исследования в данной работе система по обеспечению информационной безопасности.

Для достижения поставленной цели необходимо решить задачи:

- провести исследование порядка обработки персональных данных в системе публикации контента в медицинском Учреждении на предмет соответствия требованиям 152-ФЗ и его подзаконным актам;
- составление модели вероятности угроз;
- проведение обоснования выбора средств защиты информации (далее – СЗИ) для создания подсистемы защиты персональных данных;

– конструирование подсистемы защиты персональных данных в соответствии с требованиями действующего законодательства.

Практическая значимость выпускной квалификационной работы заключается в разработке проекта подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении. Система публикации контента — это совместный проект студентов тольяттинского государственного университета, разрабатываемый на кафедре прикладной математики и информатики. Главная задача проекта предоставление мобильного доступа медицинскому персоналу данных о пациенте.

В первой главе данной работы произведен анализ нормативно правовых актов, касающихся обработки персональных данных и анализ текущей реализации системы публикации.

Во второй главе произведено моделирование текущей системы на наличие актуальных угроз, сравнение различных средств по защите ПДн и проектирование подсистемы защиты персональных данных в системе публикации контента.

В третьей главе разобраны методы принятые для обеспечения защиты ПДн на сервере и мобильном клиенте.

В заключении подводятся итоги проделанной выпускной квалификационной работы.

1 АНАЛИЗ ПОДСИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В МЕДИЦИНСКОМ УЧРЕЖДЕНИИ

1.1 Анализ законодательной базы, регламентирующей сферу защиты персональных данных

Для того, чтобы оценить все особенности защиты персональных данных с точки зрения формирования подсистемы защиты персональных данных, необходимо рассмотреть основную законодательную практику, предусмотренную в Российской Федерации с учетом последних изменений.

В качестве основного нормативно-правового документа, регламентирующего защиту персональных данных, можно назвать Федеральный закон № 152 ФЗ «О персональных данных» от 27.07.2006 с учетом всех принятых позднее изменений и дополнений. В этом законе не только дается понятие о персональных данных, но и регулируются возможные, в том числе в медицинском учреждении, отношения по сбору, обработке и хранению информации, связанной с субъектами персональных данных [1].

Согласно данному закону, к персональным данным относится любая информация о физическом лице: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, идентификационные данные документов (паспорт, СНИЛС и т. п.), семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация. При этом под обработкой персональных данных понимаются такие действия с ними, как систематизация, накопление, хранение, уточнение, использование, распространение, обезличивание, блокирование, а также уничтожение данных.

Еще одним нормативно-правовым актом, определяющим использование персональных данных, является Постановление Правительства Российской Федерации № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008. Согласно этому документу, обработка персональных данных, содержащихся в защищенной системе либо извлеченных из подобной системы, считается неавтоматизированной, если такие действия с этими

данными, как использование, уточнение, распространение и уничтожение относительно каждого из субъектов персональных данных осуществляются при непосредственном участии самого субъекта, т. е. человека [2].

В более позднем Постановлении Правительства Российской Федерации от 1 ноября 2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» № 1119 уже строго прописываются требования, направленные на обеспечение информационной безопасности. Согласно этому Постановлению, защищенная система представляет собой информационную среду, обрабатывающую специальные категории персональных данных [3].

В тексте положения устанавливаются требования к обеспечению безопасности персональных данных при их обработке в защищенной сети с помощью систем защиты персональных данных, среди которых можно выделить следующие группы мероприятий:

- организационные меры;
- средства защиты информации (в том числе и шифровальные средства);
- средства предотвращения несанкционированного доступа;
- средства предотвращения утечки информации по техническим каналам;
- программно-технические воздействия на технические средства обработки персональных данных.

В определенном смысле переломным моментом в развитии нормативно-правовой базы по защите персональных данных можно считать Приказ Федеральной службы безопасности Российской Федерации № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 14.02.2013. Благодаря появлению данного документа, была реализована первая попытка объединения в одном нормативно-правовом акте самых основных моментов, связанных с защитой персональных данных. Помимо этого, в данном документе приводится пред-

варительная классификация всех средств и систем защиты информации, имеющей непосредственное отношение к персональным данным [4].

Анализ рассмотренной законодательной базы показывает, что в качестве основных мер, обеспечивающих поддержание стабильно надежного уровня защиты передаваемых в локальной сети персональных данных, необходимо применять защищенные каналы связи. На основании концепции и требованиям к комплексной медицинской информационной системе, разработанной министерством здравоохранения и социального развития самарской области, для организации криптографической защиты каналов связи при информационном обмене в составе медицинских информационных систем используются технологии построения виртуальных частных сетей [13].

Последовательный анализ вышеприведенных документов позволяет сформулировать алгоритм действий необходимых для разработки средств защиты ПДн:

- обследование текущей системы обработки ПДн;
- определение уровня защищенности;
- разработка модели угроз;
- оптимизация процессов обработки ПДн;
- создание системы защиты ПДн.

1.2 Анализ архитектуры системы публикации контента в медицинских учреждениях

На сегодняшний день для доступа к информационным системам медицинского учреждения используются автоматизированные рабочие места с установленными на их специализированного программного обеспечения.

Автоматизированные рабочие места в медицинских учреждениях представляют из себя рабочее пространство с вычислительной техникой и программным обеспечением, обеспечивающие сбор, хранение и обработку ме-

дицинской информации с целью принятия организационных, диагностических и других решений.

Типовая схема работы информационной системы медицинского учреждения представлена на рисунке 1.1.

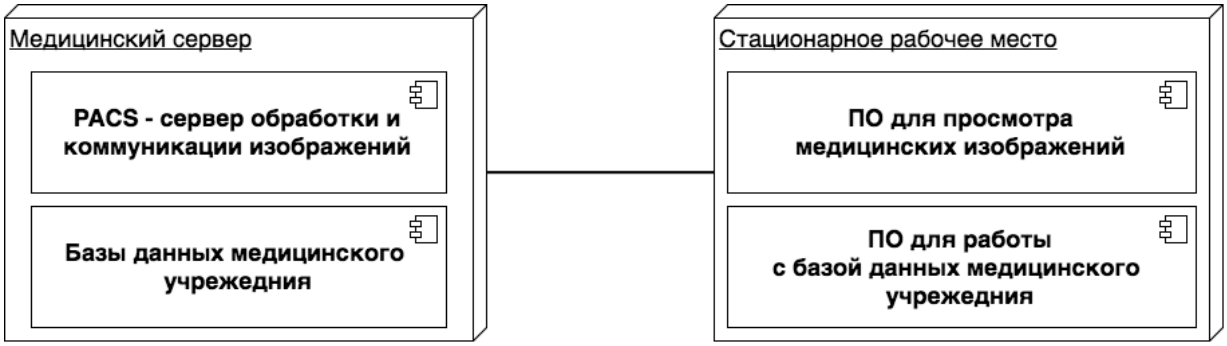

Рисунок 1.1 – Диаграмма компонентов типовой системы взаимодействия с контентом в медицинском учреждении

Система публикации контента предлагает дополнение к текущей архитектуре. Для организации мобильного доступа к информационной системе организуется промежуточный сервер системы публикации контента, который занимается агрегацией данных из информационных систем медицинского учреждения и представлением их для мобильного устройства. Диаграмма компонентов системы публикации контента представлена на рисунке 1.2.

Согласно диаграмме система публикации контента имеет соединение с текущей архитектурой медицинского учреждения и имеет в себе два компонента: промежуточную систему хранения и сервер управления контентом. С сервером управления контентом взаимодействует мобильное устройство, имеющее в себе два компонента: браузер и клиент для просмотра медицинских изображений. Так как мобильное устройство подразумевает беспроводные способы подключения к сети, стоит отдельно рассмотреть способ передачи данных между мобильным клиентом и сервером. В проекте системы публикации контента беспроводное соединение между мобильным устройством и сервером происходит по беспроводной сети WiFi.

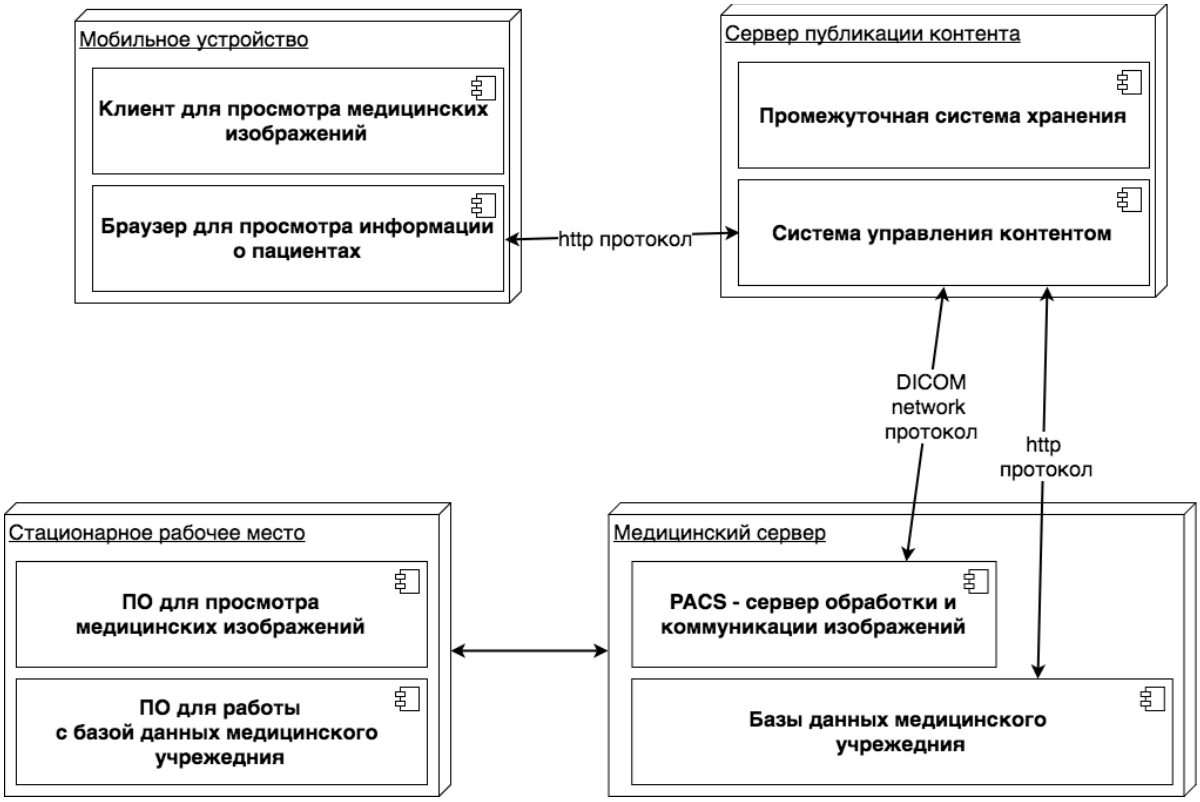

Рисунок 1.2 – Диаграмма компонентов системы публикации контента в медицинском учреждении

На основании анализа нормативно-правовых актов был сформулирован алгоритм действий, необходимых для создания средств защиты персональных данных также сформулирован технических подход к организации защиты беспроводного канала связи.

2 ПРОЕКТИРОВАНИЕ ПОДСИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Методы направленные на организацию защиты персональных данных в медицинском учреждении

Для выбора и реализации методов по защите информационной системы, в которой присутствует обработка персональных данных, необходимо:

- составить модель вероятности угроз;
- проанализировать методы и способы, которые должны обеспечить нейтрализацию предполагаемых угроз безопасности при обработке и хранению ПДн;
- для установления перечня мер защиты ПДн определить исходный уровень защищенности (далее УЗ) информационной системы.

