

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ
ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение
высшего образования

Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ (№ 12)

Тема: Проектирование «ПРОЕКТИРОВАНИЕ ПОДСИСТЕМЫ
УПРАВЛЕНИЯ ТРЕБОВАНИЯМИ»

Коллективная разработка

ФИО	№ группы	Роли в проекте
Кутузов А.В.	М20-512	Архитектор, системный аналитик
Богословский Д.М	М20-512	Разработчик, Технический писатель
Лашина Д. С.	М20-512	Руководитель, бизнес-аналитик проекта
Ванин М.В.	М20-512	Разработчик, Бизнес-аналитик
Волков Е.А.	М20-512	Разработчик, Тестировщик

Перечень документов: Устав Проекта, Техническое Задание,
Пояснительная Записка, Модель Угроз и Модель Нарушителей

Оценка _____

Ст.преп.каф.12 _____

Красникова С.А.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ
КАФЕДРА КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ (№ 12)

Тема: Проектирование «ПРОЕКТИРОВАНИЕ ПОДСИСТЕМЫ
УПРАВЛЕНИЯ ТРЕБОВАНИЯМИ»

Коллективная разработка

ФИО	№ группы	Роли в проекте
Кутузов А.В.	М20-512	Архитектор, системный аналитик
Богословский Д.М	М20-512	Разработчик, Технический писатель
Лашина Д. С.	М20-512	Руководитель, бизнес-аналитик проекта
Ванин М.В.	М20-512	Разработчик, Бизнес-аналитик
Волков Е.А.	М20-512	Разработчик, Тестировщик

Оценка _____

Ст.преп.каф.12 _____

Красникова С.А.

Москва, 2021

КАФЕДРА КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ (№ 12)

**ПРОЕКТИРОВАНИЕ ПОДСИСТЕМЫ УПРАВЛЕНИЯ
ТРЕБОВАНИЯМИ
УСТАВ ПРОЕКТА**

Листов 18

Версия 1.0

Москва, 2021

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ И ПОРЯДОК АКТУАЛИЗАЦИИ ДОКУМЕНТА	5
1.1. НАЗНАЧЕНИЕ ДОКУМЕНТА	5
1.2. ПОРЯДОК ПОДДЕРЖКИ ДОКУМЕНТА В АКТУАЛЬНОМ СОСТОЯНИИ	5
2. ОБЩИЕ СВЕДЕНИЯ	6
2.1. НАЗВАНИЕ ПРОЕКТА	6
2.2. СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА	6
2.3. ЗАКАЗЧИК, КЛЮЧЕВЫЕ УЧАСТНИКИ И ЗАИНТЕРЕСОВАННЫЕ СТОРОНЫ ПРОЕКТА	6
2.4. ЦЕЛИ ПРОЕКТА	6
3. СОДЕРЖАНИЕ ПРОЕКТА	8
4. СВЯЗАННЫЕ ПРОЕКТЫ (МЕРОПРИЯТИЯ)	8
5. РОЛИ И КОММУНИКАЦИИ В ПРОЕКТЕ	9
5.1. Роли в проекте	9
5.2. ВЗАИМОДЕЙСТВИЕ С ЗАИНТЕРЕСОВАННЫМИ СТОРОНАМИ ПРОЕКТА	11
5.3. ПОДГОТОВКА, СОГЛАСОВАНИЕ И УТВЕРЖДЕНИЕ ДОКУМЕНТОВ ПРОЕКТА	12
5.4. КООРДИНАЦИЯ РАБОТ И КОММУНИКАЦИИ В ПРОЕКТЕ	12
6. РИСКИ ПРОЕКТА	13
7. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	16
ПРИЛОЖЕНИЕ 1. РОЛИ И КОНТАКТНАЯ ИНФОРМАЦИЯ	17
СПИСОК ИЗМЕНЕНИЙ	18

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ЖИЗНЕННЫЙ ЦИКЛ ПРОЕКТА	Последовательность фаз проекта, задаваемая исходя из потребностей управления проектом
ЗАИНТЕРЕСОВАННАЯ СТОРОНА	Организация, индивидуальное лицо или группа лиц, заинтересованная в результатах проекта или оказывающая влияние на результат проекта
КОНТРОЛЬНАЯ ТОЧКА (ВЕХА) ПРОЕКТА	Важное событие проекта, обычно связанное с достижением основных результатов
ОПЕРАЦИЯ	Элемент работ проекта, обычно имеется ожидаемая длительность, потребности в ресурсах, стоимость
ПОЛЬЗОВАТЕЛЬ	Департамент здравоохранения города Москвы (по тексту пишется с заглавной буквы)
ПРОГРАММА	Программа модернизации здравоохранения (по тексту пишется с заглавной буквы)
ПРОЕКТ	Уникальный процесс, состоящий из совокупности скоординированных и управляемых видов деятельности с начальной и конечной датами, предпринятый для достижения цели, соответствующий конкретным требованиям, включающий ограничения по срокам, стоимости и ресурсам
РИСК ПРОЕКТА	Неопределенное событие или условие, которое может положительно или отрицательно повлиять на выполнение и результат проекта. У риска есть источник и, в случае наступления риска, последствия
РОЛЬ В ПРОЕКТЕ	Набор выполняемых функций
УСТАВ ПРОЕКТА	Документ, регламентирующий жизненный цикл проекта
ФАЗА	Объединение логически связанных операций проекта, фаза обычно завершается достижением одного из основных результатов проекта

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

НИОКР	Научно-исследовательские и опытно-конструкторские работы
СУБД	Система управления базами данных
ТЗ	Техническое задание

1. НАЗНАЧЕНИЕ И ПОРЯДОК АКТУАЛИЗАЦИИ ДОКУМЕНТА

1.1. Назначение документа

Устав проекта (далее, Устав) служит основным приоритетным документом для всех участников проекта. Назначение Устава - описать основания и рациональный способ принятия решений по реализации проекта. Устав полностью описывает предмет, цели, границы и способы реализации проекта. Устав обеспечивает целостность проекта, то есть согласованность действий всех участников на всех этапах проекта.

1.2. Порядок поддержки документа в актуальном состоянии

Документ подготовлен и актуализируется Исполнителем, согласовывается Проектным офисом Программы, утверждается Государственным заказчиком. Исполнители по документу представлены в таблице 1 (1 - порядковый номер таблицы в документе).

Таблица 1 – Перечень ответственных исполнителей документа

ФИО	Организация, должность	Телефон	e-mail
Кутузов А.В.	НИЯУ МИФИ студент		artilleriaartem@gmail.com
Богословский Д.М.	НИЯУ МИФИ студент		bogol243@gmail.com
Лашина Д. С.	НИЯУ МИФИ студент		daxalas.96@gmail.com
Ванин М.В.	НИЯУ МИФИ студент		markthefolkin@gmail.com
Волков Е.А.	НИЯУ МИФИ студент		eavolkov96@gmail.com

2. ОБЩИЕ СВЕДЕНИЯ

2.1. Название проекта

Наименование проекта: Подсистема управления требованиями

Краткое наименование проекта: ПУТР

2.2. Сроки выполнения проекта

Начало проекта: 06.09.2021 (6 сентября 2021 года)

Окончание проекта: Не более 4 месяцев со дня начала работ.

2.3. Заказчик, ключевые участники и заинтересованные стороны проекта

Заказчик: Красникова Светлана Анатольевна

Пользователь: Красникова Светлана Анатольевна

Исполнитель: Магистранты группы М20-512

Заинтересованные стороны: Кафедра 12

2.4. Цели проекта

В таблице 2 представлено описание целей проекта ПУТР и критериев оценки достижения целей проекта.

Таблица 2 - Цели создания Системы и критерии оценки достижения целей

Цель	Показатель	Критерии оценки достижения целей
Сокращение времени анализа требований для аналитика	Пользователь имеет возможность задокументировать требование	Требование задокументировано пользователем
Сокращение времени анализа требований для тестировщика	Пользователь имеет доступ к требованиям и может их просматривать	Просмотр требований пользователем

В рамках подсистемы требований разработать функциональность для установки статуса требований пользователем	Пользователь имеет возможность установить статус для конкретного требования	Установка пользователем статуса требования
В рамках подсистемы требований разработать функциональность для изменения требований пользователем	Пользователь имеет возможность изменить требование	Требование изменено пользователем

3. СОДЕРЖАНИЕ ПРОЕКТА

Таблица 3 – Содержание работ проекта

Ид.	Название задачи	Длительность	Начало	Окончание
1	Разработка плана и устава проекта	7	07.09	14.09
2	Моделирование автоматизируемых процессов	7	07.09	14.09
3	Моделирование функций системы	7	14.09	21.09
4	Моделирование предметной области		21.09	28.09
5	Разработка ТЗ	7	28.09	05.10
6	Разработка диаграммы сущность-связь	7	12.10	19.10
7	Разработка макета интерфейса пользователя	7	19.10	26.10
8	Проектирование архитектуры системы	7	26.10	02.11
9	Разработка модели угроз и модели нарушителя ИБ	7	02.11	09.11
10	Разработка ПЗ к ТП	7	09.11	16.11
11	Разработка прототипа системы	42	16.11	14.12
12	Документирование прототипа	14	14.12	21.12

4. СВЯЗАННЫЕ ПРОЕКТЫ (МЕРОПРИЯТИЯ)

В рамках Проекта Подсистема управления требованиями должна взаимодействовать с Подсистемой управления задачами и проектами.