Уровни защищенности определяются на основании Постановления Правительства №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и представлены в таблице 2.1.

Таблица 2.1 – Определения уровня защищенности ПДн в ИСПДн

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип (НДВ в СПО)	2 тип (НДВ в ППО)	3 тип (нет НДВ)
Специальные персональные данные касающиеся: расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных	Не сотрудников	Более 100 000	УЗ 1	УЗ 1	УЗ 2
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Любое	УЗ 1	УЗ 2	УЗ 3

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип (НДВ в СПО)	2 тип (НДВ в ППО)	3 тип (нет НДВ)
Биометрические сведения, на основании которых можно установить его личность	Любых	Любое	УЗ 1	УЗ 2	УЗ 3
Общедоступные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных"	Не сотрудников	Более 100 000	УЗ 2	УЗ 2	УЗ 2
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 2	УЗ 3	УЗ 4
Иные если персональные данные субъектов персональных данных, не представленные в трех предыдущих группах.	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 1	УЗ 3	УЗ 4

Сокращения, встречаемые в таблице:

- НДВ — не декларированные возможности;
- СПО — системное программное обеспечение;
- ППО — прикладное программное обеспечение.

Соответственно от уровня защищенности производится выбор мер по защите ПДн. На основании сравнения можно сделать вывод, что система публикации контента в медицинском учреждении имеет УЗ 3. В таблице 2.2 приводится печень мер с сопоставлением УЗ ИСПДн.

Таблица 2.2 – Определение минимального перечня мероприятий по защите ПДн

Перечень мер защиты	Уровни защищенности			
	1	2	3	4
Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	+	+	+	+
Обеспечение сохранности носителей персональных данных	+	+	+	+
Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	+	+	+	+
Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	+	+	+	+
Назначение должностного лица, ответственного за обеспечение безопасности персональных данных в ИСПДн	+	+	+	-
Ограничение доступа к содержанию электронного журнала сообщений	+	+	-	-
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе	+	-	-	-
Создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности	+	-	-	-

Для соответствия требованиям по организации защиты ПДн в системе публикации контента из всех действий по уровню защищенности 3 необходимо произвести расчет вероятности угроз. Данная модель необходима для выбора метода и средств необходимых в системе защиты персональных данных.

2.2 Расчет реализации угроз информационной безопасности для системы публикации контента в медицинском учреждении

Для составления модели возможности реализации угрозы используются два показателя: уровень исходной защищенности ИСПДн и вероятность реализации рассматриваемой угрозы.

Для нахождения уровня исходной защищенности системы публикации в медицинском учреждении был произведен анализ структурно-функциональных характеристик информационной системы. Анализ приведен в таблице 2.4.

Таблица 2.4 – Показатели исходной защищенности системы публикации в медицинском учреждении

Структурно-функциональные характеристики информационной системы, условия ее эксплуатации		Уровень проектной защищенности		
Категория	Показатель	Высокий	Средний	Низкий
По структуре информационной системы	Распределенная информационная система	0	0	1
По используемым информационным технологиям	Системы на основе виртуализации	0	0	1
По используемым информационным технологиям	Системы с мобильными устройствами	0	0	1
По архитектуре информационной системы	Системы на основе тонкого клиента	0	0	1
По архитектуре информационной системы	Системы с удаленным доступом пользователей	0	0	1
По архитектуре информационной системы	Использование выделенных каналов связи	0	1	0
По наличию (отсутствию) взаимосвязей с иными информационными системами	Взаимодействующая с системами	0	0	1

Структурно-функциональные характеристики информационной системы, условия ее эксплуатации		Уровень проектной защищенности		
Категория	Показатель	Высокий	Средний	Низкий
По наличию взаимосвязей к сетям связи общего пользования	Неподключенная	1	0	0
По размещению технических средств	Расположенные в пределах одной контролируемой зоны	1	0	0
По режимам обработки информации	Многопользовательский	0	0	1
По режимам разграничения прав доступа	С разграничением	0	1	0
По режимам разделения функций по управлению информационной системой	Использование выделенных каналов для администрирования	0	1	0
По подходам к сегментированию информационной системы	Без сегментирования	0	0	1
Итог		2	3	8
Процентный уровень исходной проектной защищенности		15.38%	23.08%	61.54%

Под уровнем исходной степени защищенности определяют:

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик соответствуют уровню «высокий».
2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний».
3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

Для составления расчетов актуальных угроз безопасности персональных данных составляется таблица, где к каждой угрозе ставится коэффициенты

исходного уровня защищенности и вероятностной оценки реализации угрозы.

Числовой коэффициент y_1 ставится в соответствии градации степени исходной защищенности:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Под вероятностной оценкой реализации угрозы принимают показатель, характеризирующий, насколько вероятна реализация уязвимости. Существуют четыре градации этого показателя:

1) маловероятно – отсутствуют предпосылки для осуществления угрозы;
2) низкая вероятность – предпосылки для реализации угрозы существуют, но приняты меры, затрудняющие эксплуатация уязвимости;
3) средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;
4) высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

Числовой коэффициент y_2 – вероятностная оценка реализации угрозы определяет:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением

$$Y = \frac{y_1 + y_2}{20},$$

(2.1)

где: y_1 – степень исходной защищенности;

y_2 – вероятностная оценка реализации угрозы;

Y – коэффициент реализуемости угрозы.

По значению коэффициента реализуемости угрозы Y формируется интерпретация реализуемости угрозы следующим образом:

- если $0 \leq Y \leq 0{,}3$, то возможность реализации угрозы признается низкой;
- если $0{,}3 < Y \leq 0{,}6$, то возможность реализации угрозы признается средней;
- если $0{,}6 < Y \leq 0{,}8$, то возможность реализации угрозы признается высокой;
- если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой.

На основании этой формулы был произведен расчет реализации угроз, представленный в таблице 2.5.

Таблица 2.5 – Расчет возможности реализации угроз

Угроза	Исходная защищенность системы публикации контента (y_1)	Вероятностная оценка реализации угрозы (y_2)	Вероятность реализации угрозы (Y)
Несанкционированный анализ сетевого трафика	6	7	0,65
Кража ПДн путем копирования на внешний носитель	3	2	0,25
Подмена или модификация текущего приложения обрабатывающего ПДн	6	1	0,35
Использование уязвимых мобильных ОС и приложени	1	3	0,2

Угроза	Исходная защищенность системы публикации контента (y_1)	Вероятностная оценка реализации угрозы (y_2)	Вероятность реализации угрозы (Y)
Раскрытие данных за счет побочных электромагнитных излучении и наводок	3	1	0,2
Соединение с недоверенным сервисом	3	4	0,35
Затор (Jamming) или Затопление (Flooding). Атаки, рассчитанные на создание помех или переполнения сети. С целью отказа работы системы.	2	2	0,2
НСД к ресурсам организации содержащие коммерческую тайну или ПДн	4	4	0,4

На основании приведенных расчётов вероятности угроз можно сделать вывод по уязвимым местам в системе публикации контента. Отдельно выделить угрозы с вероятностью реализации выше 0,6. Угроза «несанкционированный анализ сетевого трафика» имеет коэффициент 0,65, поэтому реализация методов по устранению этой угрозы имеет высокий приоритет. Так же в системе необходимо проработать вопросы по устранению угроз имеющие коэффициент выше 0,3:

– соединение с недоверенным сервисом;

– НСД к ресурсам организации, содержащие коммерческую тайну или ПДн;
– подмена или модификация текущего приложения обрабатывающего ПДн.

На основании выделенных угроз можно произвести формирование требований к подсистеме защиты персональных данных.

2.3 Формирование требований для подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении

Для формирования требований к подсистеме защиты ПДн воспользуемся классификацией FURPS+ [23].

Функциональными требованиями для подсистемы защиты персональный

данных в системе публикации контента являются организация защиты канала связи между сервером и мобильным устройством и возможность модерирования доступа к системе публикации контента.

С точки зрения удобства использования в подсистеме необходимо реализовать простоту работы для нетехнического персонала медицинского учреждения. При работе на мобильном устройстве пользователь не должен заходить в настройки системы и настраивать подключение к серверу.

Требование по надежности является основным для систем защиты ПДн. В рамках разработки подсистемы защиты персональных данных необходимо проработать вопросы стабильности и безопасности сетевого соединения. Перечень требований к подсистеме защиты персональных данных в системе публикации контента в медицинском учреждении представлен в таблице 2.6.

Таблица 2.6 – Требования к подсистеме защиты персональных данных в системе публикации контента в медицинском учреждении

№	Требование	Статус	Полезность	Обоснование выбора

№	Требование	Статус	Полезность	Обоснование выбора
Funcrionality – Функциональные требования				
1.	Создание защищенного канала соединения мобильного устройства и сервера	Одобренные	Критичное	В подсистеме должен быть реализован компонент создания защищенного VPN соединения
2.	Мобильное устройство должно без лишних настроек подключаться к защищенному серверу	Одобренные	Важное	В подсистеме должен быть реализован компонент мобильного клиента для создания подключения к защищенному серверу
3.	Администрирование ключей для подключения к серверу	Одобренные	Важное	В приложении должен быть реализован функционал для модерирования ключей для подключения к серверу
Usability – Требования к удобству использования				
4.	Мобильное приложение должно формировать вывод данных в виде статус бара для визуализации параметров текущего подключения	Одобренные	Критичное	Мобильные приложения реализуют отображение статусный строки состояния
Performance – Требования к производительности				
5.	Скорость соединения по защищенному каналу должна иметь минимальные потери и должна составлять не менее 25 Мбит/с	Одобренные	Критичное	Методы для защиты персональных данных используемые в подсистеме должны поддерживать канал связи, требуемый для работы мобильного приложения системы публикации контента
Physical requirements – Физические требования				
6.	Устройство должно иметь разъем для карты памяти формата microSD	Одобренные	Критичное	Устройство должно будет иметь разъем под карты в формате microSD для реализации подключения по ключу находящегося на внеш-

№	Требование	Статус	Полезность	Обоснование выбора
				нем носителе
7.	Наличие интернет-соединения по беспроводной сети WiFi	Одобренные	Критичное	На устройстве должно присутствовать для подключения по беспроводной сети WiFi

Подсистема должна создавать защищенный канал соединения с минимальными потерями в скорости. В приложении на мобильном устройстве необходимо проработать систему визуализации параметров текущего подключения. Необходимо разработать модуль администрирования ключей для подключения к серверу публикации контента.

2.4 Выбор средств защиты соединения между сервером публикации контента и мобильным клиентом

Для организации подсистемы защиты ПДн по каналу связи в системе публикации контента требуется произвести анализ способов организации защиты сетевого соединения. На основании концепции и требованиям к комплексной медицинской информационной системе, разработанной министерством здравоохранения и социального развития самарской области, для организации криптографической защиты каналов связи при информационном обмене в составе медицинских информационных систем используются технологии построения виртуальных частных сетей [13]. По данным условиям подходит технология VPN (Virtual Private Network – виртуальная частная сеть).

VPN — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети. Преимущества использования VPN для защиты канала является возможность применение механизмов шифрования передаваемых пакетов.

Сравнение технологии реализации VPN соединений представлено в таблице 2.7.

Таблица 2.7 – Сравнение технологии реализации VPN

Тип VPN	Высокая скорость работы	Защищенность канала связи	Поддержка мобильными устройствами	Возможность модификации	Итог
PPTP	1	0	1	0	2
L2TP -IPsec	0	1	1	0	2
OpenVPN	1	1	1	1	4

Среди технологий реализации был сделан выбор в пользу OpenVPN, который имеет высокую скорость передачи данных и открытый исходный код реализации что позволит создать и настроить под свои нужды подсистему защиты персональных данных при передаче по беспроводной сети.

2.5 Проектирование диаграммы прецедентов подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении

В результате проведённого анализа системы публикации контента было разработано решение по внедрению в текущую архитектуру системы двух компонентов для организации защищенного сетевого соединения между сервером и мобильным клиентом.

В рамках проектирования подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении была разработана диаграмма прецедентов, представленная на рисунке 2.1. Согласно ей администратор подсистемы может создавать и удалять ключи для организации доступа к серверу публикации контента и так же записывать ключи на microSD носитель и передает его медицинскому персоналу. В свою очередь медицинскому персоналу для доступа к системе необходимо вставить microSD носитель в мобильное устройство и пройти аутентификацию согласно данному ему ключу.

Актеры, представленные на диаграмме прецедентов:

1. Пользователь системы – человек, использующий мобильное приложение для работы с системой публикации контента.
2. Администратор системы – человек, управляющий ключами для подключения к OpenVPN серверу.

Прецеденты разрабатываемого приложения описаны в таблицах 2.8, 2.9, 2.10.

Рисунок 2.1 – Диаграмма прецедентов подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении

Таблица 2.8 – Прецедент «Получение расписания групп»

Прецедент: Создание ключа для подключения
ID: 1
Краткое описание: Реализация функции создания ключа для подключения.
Главные актеры: 1. Администратор системы
Второстепенные актеры:
Предусловие: Прецедент начинается по инициативе администратора системы
Основной поток:

Прецедент: Создание ключа для подключения
1. Администратора системы вводит параметры ключа для подключения. 2. Приложение подает команды OpenVPN серверу для создания ключа. 3. Приложение записывает данные ключа в базу данных ключей.
Постусловие: Приложение получило и создало ключ для подключения к OpenVPN серверу
Альтернативные потоки: Нет

Таблица 2.9 – Прецедент «Отзыв сертификата ключа для подключения»

Прецедент: Отзыв сертификата ключа для подключения
ID: 2
Краткое описание: Реализация функции отзыва ключа для подключения.
Главные актеры: 1. Администратор системы
Второстепенные актеры:
Предусловие: Прецедент начинается по инициативе администратора системы
Основной поток: 1. Администратор системы выбирает номер ключа, для удаления из списка имен. 2. Приложение подает команды OpenVPN серверу для отзыва ключа. 3. Приложение удаляет данные ключа из базы данных ключей.
Постусловие: Приложение отозвало ключ для подключения к OpenVPN серверу
Альтернативные потоки: Нет

Таблица 2.10 – Прецедент «Аутентификация пользователя»

Прецедент: Аутентификация пользователя
ID: 3
Краткое описание: Реализация функции для организации аутентификация пользователя к серверу

Прецедент: Аутентификация пользователя
OpenVPN.
Главные актеры: 2. Медицинский персонал
Второстепенные актеры:
Предусловие: Прецедент начинается по инициативе медицинского персонала
Основной поток: 1. Сотрудник медицинского учреждения вставляет microSD карту с ключом для подключения OpenVPN серверу в мобильное устройство 2. Сотрудник медицинского учреждения запускает приложение для доступа к системе публикации контента. 3. Модуль приложения для установления соединения с OpenVPN сервером, считывает ключ для подключения с microSD карты. 4. Модуль приложения для установления соединения с OpenVPN сервером, запрашивает доступ к OpenVPN серверу. 5. Модуль приложения для установления соединения с OpenVPN сервером, создает соединение с сервером OpenVPN.
Постусловие: Приложение установило соединение с системой публикации контента
Альтернативные потоки: Нет

Таким образом, в данном пункте были составлены основные прецеденты, описаны самые важные из них, выделены 2 актера, и составлена диаграмма прецедентов в которой было показано, какой актёр взаимодействует с каким прецедентом.

2.6 Проектирование диаграммы последовательности для подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении

В соответствии с диаграммой прецедентов необходимо реализовать диаграмму последовательности подсистемы защиты персональных данных. Подсистема должна представлять доступ к серверу публикации контента ме-

дицинскому персоналу. Для этого, подсистеме защиты персональных данных необходимо выполнить следующий алгоритм действий:

1. Для того, чтобы получить ключ для подключения к системе, пользователь публикации должен запросить его у администратора системы
2. Администратор через интерфейс управления OpenVPN сервером подает запрос на создание ключа.
3. Администратор копирует ключ с сервера публикации контента и записывает его на microSD карту, которую передает пользователю обратившегося за ключом.
4. Пользователь вставляет microSD в мобильное устройство и у него происходит подключение по каналу OpenVPN к серверу публикации контента автоматически.

Диаграмма последовательности разработанная в рамках данной работы, представленная на рисунке 2.2.

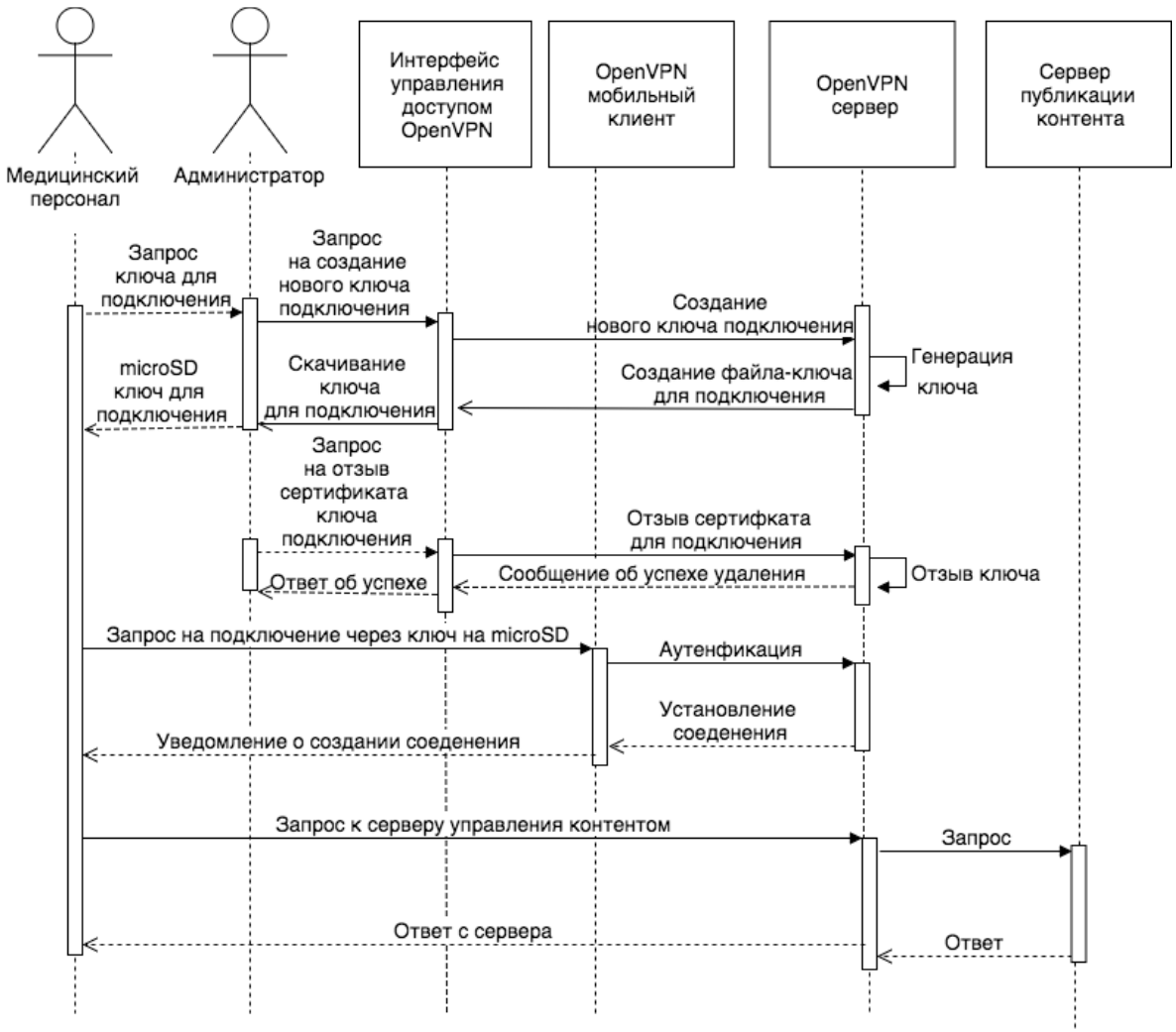

Рисунок 2.2 –Диаграмма последовательности подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении

Построенная диаграмма последовательности отображает динамический аспект подсистемы защиты персональных данных и позволяет определить порядок реализации функций.

2.7 Проектирование диаграммы компонентов для подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении

Для реализации защиты канала связи в системе публикации контента была выбрана технология OpenVPN. Диаграмма компонентов подсистемы защиты персональных данных представлена на рисунке 2.3.

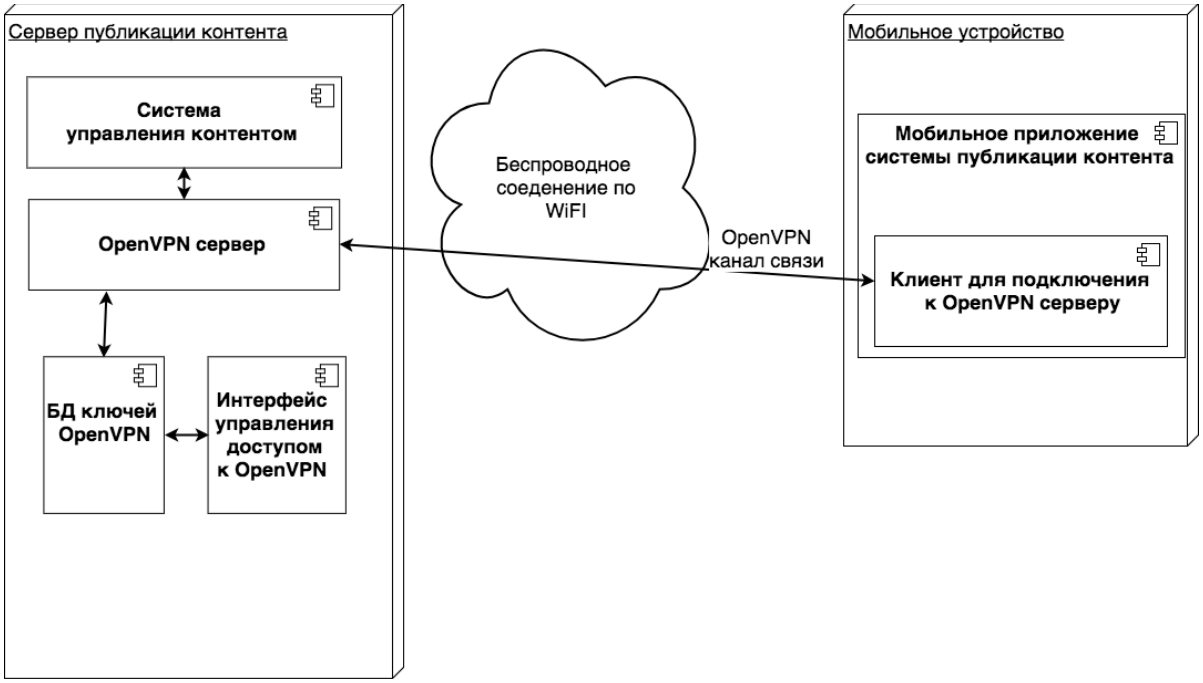

Рисунок 2.3 –Диаграмма компонентов подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении

Компонент OpenVPN сервер является стандартной реализацией. Компонент интерфейса управления доступом к OpenVPN необходимо разработать для взаимодействия с базой данных ключей OpenVPN. Компонент, находящийся в составе мобильного устройства – клиент для подключения к OpenVPN серверу, разрабатывается в рамках данной работы и взаимодействует с мобильным приложением системы публикации контента. Подключение к серверу должно происходить без взаимодействий с меню настроек устройства и быть понятным для пользователя системы публикации контента.