5. РОЛИ И КОММУНИКАЦИИ В ПРОЕКТЕ

5.1. Роли в проекте

В таблице 4 представлено детальное описание ролей проекта.

Таблица 4 – Роли в проекте

№	Роль	Основные функции / Зоны ответственности
1	Руководитель Проекта со стороны Заказчика	<ol style="list-style-type: none">1) согласование Устава проекта;2) взаимодействие по организационным вопросам с ответственными за другие мероприятия Программы и внешние по отношению к Программе мероприятия/ системы, связанные с реализацией проекта;3) мониторинг хода работ по контрольным точкам плана Проекта на основе регулярных отчётов Исполнителя;4) организация приемки работ Исполнителя;5) устранение возможных организационных проблем при проведении работ по проекту со стороны заказчика и Пользователя;6) эскалация рисков и проблем на уровень Куратора проекта со стороны Заказчика
2	Руководитель Проекта со стороны Исполнителя	<ol style="list-style-type: none">1) разработка Устава и плана проекта, согласование с Заказчиком и контроль их выполнения проектной командой;2) обеспечение своевременного решения возникающих проблем или своевременной их передачи на необходимый уровень управления проектом для рассмотрения и принятия решения;3) оперативное планирование загрузки членов проектной команды;4) ведение журнала регистрации проблем;5) ведение журнала регистрации рисков;6) выполнение задач в соответствии с планом-графиком проекта;

		7) формирование отчётности о ходе реализации проекта;
3	Архитектор проекта	1) Разбиение на технические подсистемы/слои/компоненты/модули; 2) Разработка ключевых технических сценариев взаимодействия компонентов; 3) Определение протоколов взаимодействия компонентов (проектирование технических интерфейсов); 4) Определение форматов хранения и передачи данных; 5) Архитектурный надзор разработки 6) Текущее консультирование команды 7) Написание технического проекта.
4	Бизнес-аналитик проекта	1) Выявление потребностей Заказчика по средствам коммуникации; 2) Формулирование концепции решения; 3) Оформление концепции в техническое задание с конкретными требованиями к Проекту; 4) Консультация Рабочей команды во время разработки продукта;
5	Системный аналитик проекта	1) Формализация и спецификация требований; 2) Написание технического задания на уровне функциональных требований и программной реализации; 3) Анализ рисков и причин возникновения ошибок при разработке систем;
6	Разработчик проекта	1) Написание кода для решений проектных задач в соответствии с поставленным техническим заданием; 2) Поддержка текущих решений; 3) Помощь техническим писателям в документировании реализованной функции
7	Тест-аналитик проекта	1) Составление плана тестирования проектных

		решений; 2) Автоматизация испытаний; 3) Выбор инструментов, метрик и стандартов для тестирования;
8	Тестировщик проекта	1) Тестирование программы установки, всех функций и пользовательского интерфейса согласно плану тестирования; 2) Проведение автоматизации тестирований; 3) Регистрация результатов автоматизированных испытаний и анализ обнаруженных неполадок;
9	Технический писатель проекта	1) Оформление документов в соответствии со стандартом ГОСТ, их структурирование в единый том, а также подготовка необходимых графиков и схем; 2) Поддержка документов в актуальном состоянии; 3) Обучение работе с проектом и техническая поддержка его пользователей;

Поименный список участников проекта с их контактными данными представлен в Приложение 1. Приложение 1 может дополняться в ходе выполнения проекта.

5.2. Взаимодействие с заинтересованными сторонами проекта

В таблице 5 представлены описание взаимодействия с заинтересованными участниками проекта.

Таблица 5 – Взаимодействие с заинтересованными участниками проекта

№	Участник	Описание взаимодействия	Ответственный (на уровне ролей проекта)
1	Красникова Светлана Анатовна	Сдача проекта	Менеджер по внедрению со стороны Исполнителя
2	Подсистема управления задачами	Интеграция подсистем	Менеджер по внедрению со стороны Исполнителя

5.3. Подготовка, согласование и утверждение документов проекта

В таблице 6 представлены описание ответственностей участников проекта в части подготовки, согласования и утверждения документов проекта.

Обозначения: П - подготовка, С - согласование, У – утверждение, РП – руководитель проекта, СА – системный аналитик, ТП – технический писатель, Т – тестировщик, БА – бизнес-аналитик, А – архитектор, ТА – тестировщик-аналитик, ПР - программист, АП- администратор проекта

Таблица 6 – Матрица согласования документов

№ п/п	Документ	Заказчик	Исполнитель								
		РП	РП	АП	СА	ТП	Т	ТА	БА	А	ПР
1.	Устав проекта	У, С		П							
2.	План-график проекта	У, С	П								
3.	Регулярная отчётность по проекту для Заказчика		П								
4.	Документы, разрабатываемые в ходе выполнения проекта:										
5.	ТЗ	У, С	С	П	П	П			П	С	
6.	ПЗ к ТП	У, С	С	С	П	П			С	П	П
7.	ПМИ	У, С	С	С	С	П	П	П		С	С
8.	РП	У, С	С	С	С	П			С	С	
9.	РА	У, С	С	С	С	П				С	
10.	Общее описание системы	У, С	С	С	П	П				С	С

5.4. Координация работ и коммуникации в проекте

Координационный совет

Для управления проектом создается Координационный совет, в состав которого входят:

- Руководитель проекта со стороны Исполнителя;
- Бизнес – аналитик;
- Системный аналитик;
- Архитектор;
- Технический писатель;
- Программист;
- Тест-аналитик;
- Тестировщик;

Функции координационного совета являются:

- Утверждение технических решений;

- Выработка поручений участникам рабочей группы;
- Принятие решений по привлечению ресурсов;
- Принятие решений по изменениям состава рабочей группы;
- Выработка предложений по привлечению субподрядчиков;
- Выработка предложений по изменению сроков проекта;

Координационный совет собирается не реже 1 раза в 3 недели, плановое заседание проводится по понедельникам с 18:00 до 19:00 мск по месту расположения Проектного офиса Программы. Руководитель проекта со стороны Государственного заказчика и Руководитель проекта со стороны Исполнителя могут по собственной инициативе организовать внеплановое заседание Координационного совета, предупредив участников не менее чем за 1 сутки.

Проектная группа

Заседания ПГ проводятся на регулярной основе не реже, чем 1 (Один) раз в неделю. Приглашение на заседание ПГ направляется председателем ПГ не менее, чем за 2 (Два) рабочих дня до даты заседания. Приглашение направляется посредством электронной почты на электронные адреса, указанные в «Приложении № 2» к Уставу. При необходимости на ПГ могут быть приглашены члены Рабочей группы Проекта. Повестка заседания ПГ оговаривается в тексте приглашения. Не менее чем за 1 (Один) рабочий день всем членам ПГ направляется отчет о ходе выполнения (статусе) Проекта.

Рабочая группа

Рабочая группа (РГ) создана для объединения участников Проекта, принимающих непосредственное участие в выполнении Проекта. РГ не является группой управления Проектом. Эксперты из РГ привлекаются в группы управления Проектом только при необходимости. Состав участников РГ указан в разделе «Приложение № 2» к Уставу.

Порядок разрешения открытых вопросов

Любой сотрудник рабочей группы, имеющий вопрос, не получивший разрешения в рабочем порядке, формулирует свой вопрос в ходе заседания. Суть вопроса, принятое решение, ответственное лицо и срок исполнения регистрируются в протоколе заседания. Члены рабочей группы могут требовать предоставления письменного ответа на вопрос с визой ответственного лица, что также должно быть зафиксировано в протоколе. Список открытых вопросов прилагается к протоколу совещания членов рабочей группы. Открытые вопросы могут быть закрыты по согласованию с сотрудником, поставившим вопрос. Факт согласования закрытия вопроса отражается в протоколе заседания рабочей группы, вопросы, на которые даны ответы, удаляются из списка открытых вопросов. Все открытые вопросы выносятся на рассмотрение Проектной группы.

6. РИСКИ ПРОЕКТА

Риски проекта представлены в таблице 7.