Для реализации предложенного архитектурного решения были поставлены следующие задачи:

– разработать интерфейс управления доступом к OpenVPN серверу, в котором будет реализовано администрирование ключей для подключения;

– разработать модуль для мобильного клиента способного подключаться к серверу публикации контента по зашифрованному туннельному шифрованию;
– интегрировать подсистему защиты ПДн в текущую систему публикации контента.

Таким образом, во второй главе произведено проектирование средств по защите ПДн. В ходе составления вероятностной модели угроз было выявлено, что узким местом обработки ПДн является соединение сервера публикации контента с мобильным устройством. На основании чего было произведено исследование технологий по организации VPN. Для обеспечения защиты лучшим решением по совокупности критериев была определена реализация технологии OpenVPN. В рамках проектирования была составлена Диаграмма компонентов, прецедентов и последовательности планируемой подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении.

3 РАЗРАБОТКА ПОДСИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Реализация компонента интерфейс управления доступом к OpenVPN серверу

Для организации настройки OpenVPN и генерации ключей подключения в рамках выпускной квалификационной работы был разработан bash скрипт, работающий на дистрибутивах ОС Linux разработанных на базе Debian. Листинг файла скрипта на языке bash приведён в Приложении А.

При запуске скрипт анализирует файловую систему на наличие конфигурационного файла OpenVPN сервера по стандартному пути (/etc/openvpn/server.conf) и запускает один из двух режимов работы.

При отсутствии конфигурационного файла сервера скрипт запускает режим установки OpenVPN. Скрипт определяет ip адрес сервера во внутренней корпоративной сети с помощью команды (ip addr show) и предлагает его как значение по умолчанию для настройки сервера. Так же во время выполнения скрипта спрашивается порт для работы, настройки DNS северов, и имя ключа для подключения, который автоматически сгенерируется после завершения процесса установки.

При наличии конфигурационного файла по пути (/etc/openvpn/server.conf) скрипт запускает режим администрирования из командный строки. В этом режиме скрипт предлагает 4 действия на выбор:

1. Добавление нового пользователя;
2. Отзыв сертификата старого пользователя;
3. Удаление OpenVPN сервера;
4. Выход из меню (завершение работы скрипта).

Полный алгоритм работы скрипта представлен на блок-схеме, изображенной на рисунке 3.1.

Для упрощения генерации новых ключей в скрипте во время установки происходит генерация файла шаблона client-common.txt. Блок схема алгоритма установки OpenVPN представлен на рисунке 3.2.

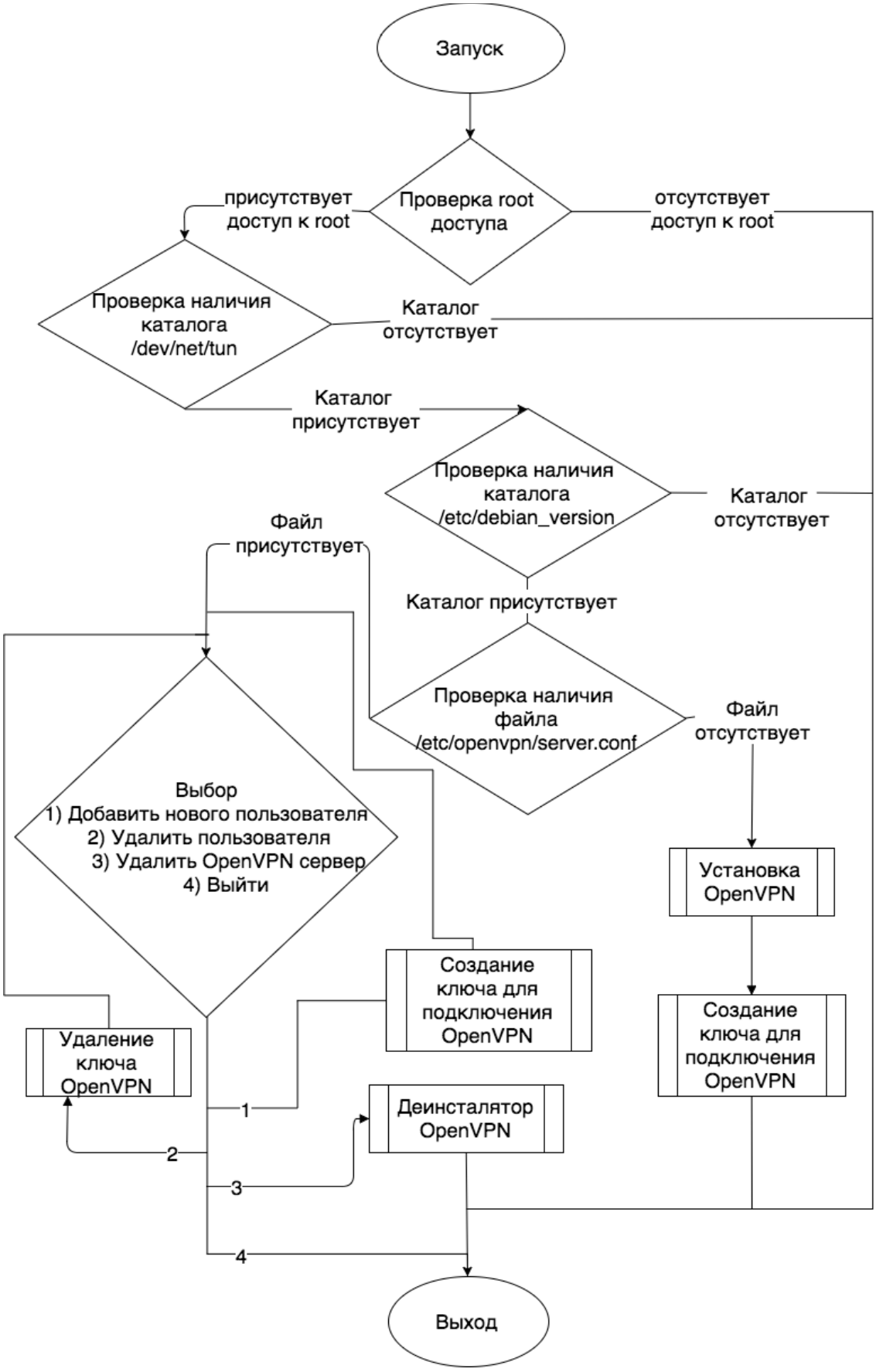

Рисунок 3.1 – Блок-схема алгоритма работы скрипта компонента администрирования OpenVPN сервера

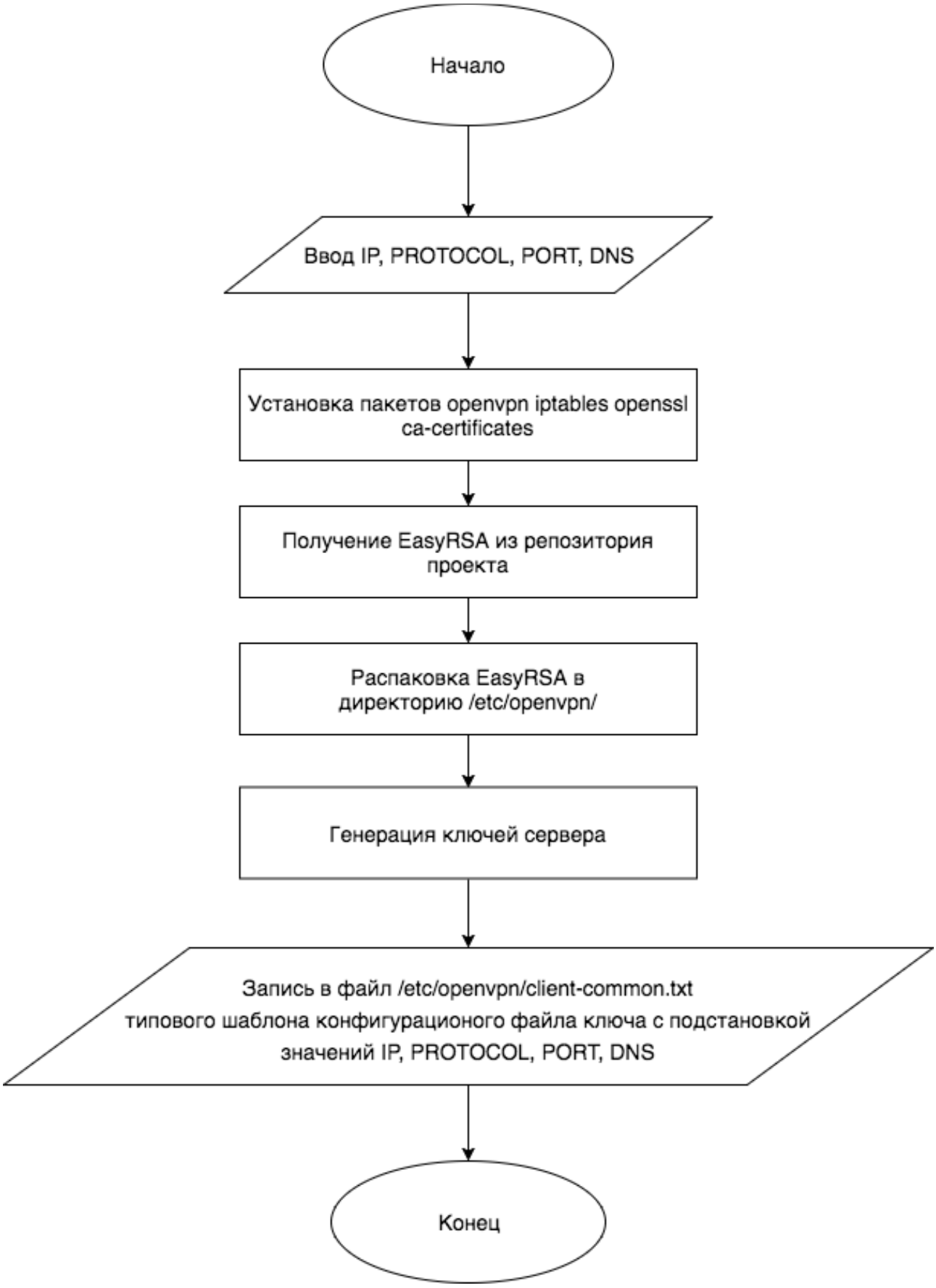

Рисунок 3.2 – Блок-схема алгоритма установки OpenVPN сервера

Для реализации функциональности по добавлению новых ключей интерфейс управления доступом к OpenVPN серверу скопировав текст из файла (client-common.txt) в конфигурационный файл для настройки подключения к OpenVPN и добавив в него необходимые текст ключа центра сертификации, сертификата и ключа сервера, подписи HMAC и файла Diffie-Hellman, будет создан файл готовый для создания подключения. Подробный алгоритм генерации нового ключа представлен на рисунке 3.3.

Для выбора ключа, у которого необходимо отозвать сертификат происходит вывод всех строк из файла /etc/openvpn/easy-rsa/pki/index.txt с их нумерацией. Выбранный номер используется в качестве значения для ключа у которого отзовут сертификат. Алгоритм работы удаления ключа для подключения представлен н рисунке 3.4.

Алгоритм удаления OpenVPN сервера представлен на рисунке 3.5.

3.2 Реализация компонента клиент для подключения к серверу OpenVPN с мобильного устройства

Для разработки мобильного клиента была выбрана реализация с открытым исходным кодом проекта ics-openvpn. На основе кодовой базы ics-openvpn в рамках данной работы реализована функциональность создание VPN подключения на основе конфигурационного файла расширения ovpn, лежащего на microSD носителе.

В рамках работы над выпускной квалификационной работой был также разработан клиент, внедряемый в основное мобильное приложение системы публикации контента в медицинском учреждении. Для работы с методами и классами, которые присутствуют в проекте ics-openvpn был разработано приложение, в котором ics-openvpn является дополнительным модулем, реализующим функциональность только самого подключения. Остальные функции необходимые для работы (получение конфигурационного файла с носителя, отображение состояния подключения и управление подключением) приложения являются практической частью.

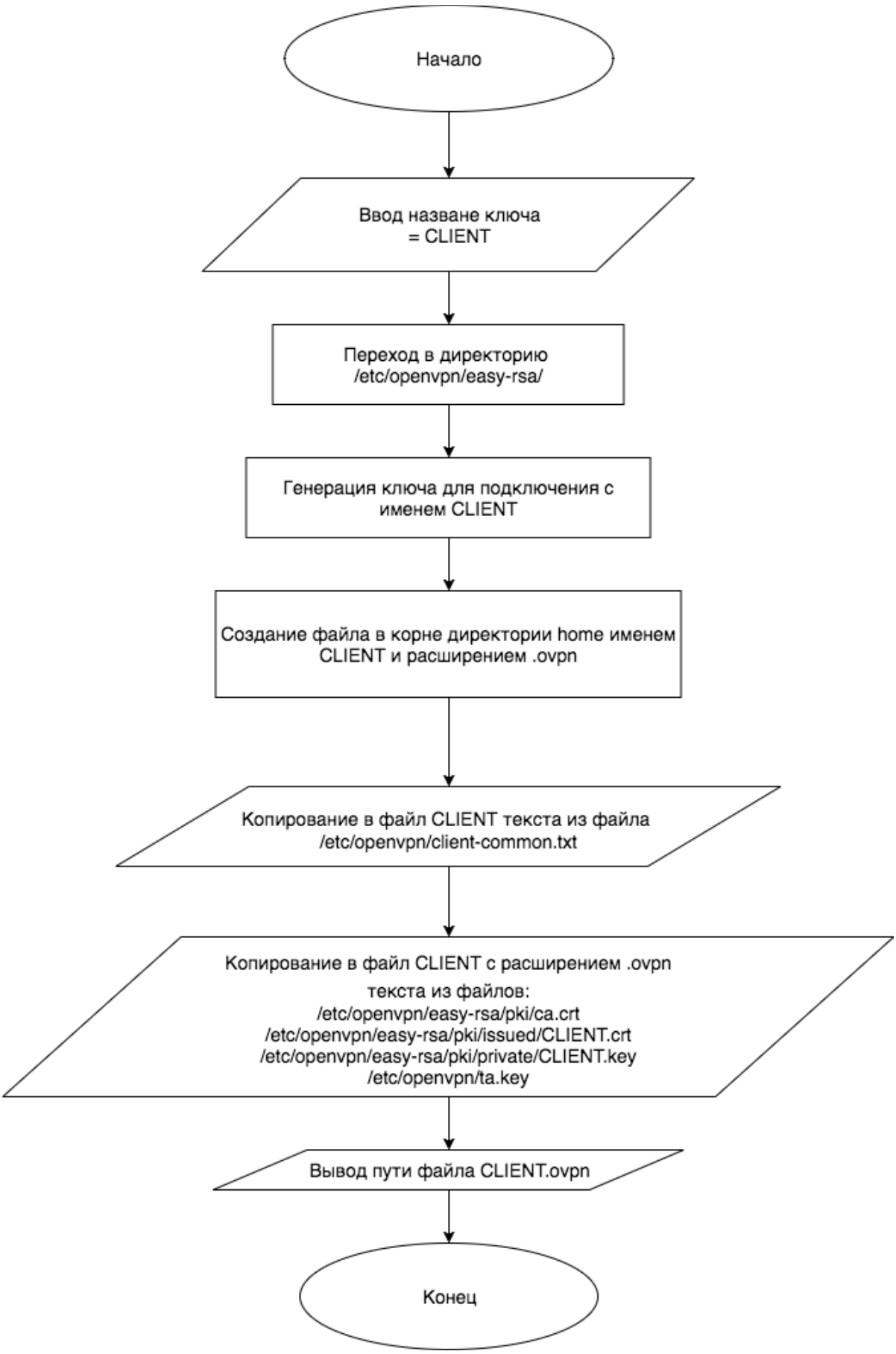

Рисунок 3.3 – Блок-схема алгоритма создания OpenVPN сервера

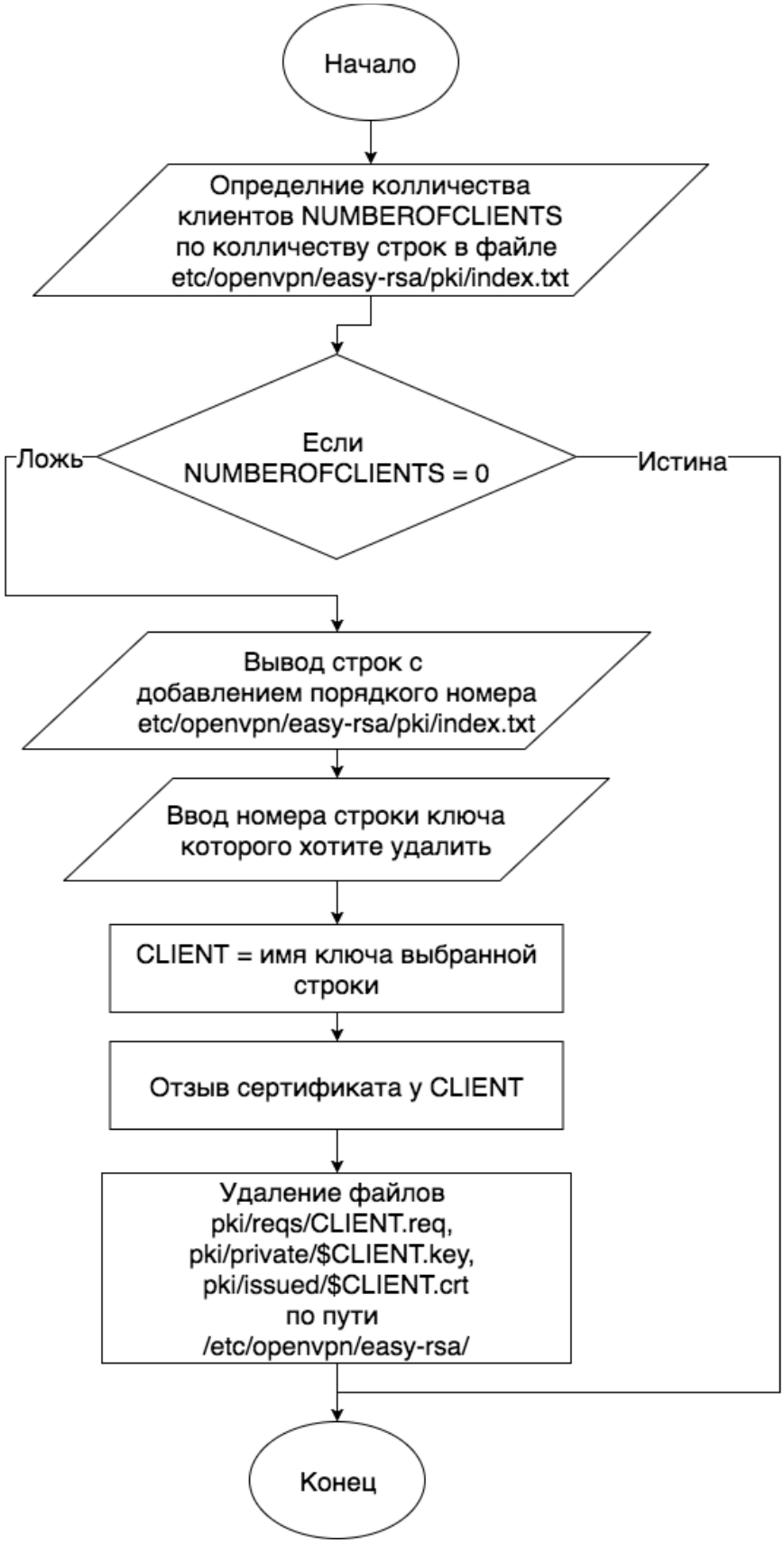

Рисунок 3.4 – Блок-схема алгоритма отзыва сертификата для клиента OpenVPN

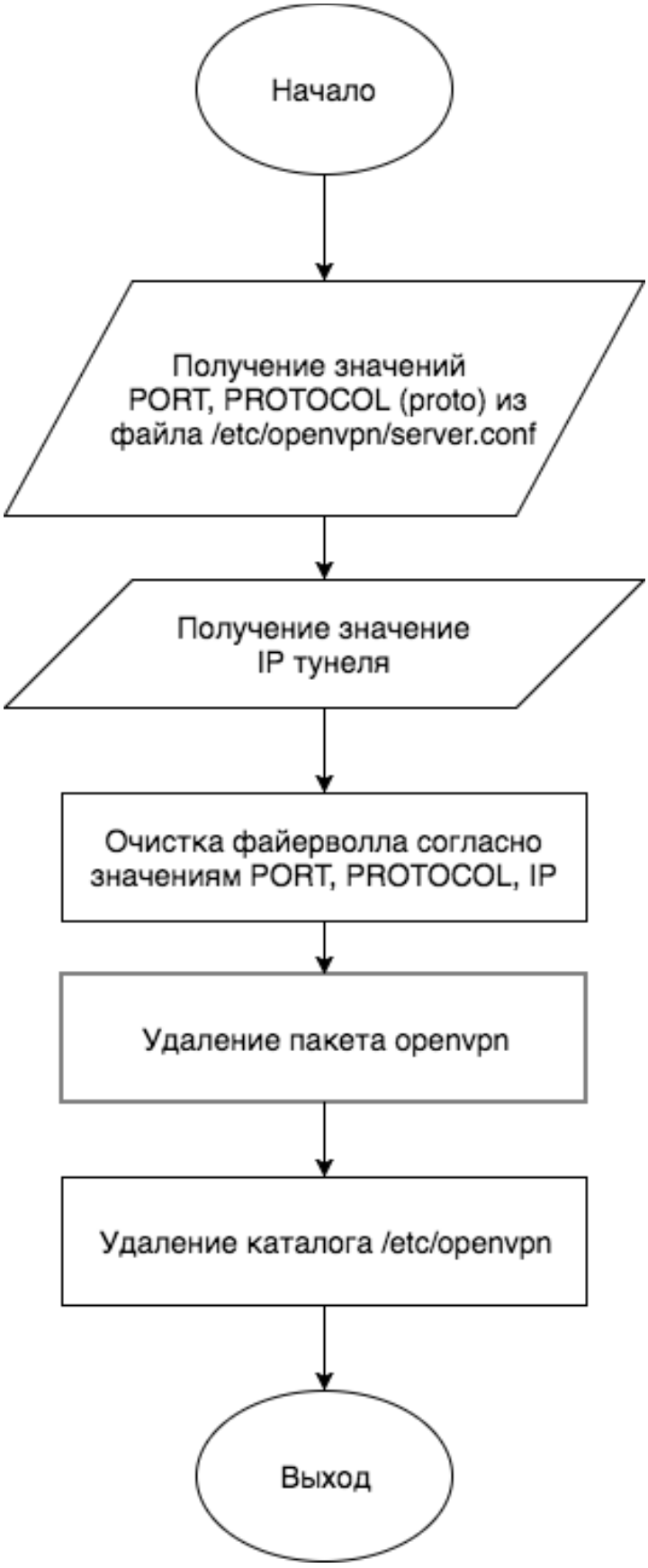

Рисунок 3.5 – Блок-схема алгоритма удаление OpenVPN сервера

Диаграмма классов разработанного модуля мобильного клиента изображена на рисунке 3.6. Единственный экран мобильного приложения определяется в классе MainActivity. Функция initVpn() в MainActivity создает объект типа VpnUiLogic и запускает у него метод init(). В методе init() создаёт объект типа OpenVpnConnectWrapper, который наследуется от VpnStatus.StateListener и вызывает у него такой же метод init() . В методе init() класса OpenVpnConnectWrapper активирует слушателя статуса VPN подключения и демонстрирует его в статусной строке Android. Так же в методе init() происходит создание объекта типа VpnAutoConfig. В классе VpnAutoConfig в методе getAutoConfigFromAsset(), который используя ключ файл расширения ovpn, создает строку для осуществления метода connectVPN().