Таблица 7 – Риски проекта

№	Наименование риска	Ответственный за мониторинг и реагирование на возникновение риска	На что влияет возникновение риска	Предложения по предотвращению/реагированию на возникновение риска
Технологические				
1.	Платный сервер	Архитектор	Невозможность	Координация с

	или технология с помощью которой разрабатываем приложение	проекта со стороны Исполнителя	внедрения и эксплуатации	участниками и заинтересованными сторонами проекта
2	Не сможет произойти интеграция с проектом управления задачами из-за выбранных технологий	Архитектор проекта со стороны Исполнителя	Невозможность внедрения и эксплуатации	Координация с участниками и заинтересованными сторонами проекта
3	База данных, которая используется в программной системе, не обеспечивает обработку ожидаемого объема транзакций	Архитектор проекта со стороны Исполнителя	Неустойчивое состояние системы и чрезмерно долгое время отклика	Координация с участниками и заинтересованными сторонами проекта, обоснованный выбор СУБД
4	Программные компоненты, которые используются в системе, имеют дефекты, ограничивающие их функциональные возможности	Архитектор проекта со стороны Исполнителя	Непредсказуемое поведение системы, отказоустойчивость не гарантирована	Контроль разработки, проектирование тест-кейсов и периодическое проведение регрессионного тестирования
Организационные				
1	Участники проекта серьезно болеют	Руководитель проекта со стороны Государственного заказчика Руководитель проекта со стороны Исполнителя	Срыв сроков проекта Снижение качества проекта	Самоизоляция и удаленная работа
2	Несвоевременное развертывание рабочей АС	Руководитель проекта со стороны	Срыв сроков проекта Нарушение работы	Координация с участниками и заинтересованными сторонами проекта,

		Исполнителя	смежных АС	определение и контроль промежуточных вех и результатов
3	В проектной команде, выполняющей разработку ПО, произошла реорганизация	Руководитель проекта со стороны Исполнителя	Изменились приоритеты по управлению проектом	Своевременное выявление проблемы и перераспределение должностных обязанностей

7. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ 34.003-90. АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.
2. РД 50-34.698-90 АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ ТРЕБОВАНИЯ К СОДЕРЖАНИЮ ДОКУМЕНТОВ.
3. Руководство к Своду знаний по управлению проектами. PMBOK Guide. Редакция 2000г

ПРИЛОЖЕНИЕ 1. РОЛИ И КОНТАКТНАЯ ИНФОРМАЦИЯ

1.

№	Проектная роль	ФИО	Организация	Контактные данные	
				телефон	email
1.	Архитектор, системный аналитик	Кутузов А.В.	НИЯУ МИФИ		artilleriaartem@gmail.com
2.	Разработчик, Технический писатель	Богословский Д.М.	НИЯУ МИФИ		bogol243@gmail.com
3.	Руководитель, бизнес-аналитик проекта	Лашина Д. С.	НИЯУ МИФИ		daxalas.96@gmail.com
4.	Разработчик, Бизнес-аналитик	Ванин М.В.	НИЯУ МИФИ		markthefolkin@gmail.com
5.	Разработчик, Тестировщик	Волков Е.А.	НИЯУ МИФИ		eavolkov96@gmail.com

СПИСОК ИЗМЕНЕНИЙ

Дата	Версия	Описание изменений	Автор

ОРГАНИЗАЦИЯ

УТВЕРЖДАЮ

Должность

(личная подпись) (расшифровка подписи) X.X. XXXX
«__» _____ 20__ г

УТВЕРЖДАЮ

Должность

(личная подпись) (расшифровка подписи) X.X. XXXX
«__» _____ 20__ г

ПОДСИСТЕМА УПРАВЛЕНИЯ ТРЕБОВАНИЯМИ

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Версия 1.0

СОГЛАСОВАНО

Должность

(личная подпись) (расшифровка подписи) X.X. XXXX
«__» _____ 20__ г

Представители организации

Разработчика

Должность

(личная подпись) (расшифровка подписи) X.X. XXXX
«__» _____ 20__ г

ОРГАНИЗАЦИЯ

ПОДСИСТЕМА УПРАВЛЕНИЯ ТРЕБОВАНИЯМИ
ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Листов 22

Версия 1.0

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ.....	4
1.1. Полное наименование системы и ее условное обозначение.....	4
1.2. Плановые сроки начала и окончания работы по созданию системы	4
1.3. Заказчик, ключевые участники и заинтересованные стороны	4
2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ	5
2.1. Назначение системы.....	5
2.2. Цели создания системы.....	5
3. ХАРАКТЕРИСТИКА ОБЪЕКТОВ АВТОМАТИЗАЦИИ	6
4. ТРЕБОВАНИЯ К СИСТЕМЕ.....	6
4.1. Требования к системе в целом	6
4.1.1. Требования к структуре и функционированию системы.....	6
4.1.2. Требования к численности и квалификации персонала системы и режиму его работы.....	7
4.1.3. Показатели назначения.....	8
4.1.4. Требования к надежности.....	8
4.1.5. Требования безопасности.....	9
4.1.6. Требования к эргономике и технической эстетике.....	9
4.1.7. Требования к транспортабельности системы.....	9
4.1.8. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы	9
4.1.9. Требования к защите информации от несанкционированного доступа	9
4.1.10. Требования по сохранности информации	9
4.1.11. Требования по стандартизации и унификации	10
4.2. Требования к функциям, выполняемым системой.....	10
4.2.1. Варианты использования системы	10
4.2.2. Функции системы.....	10
4.3. Требования к видам обеспечения	12

4.3.1. Требования к информационному обеспечению системы	12
4.3.2. Требования к лингвистическому обеспечению Системы	12
4.3.3. Требования к программному обеспечению системы	12
4.3.4. Требования к техническому обеспечению системы	12
5. ТРЕБОВАНИЯ СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО СОЗДАНИЮ (РАЗВИТИЮ) СИСТЕМЫ	13
6. ПРОГРАММА И МЕТОДИКА ИСПЫТАНИЙ	14
7. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ	14
8. ИСТОЧНИКИ РАЗРАБОТКИ	15
ПРИЛОЖЕНИЕ 1 (ACTIVITY DIAGRAM. ПРОЦЕСС РАБОТЫ С ТРЕБОВАНИЯМИ)	17
ПРИЛОЖЕНИЕ 2 (ACTIVITY DIAGRAM. СОЗДАНИЕ БИЗНЕС- ТРЕБОВАНИЙ)	18
ПРИЛОЖЕНИЕ 3 (ACTIVITY DIAGRAM. РАБОТЫ ПО РЕЛИЗУ)	19
ПРИЛОЖЕНИЕ 4 (USE-CASE DIAGRAM)	20
ПРИЛОЖЕНИЕ 5 (СХЕМА БАЗЫ ДАННЫХ)	21
ПРИЛОЖЕНИЕ 6 (ДИАГРАММА КЛАССОВ)	22

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование системы и ее условное обозначение

Полное наименование Системы: Подсистема Управления Требованиями

Условное обозначение Системы: ПУТР

Далее по тексту также используется сокращенное условное обозначение и «Система».

1.2. Плановые сроки начала и окончания работы по созданию системы

Плановые сроки начала работ по созданию Системы: 14 сентября 2021 года

Плановые сроки окончания работ по созданию Системы: до 31 декабря 2021 года

1.3. Заказчик, ключевые участники и заинтересованные стороны

Заказчик: Красникова С.А.

Пользователь: Бизнес-аналитики, руководители, архитекторы, системные аналитики.

Исполнитель: Группа М20-512.

Заинтересованные стороны: Смежные подсистемы, приведенные в таблице 1.

Таблица 1 – Связанные проекты (мероприятия).

п/п	Связанный проект (мероприятие)			Контрольная точка	
	Наименование	Характер влияния	Сроки выполнения работ	Наименование	Дата
	Подсистема управления проектами и задачами	Система-приемник, система-поставщик	27.12.2021	Развертывание и проведение демонстрации на тестовом стенде	27.12.2021

2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1. Назначение системы

Система предназначена для ведения требований в рамках проекта, разбивки по релизам, формирования спецификаций, передачи разработанных спецификаций в системы управления проектами и тестированием.

2.2. Цели создания системы

Цели создания системы приведены в таблице 2.

Таблица 2. Цели создания системы.

Цель	Показатель	Критерии оценки достижения целей
Сокращение времени анализа требований для аналитика	Пользователь может задокументировать требование	Требование задокументировано пользователем
Сокращение времени анализа требований для тестировщика	Пользователь имеет доступ к требованиям и может их просматривать	Просмотр требований пользователем
В рамках подсистемы требований разработать функциональность для установки статуса требований пользователем	Пользователь имеет возможность установить статус для конкретного требования	Установка пользователем статуса требования
В рамках подсистемы требований разработать функциональность для изменения требований пользователем	Пользователь имеет возможность изменить требование	Требование изменено пользователем

3. ХАРАКТЕРИСТИКА ОБЪЕКТОВ АВТОМАТИЗАЦИИ

Объектом автоматизации является процесс работы с требованиями в рамках проектов по разработке программного обеспечения. В процессе задействованы следующие пользователи по ролям: Бизнес Аналитик, Системный Аналитик, Архитектор, Главный Тестировщик, Руководитель, Разработчик. Система предполагает частый обмен данными между пользователями с целью расширения списка требований, согласования новых требований и получения требований для выполнения и проверки, что создаёт предпосылки к разработке и внедрению для этих целей автоматизированной системы управления требованиями.

Текущий процесс работы с требованиями на предприятии предполагает работу 20-30 сотрудников. Объем выполняемых новых проектов в год: 5. Дополнительно, в среднем 5-10 проектов находятся в статусе поддерживаемых. Количество требований в проекте может составлять величину порядка 10 тысяч. На каждый проект в стадии активной разработки приходится по 4 квартальных релиза. Количество требований в составе релиза в среднем составляет величину порядка 1000.

Автоматизации подлежат процессы создания и управления требованиями, как атомарными, так и в составе проектов и релизов. Описание приведено в Приложении 1 (Activity Diagram. Процесс работы с требованиями), Приложении 2 (Activity Diagram. Создание бизнес-требований), Приложении 3 (Activity Diagram. Работы по релизу), Приложении 4 (Use-case Diagram).

4. ТРЕБОВАНИЯ К СИСТЕМЕ

4.1. Требования к системе в целом

4.1.1. Требования к структуре и функционированию системы

Требования к функционированию

Система должна быть доступна в любое время. Время проведения профилактических работ оговаривается заранее, и не должно превышать 24 часа.

Требования к структуре

Система реализуется как web-приложение, имеющее трехзвенную архитектуру. Доступ клиента к приложению осуществляется через тонкий клиент.

Система должна обеспечивать возможность взаимодействия со смежными подсистемами для обмена с ними информацией, файлами и документами по сети.

Система состоит из нескольких подсистем: подсистема работы с требованиями, подсистема спецификаций, подсистема интеграции.

4.1.1.1. Перечень подсистем и основные их назначение

Состав подсистем, их назначение и основные характеристики представлены в таблице 3.

Таблица 3 - Назначение подсистем и их основные характеристики

№	Название подсистемы	Назначение подсистемы
1	Подсистема работы с требованиями	Создание и редактирование атомарных требований
2	Подсистема работы со спецификацией	Создание и редактирование спецификаций
3	Подсистема интеграции	Интеграция с системой управления проектами

4.1.2. Требования к численности и квалификации персонала системы и режиму его работы

В таблице 4 описаны требования к пользователям и администраторам системы.

Таблица 4 – Требования к численности и квалификации персонала системы.

№	Должность	Требования	Численность
1	Системный администратор	Системный администратор должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию программных и технических средств, применяемых в системе.	2
2	Администратор баз данных	Администратор баз данных должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию используемых в АС СУБД.	2
3	Пользователь (Аналитик)	Пользователь системы управления требованиями должен обладать навыками системного и интеграционного анализа для того, чтобы корректно выполнять работу по заполнению спецификации требований и учёта всех необходимых зависимостей.	5
4	Пользователь (Тестировщик)	Требования к квалификации в соответствии с занимаемой должностью. Дополнительная квалификация для работы с системой не требуется.	10
5	Пользователь (Разработчик)	Требования к квалификации в соответствии с занимаемой должностью. Дополнительная квалификация для работы с системой не требуется.	20
6	Пользователь (Руководитель проекта)	Требования к квалификации в соответствии с занимаемой должностью. Дополнительная квалификация для работы с системой не требуется.	5

Режим функционирования персонала:

- Системные администраторы: 5/2, 09:00 – 18:00. Однако, для обеспечения круглосуточной поддержки посменно следуют графику дежурств, а именно могут подключиться в нерабочее время для решения возникших проблем во время эксплуатации системы.
- Администраторы баз данных: 5/2, 09:00 – 18:00.
- Пользователи: 5/2, 09:00 – 18:00. Возможны индивидуальные изменения в рабочем графике со стороны работника или руководства.

Возможны внеплановые выходы в нерабочее время.

4.1.3. Показатели назначения

При изменении текущих рабочих процессов и методов управления Система может незначительно модернизироваться и оптимизироваться, однако основная концепция останется неизменной, так как процесс управления требованиями так таковой не может измениться существенно.

При увеличении количества обрабатываемых данных или пользовательской нагрузки возможна деградация производительности системы.

Предположительный рост системы за временной период 2021-2026гг – возможен несущественный прирост (не более 5%) пользователей-клиентов системы, а также рост объема данных, накапливающихся по мере использования системы.

В течение рабочего времени нагрузка на систему распределена равномерно. Нагрузка на систему складывается из запросов на просмотр требований (как атомарных, так и в составе спецификаций), запросов на добавление и редактирование требований, поисковых запросов. Количество поддерживаемых атомарных требований – величина порядка сотни тысяч. Максимальное количество одновременно работающих в системе пользователей – 50. Среднее количество требований на релиз – 1000. Среднее количество требований на проект – 10000. Хранимый объем данных по большей части складывается из информации об атомарных требованиях. Для поддержки ста проектов величина хранимой информации будет приблизительно равна 1 Гигабайту.

4.1.4. Требования к надежности

Система должна стабильно работать в условиях, описанных в пункте 4.1.3 данного технического задания.

Допустимое количество отказов системы: не более 1 раза в месяц, при этом время восстановления системы не должно превышать 8 часов.

4.1.5. Требования безопасности

Все сотрудники, пользующиеся вычислительной техникой при работе с системой и ее обслуживании должны соблюдать стандартные требования к технике безопасности при работе с компьютерной техникой.

4.1.6. Требования к эргономике и технической эстетике

Система должна иметь практичный, интуитивно понятный интерфейс с хорошей контрастностью шрифтов и без ярких, отвлекающих элементов дизайна.

4.1.7. Требования к транспортабельности системы

Не предъявляются.

4.1.8. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы

Система должна эксплуатироваться на оборудовании, предназначенном для непрерывной работы 24/7 за исключением периодов технического обслуживания. Техническое обслуживание должно проводиться в нерабочее время, не длиться дольше суток и заранее обговариваться.

В процедуры планового технического обслуживания входят:

- Обновление аппаратных и программных компонентов системы.
- Проведение профилактической диагностики работоспособности системы.

4.1.9. Требования к защите информации от несанкционированного доступа

Система должна хранить все данные в защищённом от несанкционированного доступа виде, а также ограничивать доступ к изменению данных пользователями, не имеющими к этому права. Права пользователей предоставляются согласно должности, полученной из подсистемы аутентификации.

Кроме того, на этапе технического проектирования должна быть разработана модель угроз и нарушителя информационной безопасности.

4.1.10. Требования по сохранности информации

Данные и информация должны храниться в БД, а также сохраняться в документах для архивации и восстановления. Резервное копирование информации в базе данных должно осуществляться не реже 1 раза в день.

4.1.11. Требования по стандартизации и унификации

Система должна быть разработана согласно общепринятым стандартам разработки для облегчения дальнейшей доработки и обслуживания всех компонентов системы, а также для взаимодействия со смежными системами, а именно:

- Моделирование поведения системы производится с помощью UML.
- Документация системы соответствует ГОСТ 34.
- Программное обеспечение разрабатывается с использованием паттернов проектирования.

4.2. Требования к функциям, выполняемым системой

4.2.1. Варианты использования системы

Варианты использования системы приведены в Приложении 4 (Use-Case Diagram).

4.2.2. Функции системы

В таблицах 5, 6, 7 представлены функции системы.

Таблица 5 – функции подсистемы работы с требованиями

№	Функция	Описание
1	Внесение атомарных требований	<p>Аналитик в системе может создать требование. Для этого ему необходимо заполнить следующие поля:</p> <ul style="list-style-type: none">• Имя требования;• Описание требования;• Статус требования (по умолчанию создается со статусом «Новое»);• Исполнитель требования (может быть указан позже);• Спецификация, в которую данное требование входит (может быть указана позже);• Тип требования;• Связанное требование (при необходимости);• Тип связи (при необходимости); <p>У требования могут быть следующие статусы:</p> <ul style="list-style-type: none">• Новое;• Отвергнуто;• Согласовано;

№	Функция	Описание
		<ul style="list-style-type: none"> Отменено; Реализовано; Нереализовано. <p>Требование может иметь следующие типы:</p> <ul style="list-style-type: none"> Функциональное; Нефункциональное. <p>У требования могут быть следующие типы связи:</p> <ul style="list-style-type: none"> Иерархия; Зависимость.
2	Модификация требований	При модификации требования в системе может быть изменён его статус, имя, описание, тип, исполнитель,
3	Просмотр списка требований	Возможность просматривать наборы требований, сгруппированных по различным правилам (Принадлежность к конкретной спецификации/релизу, дата, исполнитель, тип, статус)
4	Поиск требований	Возможность получить запрошенное требование по части его имени или описания.
5	Установка отметки о выполнении требования	Требование, выполнение которого подтверждено командой тестирования может быть отмечено в системе как выполненное

Таблица 6 – функции подсистемы работы со спецификациями

№	Функция	Описание
1	Создание спецификации	<p>Аналитик в системе может создать спецификацию. Для этого ему необходимо заполнить следующие поля:</p> <ul style="list-style-type: none"> Версия спецификации (автоматически подтягивается из Релиза); Список требований; Статус спецификации (по умолчанию создается со статусом «Не согласована»); Создатель спецификации (добавляется автоматически). <p>У спецификации могут быть следующие статусы:</p> <ul style="list-style-type: none"> Не согласована; <p>Согласована.</p>
2	Редактирование спецификации	<p>Аналитик может редактировать спецификацию до её согласования. Редактирование включает добавление требований в спецификацию, удаление требований из спецификации. Изменение описания и имени спецификации</p>
3	Согласование спецификации	Статус спецификации может быть изменён на «Согласована» при условии проверки её Архитектором и Главным Тестировщиком.