Для подключения к серверу OpenVPN требуется вызвать метод connectVPN() объекта типа VpnUiLogic. Во время вызова будет произведен запуск метод connectToVpn() класса OpenVpnConnectWrapper. Метод connectToVpn() запускает методы для получения как строковое значения на основе файла расширения ovpn с заданным в программном коде параметрам пути и имени и создает подключение с помощью классов и методов из проекта ics-openvpn.

Для отключения от OpenVPN сервера так же вызывается метод из класса VpnUiLogic, с именем disconnectVpn(). Во время его исполнения вызывается метод disconnectFromVpn() класса OpenVpnConnectWrapper, который в свою очередь посылает ics-openvpn запрос классу DisconnectVpnActivity из проекта ics-openvpn на отключение VPN соединения.

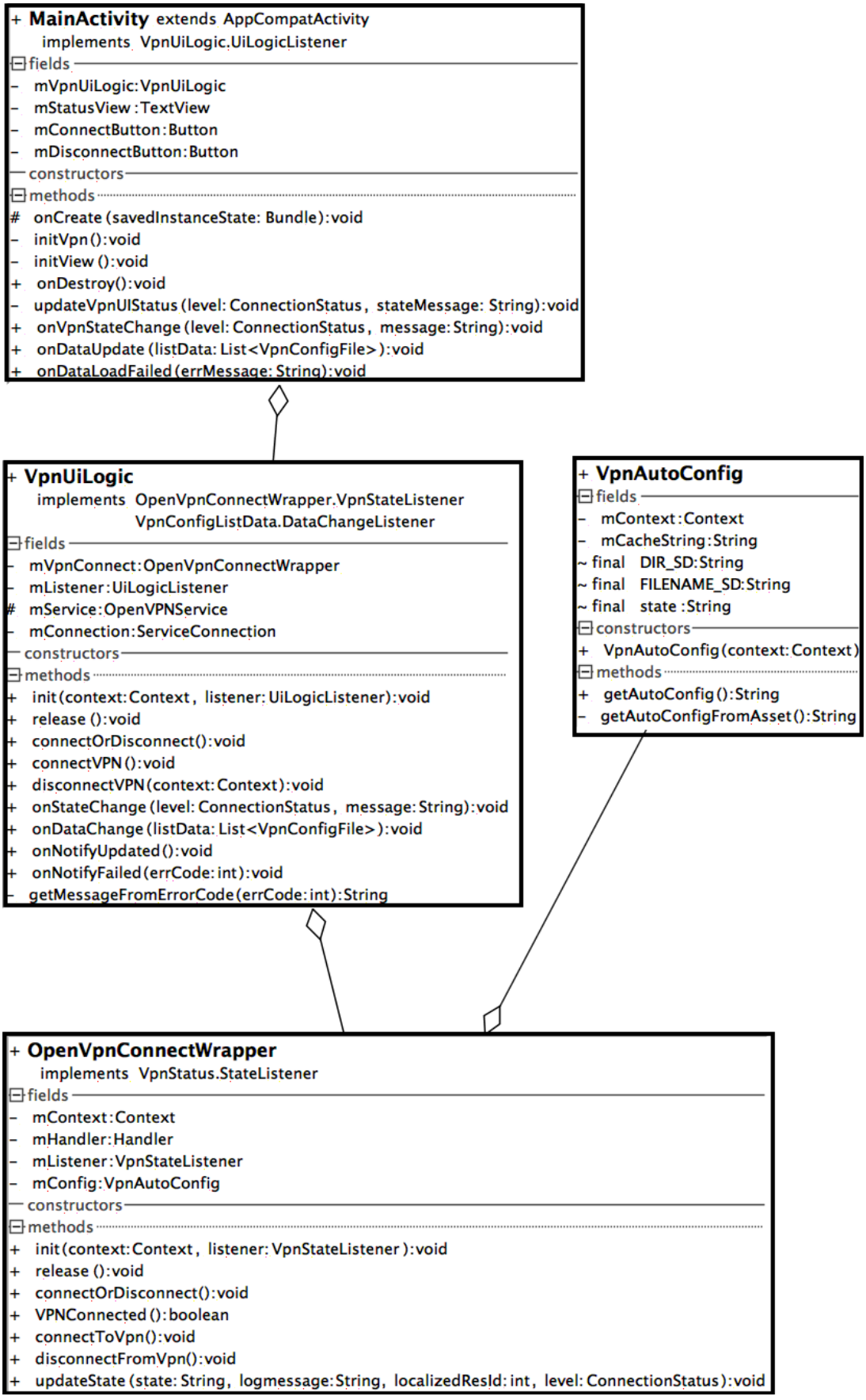

Рисунок 3.6 – Диаграмма классов модуля для подключения к OpenVPN серверу

Для авторизации используется стандартный для OpenVPN тип подключения по логину и паролю, сгенерированными при создании ovpn ключа – конфигурационного файла. Так как хранение и передача ключа не по защищенному каналу связи не соответствует стандартам защиты ПДн, для реализации этого аспекта была разработана подсистема хранения ключа – конфигурационного файла на физическом носителе. При наличии в устройстве microSD накопителя и запуска приложения – клиента, произойдет анализ файловой системы носителя и попытка подключения к OpenVPN серверу.

3.3 Разработка диаграммы развертывания подсистемы защиты персональных данных в системе публикации контента

Для развертывания подсистемы защиты персональных данных необходимо иметь сервер публикации контента, работающий на операционной системе Ubuntu минимальной версии 14.04. Установка сервера OpenVPN сервера происходит в компоненте администрирования OpenVPN сервера, который является интерфейсом для управления БД ключей для подключения. Для корректной работы OpenVPN сервера необходимо 15Мб ОЗУ.

На мобильном клиенте необходимо иметь операционную систему Android 4.1 так как модуль для подключения разрабатывался под эту платформу. Минимальная версия ОС должна быть 4.1 так как начиная с этой версии появилась реализация системного API VPN подключения.

Диаграмма развертывания подсистемы защиты персональных данных представлена на рисунке 3.7.

Инструкция по установке по установки подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении:

1. Загрузить bash скрипт openvpn-install.sh на сервер публикации контента.
2. Запустить скрипт и установить значения ip адреса сервера публикации контента, DNS сети и порта сервера.

3. Ввести значения имени и пароля ключа создаваемого для администрирования сервера OpenVPN.
4. Внедрить код проекта модуля для подключения к OpenVPN серверу в текущее мобильное приложение для работы с сервером публикации контента.

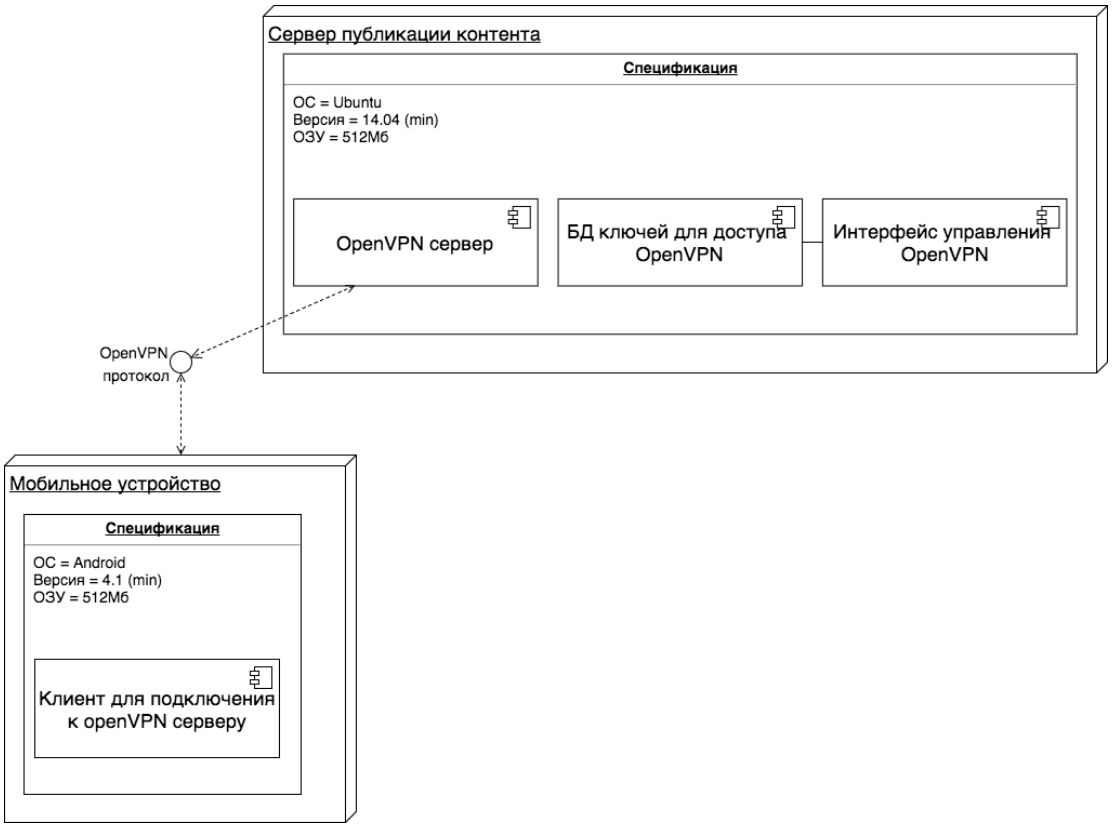

Рисунок 3.7 – Диаграмма развертывания подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении

Инструкция по добавлению нового пользователя в подсистеме защиты персональных данных в системе публикации контента в медицинском учреждении:

1. Запустить bash скрипт openvpn-install.sh на сервере публикации контента.
2. Выбрать из списка действие «Добавить нового пользователя».

3. Ввести имя ключа, срок действия ключа и пароль для осуществления подключения.
4. После прохождения процесса генерации ключа отобразится путь, где лежит ключ для подключения на сервере публикации контента. Затем следует скопировать файл ключа по предложенному пути на носитель microSD и передать его пользователю системы публикации контента.

Инструкция по удалению пользователя из подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении:

1. Запустить bash скрипт openvpn-install.sh на сервере публикации контента.
2. Выбрать из списка действие «Удалить пользователя».
3. Из предложенного списка выбрать необходимый номер имени ключа.
4. Дождаться окончания процесса отзыва сертификатов ключа и удаления ключа с сервера публикации контента.

Инструкция по подключению на мобильном устройстве к серверу системы публикации контента в медицинском учреждении с включенном модулем защиты персональных данных:

1. Вставить в мобильное устройство microSD карту с записанным на нее ключом для подключения (выдается администратором подсистемы защиты персональных данных).
2. Запустить приложение для доступа к системе публикации контента.
3. На появившемся всплывающим окне ввести пароль, заданный этому ключу администратором подсистемы защиты персональных данных.
4. Дождаться окончания процесса создания подключения к серверу публикации контента.

Таким образом, были сформулированы диаграмма развёртывания и инструкция по установке подсистемы защиты персональных данных в системе публикации контента.

В рамках разработки подсистемы защиты персональных данных в системе публикации контента в медицинском учреждении. Было разработано два компонента: bash скрипт для установки и администрирования OpenVPN сервера и модуль для мобильного клиента для подключения к серверу OpenVPN.

Компонент, разработанный для установки и администрирования OpenVPN хоть имеет ряд недостатков, связанных с удобством работы, имеет возможности по развитию в сторону добавления Российских алгоритмов шифрования и создание полноценного интерфейса администрирования сервера.

ЗАКЛЮЧЕНИЕ

Результатом выпускной квалификационной работы стала разработка проекта подсистемы защиты персональных данных системе публикации контента в медицинском учреждении.

Для разработки подсистемы защиты персональных данных произведен анализ нормативно правовых актов, касающихся обработки персональных данных и анализ текущей реализации системы публикации.

На основании анализа нормативно-правовых актов был сформулирован алгоритм действий, необходимых для создания средств защиты ПДн это:

- обследование текущей системы обработки ПДн;
- определение уровня защищенности;
- разработка модели угроз;
- оптимизация процессов обработки ПДн;
- создание подсистемы защиты ПДн.

Так же был произведен анализ архитектуры системы публикации контента. Также сформулирован технических подход к организации защиты беспроводного канала связи. Во второй главе произведен расчет вероятности различных угроз на наличие актуальных угроз, сравнение различных средств по защите ПДн и проектирование подсистемы защиты персональных данных в системе публикации контента.

Произведен анализ методов, направленных на организацию защиты персональных данных. В данной главе было определено что требуемый уровень защищенности для системы публикации контента в медицинском учреждении равен трем и был выявлен комплекс мер защиты необходимых для систем данного уровня защищенности.

Был произведен анализ классификаций угроз при обработке персональных данных. Перечень полученных угроз был использован для составления расчетов вероятности угроз.

Были сформированы требования по поддержки подсистемы защиты персональных данных. Подсистема должна создавать защищенный канал соединения с минимальными потерями в скорости. В приложении на мобильном устройстве необходимо проработать систему визуализации параметров текущего подключения. Необходимо разработать модуль администрирования ключей для подключения к серверу публикации контента.

Были рассмотрены различные технологии для реализации защищенных VPN соединений. В ходе сравнения была выбрана технология реализации с открытым исходным кодом OpenVPN как наиболее соответствующая для реализации подсистемы защиты персональных данных в системе публикации контента.

Было произведено проектирование подсистемы защиты персональных данных. Были разработаны: диаграмма прецедентов, диаграмма последовательности, диаграмма компонентов для реализации подсистемы защиты персональных данных.

Для организации настройки OpenVPN и генерации ключей подключения в рамках выпускной квалификационной работы был разработан bash скрипт, работающий на дистрибутивах ОС Linux разработанных на базе Debian.

Было представлено описание реализации компонента для подключения к серверу OpenVPN с мобильного устройства. Ключевой особенностью клиента является возможность для подключения к серверу по файлу ключу, расположенному на внешней карте памяти формата microSD. Данная возможность позволяет реализовать возможность подключения без дополнительных настроек со стороны пользователя системы публикации контента в медицинском учреждении.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

Нормативно-правовые акты

1. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ (ред. от 29.07.2017) "О персональных данных"// Собрание законодательства РФ. 2006. №31 (1 ч.). Ст. 3451;
2. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // Российская газета. 2008. 24 сентября;
3. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Российская газета. 2012. 7 ноября;
4. Приказ Федеральной службы безопасности Российской Федерации № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета. 2013. 22 мая;
5. Федеральный Российской Федерации закон от 27 июля 2006 года №149 «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. №31 (1 ч.). Ст. 3448;
6. Федеральный закон Российской Федерации от 29 ноября 2010 года №326 «Об обязательном медицинском страховании в Российской Федерации» // Собрание законодательства РФ. 2010. №49. Ст. 6422;
7. Постановление Правительства РФ от 17 ноября 2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета. 2007. 21 ноября;
8. Постановление Правительства РФ от 6 июля 2008 г. №512 «Об утверждении требований к материальным носителям биометрических персональ-

ных данных и технологиям хранения таких данных вне информационных систем персональных данных» // Российская газета. 2008. 7 ноября.

9. Постановление Правительства РФ от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // Российская газета. 2008. 24 сентября;
10. Постановление Правительства РФ от 4 октября 2010 г. № 782 «О Программе государственных гарантий оказания гражданам Российской Федерации бесплатной медицинской помощи на 2011 год» // Российская газета. 2010. 13 октября;
11. Постановление Правительства РФ от 21 марта 2012 г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» // Российская газета. 2012. 30 марта;
12. Приказ ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета. 2013. 22 мая.
13. Концепция и требования к комплексной медицинской информационной системе самарской области // [Электронный ресурс] : сайт министерства здравоохранения самарской области : http://minzdrav.samregion.ru/allfiles /

Научная и методическая литература

14. Защита конфиденциальности персональных данных с помощью обезличивания // Вестник АГГУ. - 2010, №2. С. 158-162.
15. Защита персональных данных работника // Сибирский торгово-экономический журнал. - 2008, №7.
16. Особенности регулирования защиты персональных данных работников на локальном уровне // Российское правоведение на рубеже веков: Трибуна

молодого ученого.: - Томск: Изд-во Том. ун-та. -2004. - Ч. 4 - С. 128-132.
Электронные ресурсы

17. Базовая модель угроз безопасности персональным данным при обработке в информационных системах персональных данных [Электронный ресурс] : Официальный сайт ФСТЭК России https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty
18. Код безопасности, ГК «Информзащита» [Электронный ресурс] : http://www.securitycode.ru/
19. Документация по проекту OpenVPN [Электронный ресурс] : OpenVPN сайт проекта :https://openvpn.net/index.php/open-source/documentation.html

Литература на иностранном языке

20. Smyth N. Android Studio Development Essentials // Neil Smyth // Android 6 Edition – Payload Media, 2015.
21. Crist E. Troublesshooting OpenVPN // Eric F Crist // - Pact Publishing, 2017
22. Wolfson M. Android Developer Tools Essentials – O'Reilly, 2013.
23. Alan Dennis, Barbara Haley Wixom, David Tegarden: Systems Analysis and Design with UML - 4th Edition, Wiley, 2012.
24. Kenett, Ron; Baker, Emanuel Software Process Quality: Management and Control, CRC Press, 1999.