№	Функция	Описание
4	Согласование Руководителем	При утверждении спецификации руководителем из неё автоматически создаётся Релиз, в который копируются все требования из спецификации

Таблица 7 – функции подсистемы интеграции

№	Функция	Описание
1	Получение данных о проектах из внешней системы	Загрузка в систему данных о проектах из внешней системы.
2	Синхронизация данных о проектах с внешней системой	Информация о проекте в системе может быть обновлена с учётом новых данных во внешней системе.
3	Выгрузка данных о проектах во внешнюю систему	Внешняя система может запросить данные о проекте (спецификации, релизы, списки требований)

4.3. Требования к видам обеспечения

4.3.1. Требования к информационному обеспечению системы

Для корректной работы со смежными подсистемами, описанными в таблице 9, Система предусматривает модули интеграции. Для обмена информацией со смежными подсистемами используется протокол HTTPS, а также формат данных – JSON.

В качестве средства обработки и хранения данных Система использует реляционную СУБД MySQL.

4.3.2. Требования к лингвистическому обеспечению Системы

Для разработки подсистемы управления требованиями используется язык Python. В качестве языка ввода-вывода данных и манипулирования данными используется SQL. Интерфейс пользователя реализован на русском языке.

4.3.3. Требования к программному обеспечению системы

Требования к ПО клиента: для корректной работы приложения на стороне клиента необходим один из поддерживаемых веб-браузеров: Google Chrome или Mozilla Firefox.

Требования к ПО сервера приложений: Python 3.8.

Требования к ПО сервера БД: MySQL.

4.3.4. Требования к техническому обеспечению системы

Требования к аппаратному обеспечению клиента:

- ОС: любая ОС, имеющая графический интерфейс и поддерживающая работу клиентского ПО, приведенного в 4.3.3.

- Процессор: Intel Core i3, а также более современные
- Оперативная память: 4 GB ОЗУ
- Сеть: Широкополосное подключение к интернету
- Место на диске: 5 GB

Требования к аппаратному обеспечению сервера приложений:

- Операционная система: 64-разрядная; семейства UNIX – Centos 7, Debian
- Процессор: Intel Core i5-4430 / AMD FX-6300, а также более современные
- Оперативная память: не менее 8 GB ОЗУ
- Сеть: Широкополосное подключение к интернету: не менее 100 МБит
- Место на диске: 500 GB

5. ТРЕБОВАНИЯ СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО СОЗДАНИЮ (РАЗВИТИЮ) СИСТЕМЫ

Содержание работ по созданию проекта представлено в таблице 8.

Таблица 8 – Содержание работ проекта

Ид.	Название задачи	Длительность	Начало	Окончание
1	Разработка плана и устава проекта	7	07.09	14.09
2	Моделирование автоматизируемых процессов	7	07.09	14.09
3	Моделирование функций системы	7	14.09	21.09
4	Моделирование предметной области	7	21.09	28.09
5	Разработка ТЗ	7	28.09	05.10

6	Разработка диаграммы сущность-связь	7	12.10	19.10
7	Разработка макета интерфейса пользователя	7	19.10	26.10
8	Проектирование архитектуры системы	7	26.10	02.11
9	Разработка модели угроз и модели нарушителя ИБ	7	02.11	09.11
10	Разработка ПЗ к ТП	7	09.11	16.11
11	Разработка прототипа системы	42	16.11	14.12
12	Документирование прототипа	14	14.12	21.12

6. ПРОГРАММА И МЕТОДИКА ИСПЫТАНИЙ

Для контроля и приёмки подсистемы предусмотрено демонстрационное испытание, отображающее корректную работу всех функций.

Испытания должны проводиться в соответствии с разработанным документом «методики испытаний» по ГОСТ 34.603.

7. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Перечень документов, которые должны быть подготовлены к приёмке системы:

- Устав проекта
- Техническое Задание
- Пояснительная Записка к техническому проекту
- Руководство Пользователя
- Руководство Администратора
- Программа и методика испытаний
- Общее описание системы

8. ИСТОЧНИКИ РАЗРАБОТКИ

Настоящее ТЗ разработано на основании следующих стандартов и нормативных документов:

1. ГОСТ 34.201-89 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Виды, комплектность и обозначение документов при создании автоматизированных систем.
2. ГОСТ 34.601-90 ЕСС АСУ. Автоматизированные системы. Стадии создания.
3. ГОСТ 34.602-89 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
4. РД 50-34.698-90 МЕТОДИЧЕСКИЕ УКАЗАНИЯ. ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. Автоматизированные системы. Требования к содержанию документов.
5. ПР 50.2.009-94 ГСИ. Порядок проведения испытаний и утверждения типа средств измерений.

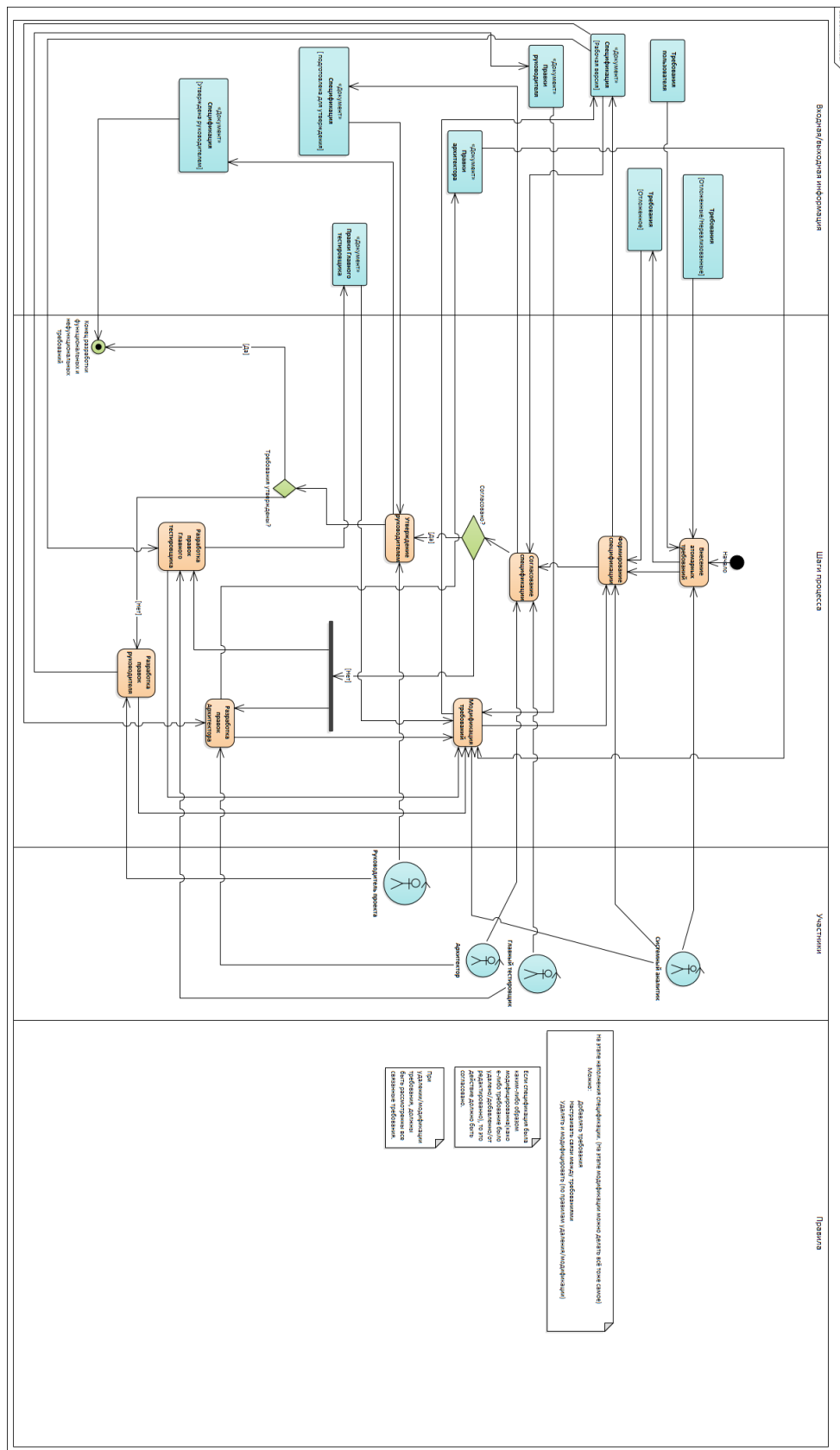
СОСТАВИЛИ

Наименование организации, предприятия	Должность исполнителя	Фамилия, имя, отчество	Подпись	Дата
МИФИ	Архитектор, системный аналитик	Кутузов А.В.		20.11.2021
МИФИ	Разработчик, Технический писатель	Богословский Д.М.		20.11.2021
МИФИ	Руководитель, бизнес-аналитик проекта	Лашина Д. С.		20.11.2021
МИФИ	Разработчик, Бизнес-аналитик	Ванин М.В.		20.11.2021
МИФИ	Разработчик, Тестировщик	Волков Е.А.		20.11.2021

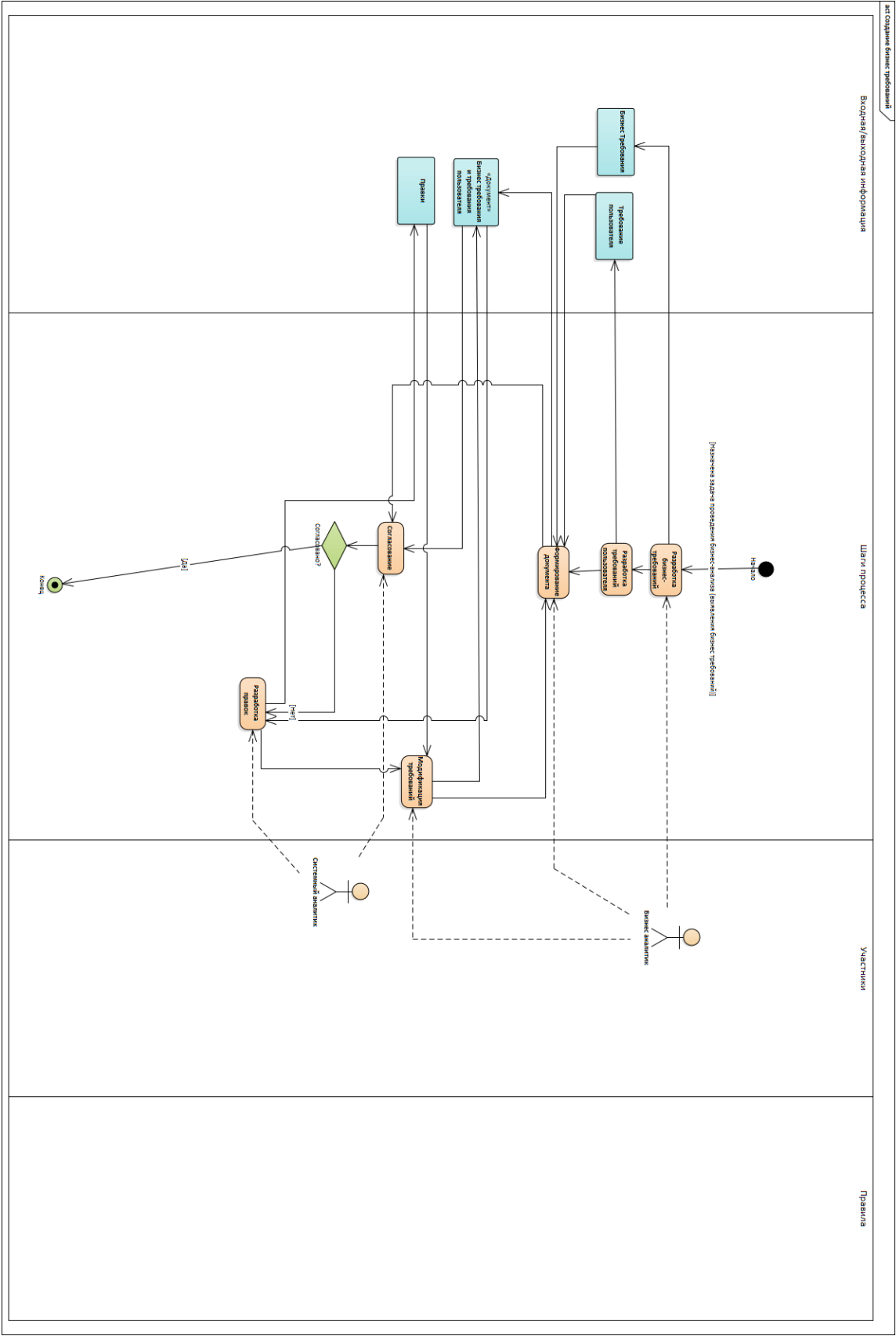
СОГЛАСОВАНО

Наименование организации, предприятия	Должность исполнителя	Фамилия, имя, отчество	Подпись	Дата

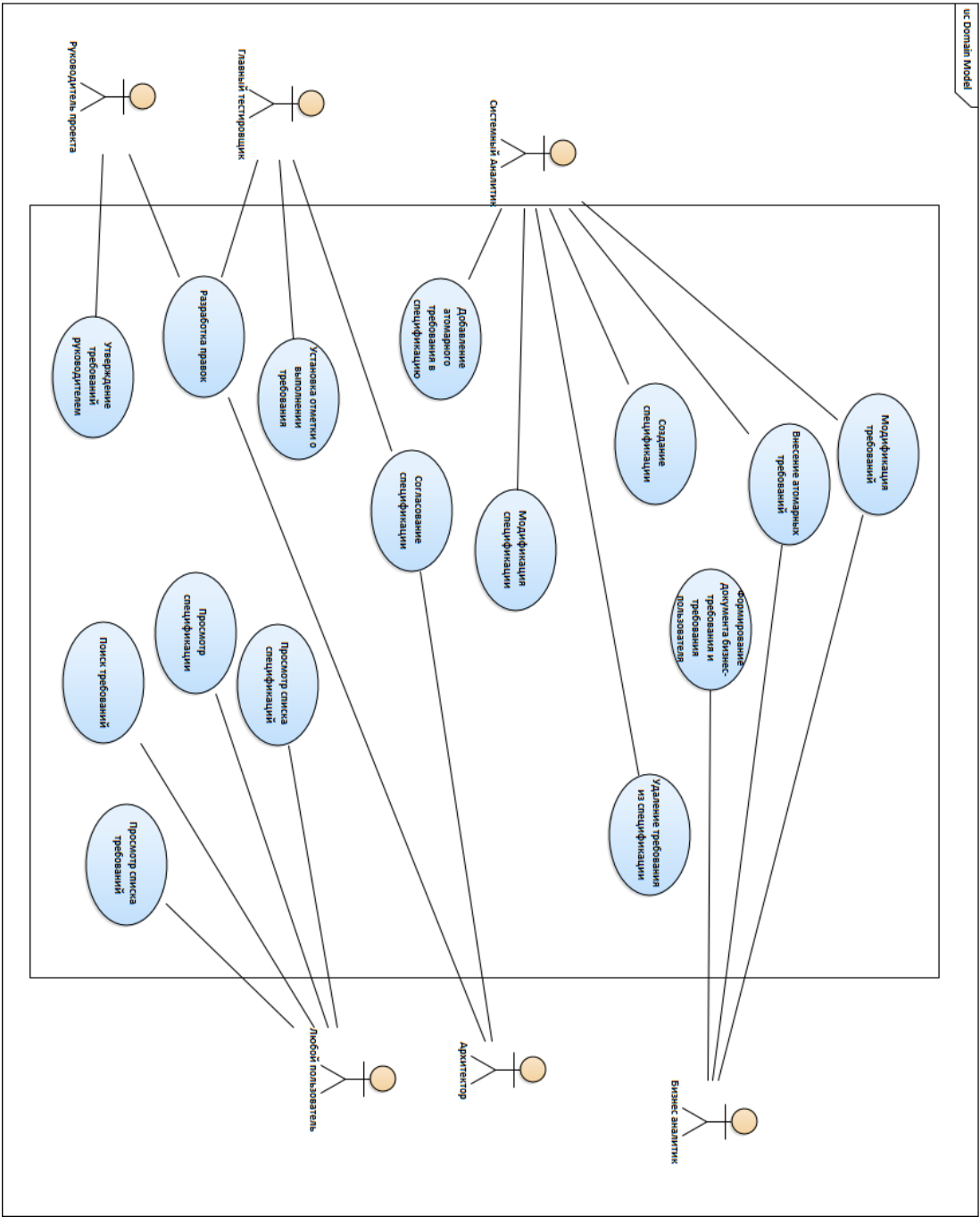
ПРИЛОЖЕНИЕ 1 (ACTIVITY DIAGRAM. ПРОЦЕСС РАБОТЫ С ТРЕБОВАНИЯМИ)



ПРИЛОЖЕНИЕ 2 (ACTIVITY DIAGRAM. СОЗДАНИЕ БИЗНЕС-ТРЕБОВАНИЙ)