ПРИЛОЖЕНИЕ А

Листинг разработанного файла openvpn-install.sh

```
#!/bin/bash
# OpenVPN installer  for Debian, Ubuntu
# For install  need run sudo bash openvpn-install.sh


if [[ "$EUID" -ne 0 ]]; then
    echo "Вы должны иметь root привелегии"
    exit 1
fi

if [[ ! -e /dev/net/tun ]]; then

    echo "TUN не доступен
Включите TUN после запустите скрипт"
    exit 2
fi

if [[ -e /etc/debian_version ]]; then
    OS=debian
    GROUPNAME=nogroup
    RCLOCAL='/etc/rc.local'
else
    echo"Похоже вы запускаете скрипт на не поддерживаемой системе. Поддержка осуществляется на Debian или Ubuntu"
    exit 3
fi

newclient () {
    cp /etc/openvpn/client-common.txt ~/$1.ovpn
    echo "<ca>">> ~/$1.ovpn
    cat /etc/openvpn/easy-rsa/pki/ca.crt >> ~/$1.ovpn
    echo "</ca>">> ~/$1.ovpn
    echo "<cert>">> ~/$1.ovpn
    cat /etc/openvpn/easy-rsa/pki/issued/$1.crt >> ~/$1.ovpn
    echo "</cert>">> ~/$1.ovpn
    echo "<key>">> ~/$1.ovpn
    cat /etc/openvpn/easy-rsa/pki/private/$1.key  >> ~/$1.ovpn
    echo "</key>">> ~/$1.ovpn
    echo "<tls-auth>">> ~/$1.ovpn
```

```
    cat /etc/openvpn/ta.key >> ~/$1.ovpn
    echo "</tls-auth>">> ~/$1.ovpn
}

IP=$(ip addr show)


if [[ -e /etc/openvpn/server.conf ]]; then
    while :
    do
    clear
        echo "OpenVPN установлен"
        echo ""
        echo "Что вы хотите сделать?"
        echo "   1) Добавить нового пользователя"
        echo "   2) Удалить пользователя"
        echo "   3) Удалить OpenVPN сервер"
        echo "   4) Выйти"
        read -p "Выберите [1-4]: " option
        case $option in
            1)
            echo ""
            echo "Введите имя ключа нового пользователя"
            echo "Только латиница и цифры"
            read -p "Client name: " -e -i client CLIENT
            cd /etc/openvpn/easy-rsa/
            ./easyrsa build-client-full $CLIENT nopass
            newclient "$CLIENT"
            echo ""
            echo "Client $CLIENT добавлен, файлконфигурациинаходитсяв"
~/"$CLIENT.ovpn"
            exit
            ;;
            2)

            NUMBEROFCLIENTS=$(tail -n +2 /etc/openvpn/easy-rsa/pki/index.txt |
grep -c "^V")
            if [[ "$NUMBEROFCLIENTS" = '0' ]]; then
                echo ""
                echo "Вы не имеете клиентов!"
                exit 6
            fi
            echo ""
            echo "Выберите клиента которого хотите удалить сертификат"
```

```
        tail -n +2 /etc/openvpn/easy-rsa/pki/index.txt | grep "^V" | cut -d '=' -f 2 | nl
-s ') '
        if [[ "$NUMBEROFCLIENTS" = '1' ]]; then
          read -p "Выберитеклиент [1]: " CLIENTNUMBER
        else
          read -p "Выберитеклиент [1-$NUMBEROFCLIENTS]: " CLIENT-
NUMBER
        fi
        CLIENT=$(tail -n +2 /etc/openvpn/easy-rsa/pki/index.txt | grep "^V"| cut -
d '=' -f 2 | sed -n "$CLIENTNUMBER"p)
        cd /etc/openvpn/easy-rsa/
        ./easyrsa --batch revoke $CLIENT
        EASYRSA_CRL_DAYS=3650 ./easyrsa gen-crl
        rm -rf pki/reqs/$CLIENT.req
        rm -rf pki/private/$CLIENT.key
        rm -rf pki/issued/$CLIENT.crt
        rm -rf /etc/openvpn/crl.pem
        cp /etc/openvpn/easy-rsa/pki/crl.pem /etc/openvpn/crl.pem
        chown nobody:$GROUPNAME /etc/openvpn/crl.pem
        echo ""
        echo "Сертификат для $CLIENT удален"
        exit
        ;;
        3)
        echo ""
        read -p "Вы хотите удалить OpenVPN? [y/n]: " -e -i n REMOVE
        if [[ "$REMOVE" = 'y' ]]; then
          PORT=$(grep '^port ' /etc/openvpn/server.conf | cut -d "" -f 2)
          PROTOCOL=$(grep '^proto ' /etc/openvpn/server.conf | cut -d "" -f 2)
          if pgrep firewalld; then
            IP=$(firewall-cmd --direct --get-rules ipv4 nat POSTROUTING | grep
'\-s 10.8.0.0/24 ""'"'"'!'"'"'" -d 10.8.0.0/24 -j SNAT --to '| cut -d "" -f 10)
            firewall-cmd --zone=public --remove-port=$PORT/$PROTOCOL
            firewall-cmd --zone=trusted --remove-source=10.8.0.0/24
            firewall-cmd --permanent --zone=public --remove-
port=$PORT/$PROTOCOL
            firewall-cmd --permanent --zone=trusted --remove-source=10.8.0.0/24
            firewall-cmd --direct --remove-rule ipv4 nat POSTROUTING 0 -s
10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT --to $IP
            firewall-cmd --permanent --direct --remove-rule ipv4 nat
POSTROUTING 0 -s 10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT --to $IP
          else
            IP=$(grep 'iptables -t nat -A POSTROUTING -s 10.8.0.0/24 ! -d
10.8.0.0/24 -j SNAT --to ' $RCLOCAL | cut -d "" -f 14)
```

```
                iptables -t nat -D POSTROUTING -s 10.8.0.0/24 ! -d 10.8.0.0/24 -j
SNAT --to $IP
                sed -i '/iptables -t nat -A POSTROUTING -s 10.8.0.0\/24 ! -d
10.8.0.0\/24 -j SNAT --to /d' $RCLOCAL
                if iptables -L -n | grep -qE '^ACCEPT'; then
                   iptables -D INPUT -p $PROTOCOL --dport $PORT -j ACCEPT
                   iptables -D FORWARD -s 10.8.0.0/24 -j ACCEPT
                   iptables -D FORWARD -m state --state RELAT-
ED,ESTABLISHED -j ACCEPT
                   sed -i "/iptables -I INPUT -p $PROTOCOL --dport $PORT -j AC-
CEPT/d" $RCLOCAL
                   sed -i "/iptables -I FORWARD -s 10.8.0.0\/24 -j ACCEPT/d"
$RCLOCAL
                   sed -i "/iptables -I FORWARD -m state --state RELAT-
ED,ESTABLISHED -j ACCEPT/d" $RCLOCAL
                fi
             fi
             if hash sestatus 2>/dev/null; then
                if sestatus | grep "Current mode" | grep -qs "enforcing"; then
                   if [[ "$PORT" != '1194' || "$PROTOCOL" = 'tcp' ]]; then
                      semanage port -d -t openvpn_port_t -p $PROTOCOL $PORT
                   fi
                fi
             fi
             if [[ "$OS" = 'debian' ]]; then
                apt-get remove --purge -y openvpn
             else
                yum remove openvpn -y
             fi
             rm -rf /etc/openvpn
             echo ""
             echo "OpenVPN удален!"
          else
             echo ""
             echo "Удаление оборвано!"
          fi
          exit
          ;;
          4) exit;;
       esac
    done
else
    clear
    echo 'OpenVPN автоматическийустановщик'
```

```
    echo ""
    echo "Для начала работы нужно узнать IPv4 address сети которая нужна для
OpenVPN подключения"
    read -p "IP address:" -e -i $IP IP
    echo ""
    echo "По какому протоколу будет вестись подключение"
    echo "   1) UDP (recommended)"
    echo "   2) TCP"
    read -p "Protocol [1-2]: " -e -i 1 PROTOCOL
    case $PROTOCOL in
        1)
        PROTOCOL=udp
        ;;
        2)
        PROTOCOL=tcp
        ;;
    esac
    echo ""
    echo "Назначьтепортдляработы OpenVPN"
    read -p "Port:" -e -i 1194 PORT
    echo ""
    echo "Чьи DNS сервера буду использоваться в вашей VPN сети?"
    echo "   1) Current system resolvers"
    echo "   2) Google"
    echo "   3) OpenDNS"
    echo "   4) NTT"
    echo "   5) Hurricane Electric"
    echo "   6) Verisign"
    read -p "DNS [1-6]: " -e -i 1 DNS
    echo ""
    echo "Название первого ключа для доступа к серверу"
    echo "Только латинские буквы и цыфры"
    read -p "Client name: " -e -i client CLIENT
    echo ""
    read -n1 -r -p "Нажмите любую клавишу для начала установки..."
    if [[ "$OS" = 'debian' ]]; then
        apt-get update
        apt-get install openvpn iptables openssl ca-certificates -y
    fi
    if [[ -d /etc/openvpn/easy-rsa/ ]]; then
        rm -rf /etc/openvpn/easy-rsa/
    fi
    wget -O ~/EasyRSA-3.0.3.tgz "https://github.com/OpenVPN/easy-
rsa/releases/download/v3.0.3/EasyRSA-3.0.3.tgz"
```

```
    tar xzf ~/EasyRSA-3.0.3.tgz -C ~/

    sed -i 's/\[\[/\[/g;s/\]\]/\]/g;s/==/=/g' ~/EasyRSA-3.0.3/easyrsa
    mv ~/EasyRSA-3.0.3/ /etc/openvpn/
    mv /etc/openvpn/EasyRSA-3.0.3/ /etc/openvpn/easy-rsa/
    chown -R root:root /etc/openvpn/easy-rsa/
    rm -rf ~/EasyRSA-3.0.3.tgz
    cd /etc/openvpn/easy-rsa/
    ./easyrsa init-pki
    ./easyrsa --batch build-ca nopass
    ./easyrsa gen-dh
    ./easyrsa build-server-full  server nopass
    ./easyrsa build-client-full  $CLIENT nopass
    EASYRSA_CRL_DAYS=3650 ./easyrsa gen-crl
    cp pki/ca.crt pki/private/ca.key  pki/dh.pem pki/issued/server.crt
pki/private/server.key  pki/crl.pem /etc/openvpn
    chown nobody:$GROUPNAME /etc/openvpn/crl.pem
    openvpn --genkey  --secret /etc/openvpn/ta.key
    echo "port $PORT
proto $PROTOCOL
dev tun
sndbuf 0
rcvbuf 0
ca ca.crt
cert server.crt
key server.key
dh dh.pem
auth SHA512
tls-auth ta.key 0
topology subnet
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt"> /etc/openvpn/server.conf
    echo 'push "redirect-gateway  def1 bypass-dhcp"'>> /etc/openvpn/server.conf
    # DNS
    case $DNS  in
        1)
        grep -v '#' /etc/resolv.conf | grep 'nameserver' | grep -E -o '[0-9]{1,3}\.[0-
9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}'  | while  read line;  do
            echo "push \"dhcp-option DNS $line\""'>>  /etc/openvpn/server.conf
        done
        ;;
        2)
        echo 'push "dhcp-option DNS 8.8.8.8"'>> /etc/openvpn/server.conf
        echo 'push "dhcp-option DNS 8.8.4.4"'>> /etc/openvpn/server.conf
```

```
        ;;
        3)
        echo 'push "dhcp-option DNS 208.67.222.222"'>> /etc/openvpn/server.conf
        echo 'push "dhcp-option DNS 208.67.220.220"'>> /etc/openvpn/server.conf
        ;;
        4)
        echo 'push "dhcp-option DNS 129.250.35.250"'>> /etc/openvpn/server.conf
        echo 'push "dhcp-option DNS 129.250.35.251"'>> /etc/openvpn/server.conf
        ;;
        5)
        echo 'push "dhcp-option DNS 74.82.42.42"'>> /etc/openvpn/server.conf
        ;;
        6)
        echo 'push "dhcp-option DNS 64.6.64.6"'>> /etc/openvpn/server.conf
        echo 'push "dhcp-option DNS 64.6.65.6"'>> /etc/openvpn/server.conf
        ;;
    esac
    echo "keepalive 10 120
cipher AES-256-CBC
comp-lzo
user nobody
group $GROUPNAME
persist-key
persist-tun
status openvpn-status.log
verb 3
crl-verify crl.pem">> /etc/openvpn/server.conf
    sed -i '/\<net.ipv4.ip_forward\>/c\net.ipv4.ip_forward=1' /etc/sysctl.conf
    if ! grep -q "\<net.ipv4.ip_forward\>" /etc/sysctl.conf; then
        echo 'net.ipv4.ip_forward=1'>> /etc/sysctl.conf
    fi
    echo 1 > /proc/sys/net/ipv4/ip_forward
    if pgrep firewalld; then

        firewall-cmd --zone=public --add-port=$PORT/$PROTOCOL
        firewall-cmd --zone=trusted --add-source=10.8.0.0/24
        firewall-cmd --permanent --zone=public --add-port=$PORT/$PROTOCOL
        firewall-cmd --permanent --zone=trusted --add-source=10.8.0.0/24
        firewall-cmd --direct --add-rule ipv4 nat POSTROUTING 0 -s 10.8.0.0/24 ! -
d 10.8.0.0/24 -j SNAT --to $IP
        firewall-cmd --permanent --direct --add-rule ipv4 nat POSTROUTING 0 -s
10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT --to $IP
    else
        if [[ "$OS" = 'debian'&& ! -e $RCLOCAL ]]; then
```

```
        echo '#!/bin/sh -e
exit 0'> $RCLOCAL
    fi
    chmod +x $RCLOCAL
    iptables -t nat -A POSTROUTING -s 10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT --
to $IP
    sed -i "1 a\iptables -t nat -A POSTROUTING -s 10.8.0.0/24 ! -d 10.8.0.0/24 -j
SNAT --to $IP" $RCLOCAL
    if iptables -L -n | grep -qE '^(REJECT|DROP)'; then

        iptables -I INPUT -p $PROTOCOL --dport $PORT -j ACCEPT
        iptables -I FORWARD -s 10.8.0.0/24 -j ACCEPT
        iptables -I FORWARD -m state --state RELATED,ESTABLISHED -j
ACCEPT
        sed -i "1 a\iptables -I INPUT -p $PROTOCOL --dport $PORT -j ACCEPT"
$RCLOCAL
        sed -i "1 a\iptables -I FORWARD -s 10.8.0.0/24 -j ACCEPT" $RCLOCAL
        sed -i "1 a\iptables -I FORWARD -m state --state RELAT-
ED,ESTABLISHED -j ACCEPT" $RCLOCAL
    fi
  fi
  if hash sestatus 2>/dev/null; then
    if sestatus | grep "Current mode" | grep -qs "enforcing"; then
      if [[ "$PORT" != '1194' || "$PROTOCOL" = 'tcp' ]]; then
        semanage port -a -t openvpn_port_t -p $PROTOCOL $PORT
      fi
    fi
  fi
  if [[ "$OS" = 'debian' ]]; then
    if pgrep systemd-journal; then
      systemctl restart openvpn@server.service
    else
      /etc/init.d/openvpn restart
    fi
  else
    if pgrep systemd-journal; then
      systemctl restart openvpn@server.service
      systemctl enable openvpn@server.service
    else
      service openvpn restart
      chkconfig openvpn on
    fi
  fi
  EXTERNALIP=$(ip addr show)
```

```
    if [[ "$IP" != "$EXTERNALIP" ]]; then
        echo ""
        echo"Похоже ваш сервер не поддерживает NAT!"
        echo ""
        echo "Есливашсерверимеетподдержку NATed (e.g. LowEndSpirit), укажи-
теваш IP"
        echo"Если нет просто пропустите этот момент"
        read -p "External IP: " -e USEREXTERNALIP
        if [[ "$USEREXTERNALIP" != "" ]]; then
            IP=$USEREXTERNALIP
        fi
    fi
    echo "client
dev tun
proto $PROTOCOL
sndbuf 0
rcvbuf 0
remote $IP $PORT
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
auth SHA512
cipher AES-256-CBC
comp-lzo
setenv opt block-outside-dns
key-direction 1
verb 3"> /etc/openvpn/client-common.txt
    newclient "$CLIENT"
    echo ""
    echo "Готово!"
    echo ""
    echo "Ваш клиент для подключения доступен" ~/"$CLIENT.ovpn"
    echo "Если вы хотите больше клиентов запустите скрипт снова"
fi
```