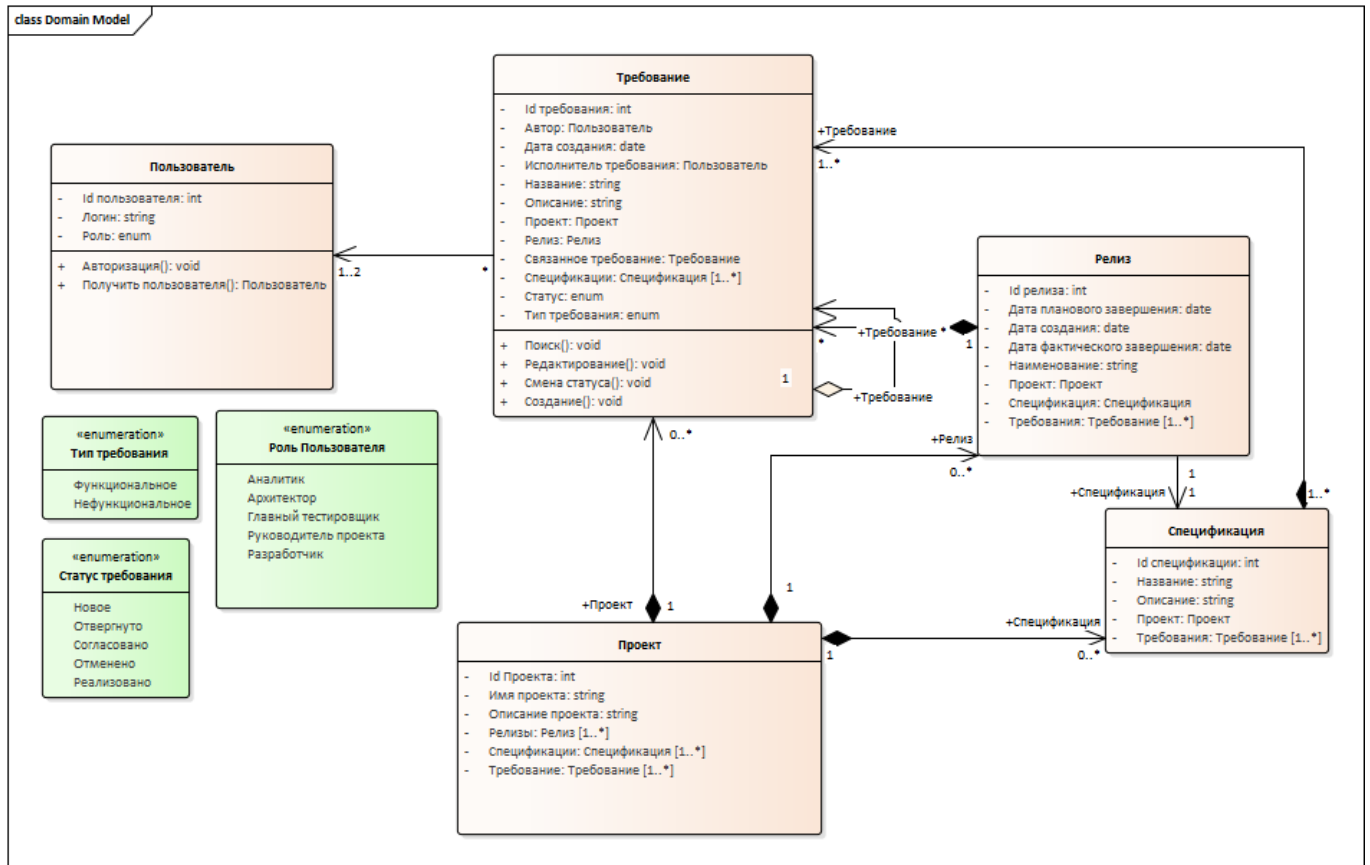
ПРИЛОЖЕНИЕ 4 (USE-CASE DIAGRAM)



ПРИЛОЖЕНИЕ 5 (СХЕМА БАЗЫ ДАННЫХ)



ПРИЛОЖЕНИЕ 6 (ДИАГРАММА КЛАССОВ)



МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ
КАФЕДРА КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ (№ 12)

Тема: Проектирование «ПРОЕКТИРОВАНИЕ ПОДСИСТЕМЫ
УПРАВЛЕНИЯ ТРЕБОВАНИЯМИ»

Коллективная разработка

ФИО	№ группы	Роли в проекте
Кутузов А.В.	М20-512	Архитектор, системный аналитик
Богословский Д.М	М20-512	Разработчик, Технический писатель
Лашина Д. С.	М20-512	Руководитель, бизнес-аналитик проекта
Ванин М.В.	М20-512	Разработчик, Бизнес-аналитик
Волков Е.А.	М20-512	Разработчик, Тестировщик

Оценка _____

Ст.преп.каф.12 _____

Красникова С.А.

Москва, 2021

КАФЕДРА КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ (№ 12)

**ПРОЕКТИРОВАНИЕ ПОДСИСТЕМЫ УПРАВЛЕНИЯ
ТРЕБОВАНИЯМИ
ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К ТЕХНИЧЕСКОМУ
ПРОЕКТУ**

Листов 32

Версия 1.0

Москва, 2021

АННОТАЦИЯ

В данном документе представлены автоматизируемые процессы, основные ключевые решения создаваемой АС и мероприятия по подготовке объекта автоматизации к вводу системы в действие.

СОДЕРЖАНИЕ

1. Общие положения.....	8
1.1. Наименование проектируемой Системы и ее условное обозначение.....	8
1.2. Перечень документов, на основании которых проектируется Система.....	8
1.3. Перечень организаций, участвующих в разработке Системы.....	8
1.4. Плановые сроки начала работы по созданию системы	8
1.5. Цели создания Системы.....	8
1.6. Назначение системы.....	9
1.7. Подтверждение соответствия проектных решений действующим нормам и правилам техники безопасности, пожаро- и взрывобезопасности	9
1.8. Сведения об использованных при проектировании нормативно-технических документах	10
1.9. Сведения о НИР, передовом опыте, изобретениях, использованных при разработке проекта	10
1.10. Очередность создания Системы и объем каждой очереди.....	10
2. ОПИСАНИЕ ПРОЦЕССА ДЕЯТЕЛЬНОСТИ.....	10
3. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ.....	11
3.1. Ограничения на технические решения.....	11
3.2. Решения по структуре Системы, подсистем, средствам и способам связи для информационного обмена между компонентами системы, подсистем.....	11
3.2.1. Схема компонент/модулей Системы.....	11
3.3. Решения по взаимосвязям Системы со смежными системами, обеспечению ее совместимости	11
3.4. Решения по режимам функционирования, диагностированию работы системы	12
3.5. Решения по численности, квалификации и функциям персонала АС, режимам его работы, порядку взаимодействия	12

3.6. Сведения об обеспечении заданных в техническом задании (ТЗ) потребительских характеристик системы (подсистем), определяющих ее качество	13
3.7. Состав функций, реализуемых системой (подсистемой)	15
3.8. Решения по комплексу технических средств, его размещению на объекте	17
3.9. Решения по составу информации, объему, способам ее организации, видам машинных носителей, входным и выходным документам и сообщениям, последовательности обработки информации и другим компонентам.....	17
3.10. Решения по составу программных средств, языкам программирования, алгоритмам процедур и операций и методам их реализации	17
3.11. Решения по обеспечению информационной безопасности.....	18
3.11.1. Угрозы информационной безопасности и точки возникновения угроз	18
4. Мероприятия по подготовке объекта автоматизации к вводу системы в действие.....	18
4.1. Мероприятия по приведению информации к виду, пригодному для обработки на ЭВМ	18
4.2. Мероприятия по обучению и проверке квалификации персонала.....	18
4.3. Мероприятия по созданию необходимых подразделений и рабочих мест	18
4.4. Мероприятия по изменению объекта автоматизации.....	18
Список использованных источников	19
ПРИЛОЖЕНИЕ А. Схема компонентов системы.....	20
Приложение б. Схема пользовательского интерфейса.....	21
Приложение В. ЛОГИЧЕСКАЯ МОДЕЛЬ ДАННЫХ	32
Список изменений	33

АРХИТЕКТУРА ИНТЕРФЕЙС

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Описание подсистем, компонент и интерфейсов системы

Разделяющая граница, через которую проходят данные или материальные объекты; соединение между двумя или большим числом компонентов модели, передающее данные или материальные объекты от одного компонента к другому

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АС

Автоматизированная система

БД

База данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Наименование проектируемой Системы и ее условное обозначение

Полное наименование проектируемой системы: *Подсистема управления требованиями*.
Далее по тексту также используется условное обозначение и «Подсистема».

1.2. Перечень документов, на основании которых проектируется Система

Техническое задание на проектирование подсистемы управления требованиями.

1.3. Перечень организаций, участвующих в разработке Системы

НИЯУ «МИФИ» (Национальный Исследовательский Ядерный Университет «МИФИ»).

1.4. Плановые сроки начала работы по созданию системы

Начало проекта: 07.09.2021 (7 сентября 2021 года)

Окончание проекта: не более 4 месяцев со дня начала работ.

1.5. Цели создания Системы

Цель создания Системы и критерии оценки достижения целей представлены в таблице 1.

Таблица 1 — Цели создания системы

Цель	Показатель	Критерии оценки достижения целей
Сокращение времени анализа требований для аналитика	Пользователь может задокументировать требование	Требование задокументировано пользователем
Сокращение времени анализа требований для тестировщика	Пользователь имеет доступ к требованиям и может их просматривать	Просмотр требований пользователем
В рамках подсистемы требований разработать функциональность для установки статуса требований пользователем	Пользователь имеет возможность установить статус для конкретного требования	Установка пользователем статуса требования
В рамках подсистемы требований разработать	Пользователь имеет возможность изменить требование	Требование изменено пользователем

Цель	Показатель	Критерии оценки достижения целей
функциональность для изменения требований пользователем		

1.6. Назначение системы

Подсистема управления требованиями предназначена для контроля действий разработки программного обеспечения.

ПУТР предназначена для:

- Управления контролем выполнения требований;
- Контроля качества выполняемых требований, сроков их выполнения;
- Изменения требований;
- Аналитики и принятия решений.

1.7. Подтверждение соответствия проектных решений действующим нормам и правилам техники безопасности, пожаро- и взрывобезопасности

Все внешние элементы технических средств Системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь зануление или защитное заземление в соответствии с ГОСТ 12.1.030-87 и ПУЭ. Система электропитания должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в цепях нагрузки, а также аварийное ручное отключение. Общие требования пожарной безопасности должны соответствовать нормам на бытовое электрооборудование. В случае возгорания не должно выделяться ядовитых газов и дымов. После снятия электропитания должно быть допустимо применения любых средств пожаротушения. Факторы, оказывающие вредные воздействия на здоровье со стороны всех элементов системы (в том числе инфракрасное, ультрафиолетовое, рентгеновское и электромагнитное излучение, вибрация, шум, электростатические поля, ультразвук строчной частоты и т.д.), не должны превышать норм (СанПиН 2.2.2./2.41340-03 от 03.06.2003 г.).

1.8. Сведения об использованных при проектировании нормативно-технических документах

При разработке автоматизированной системы и создании проектно-эксплуатационной документации Исполнитель должен руководствоваться требованиями следующих нормативных документов:

- ГОСТ 19.201-78. Техническое задание. Требования к содержанию и оформлению;
- ГОСТ 34.601-90. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания;
- ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплексность и обозначение документов при создании автоматизированных систем;

1.9. Сведения о НИР, передовом опыте, изобретениях, использованных при разработке проекта

При разработке системы никакие НИРы и изобретения не использовались.

1.10. Очередность создания Системы и объем каждой очереди

Очередность создания системы описана в таблице 2.

Таблица 2. Очередность создания системы

И д.	Название задачи	Длительность, дней	Начало	Окончание
1	Разработка плана и устава проекта	7	07.09	14.09
2	Моделирование автоматизируемых процессов	7	07.09	14.09
3	Моделирование функций системы	7	14.09	21.09
4	Моделирование предметной области	7	21.09	28.09
5	Разработка ТЗ	7	28.09	05.10
6	Разработка диаграммы сущность-связь	7	12.10	19.10
7	Разработка макета интерфейса пользователя	7	19.10	26.10
8	Проектирование архитектуры системы	7	26.10	02.11
9	Разработка модели угроз и модели нарушителя ИБ	7	02.11	09.11
10	Разработка ПЗ к ТП	7	09.11	16.11
11	Разработка прототипа системы	42	16.11	14.12
12	Документирование прототипа	14	14.12	21.12

2. ОПИСАНИЕ ПРОЦЕССА ДЕЯТЕЛЬНОСТИ

Сотрудниками компании должны быть сформулированы регламенты работы пользователей с Системой.

Требования к организации работ в условиях функционирования Системы представлены в разделе 3 ТЗ.

3. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ

3.1. Ограничения на технические решения

Ограничения на технические решения отсутствуют у данной подсистемы.

3.2. Решения по структуре Системы, подсистем, средствам и способам связи для информационного обмена между компонентами системы, подсистем

3.2.1. Схема компонент/модулей Системы

Схема компонентов Системы представлена в Приложении А.

3.3. Решения по взаимосвязям Системы со смежными системами, обеспечению ее совместимости

В данной подсистеме должна быть разработана функциональность создания требования, спецификации и релиза, а также хранения истории о данных сущностях. Описание подсистем представлено в таблице 3.

Таблица 3 - Назначение подсистем и их основные характеристики

№	Название подсистемы	Назначение подсистемы
1	Подсистема работы с требованиями	Создание и редактирование атомарных требований
2	Подсистема работы со спецификацией	Создание и редактирование спецификаций
3	Подсистема интеграции	Интеграция с системой управления проектами

Система должна быть разработана согласно общепринятым стандартам разработки для облегчения дальнейшей доработки и обслуживания всех компонентов системы, а также для взаимодействия со смежными системами:

- Моделирование поведения системы производится с помощью UML.
- Документация системы соответствует ГОСТ 34.

В рамках Проекта Подсистема управления требованиями должна взаимодействовать с Подсистемой управления задачами и проектами следующим образом: при запуске Подсистемы управления требованиями у Подсистемы управления проектами и задачами запрашивается актуальный список проектов (Id Проекта, Описание, Дата начала, Дата окончания), а также релизы (Id Проекта, Описание, Дата начала, Дата окончания). Повторный запрос списка проектов или

релизов может производиться пользователем вручную, по кнопке «Обновить». Для обмена информацией используется протокол HTTP, а также формат данных – JSON.

3.4. Решения по режимам функционирования, диагностированию работы системы

Система должна быть доступна в любое время. Время проведения профилактических работ оговаривается заранее, и не должно превышать 24 часа.

В полнофункциональном режиме доступны все функции системы для всех пользователей.

В режиме ограниченной функциональности происходит обслуживание системы, доступны функции только для администратора системы.

В аварийном режиме пользователи не имеют доступа к системе.

3.5. Решения по численности, квалификации и функциям персонала АС, режимам его работы, порядку взаимодействия

Требования к численности и квалификации персонала системы представлен в таблице 4.

Таблица 4 – Требования к численности и квалификации персонала системы.

№	Должность	Требования	Численность
1	Системный администратор	Системный администратор должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию программных и технических средств, применяемых в системе.	2
2	Администратор баз данных	Администратор баз данных должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию используемых в АС СУБД.	2
3	Пользователь (Аналитик)	Пользователь системы управления требованиями должен обладать навыками системного и интеграционного анализа для того, чтобы корректно выполнять работу по заполнению спецификации требований и учёта всех необходимых зависимостей.	5
4	Пользователь (Тестирующий)	Требования к квалификации в соответствии с занимаемой должностью. Дополнительная квалификация для работы с системой не требуется.	10

5	Пользователь (Разработчик)	Требования к квалификации в соответствии с занимаемой должностью. Дополнительная квалификация для работы с системой не требуется.	20
6	Пользователь (Руководитель проекта)	Требования к квалификации в соответствии с занимаемой должностью. Дополнительная квалификация для работы с системой не требуется.	5

Режим функционирования персонала:

- Системные администраторы: 5/2, 09:00 – 18:00. Однако, для обеспечения круглосуточной поддержки посменно следуют графику дежурств, а именно могут подключиться в нерабочее время для решения возникших проблем во время эксплуатации системы.
- Администраторы баз данных: 5/2, 09:00 – 18:00.
- Пользователи: 5/2, 09:00 – 18:00. Возможны индивидуальные изменения в рабочем графике со стороны работника или руководства.

Возможны внеплановые выходы в нерабочее время.

3.6. Сведения об обеспечении заданных в техническом задании (ТЗ) потребительских характеристик системы (подсистем), определяющих ее качество

В состав основных потребительских характеристик Системы входят:

- надежность;
- безопасность;
- производительность;
- время восстановления после сбоя.

Производительность

В таблице 5 приведены заданные параметры производительности.

Таблица 5. Параметры производительности

Тип запроса	Среднее число запросов к системе в минуту	Среднее время выполнения одного запроса в секундах	Максимальное число запросов к системе в минуту	Максимальное время выполнения одного запроса в секундах
Обновить список проектов	0.5	0.05	0.6	0.09
Создание требований	0.05	0.02	0.08	0.06
Создание зависимостей	0.05	0.03	0.08	0.05

Изменение статуса требования	0.2	0.01	0.33	0.03
Поиск по требованиям	0.4	0.06	0.66	0.09

Требуемая производительность достигается путем использования протоколов HTTP, JSON, а также СУБД MySQL.

Надежность

Для обеспечения требуемой надежности и высокой готовности, определены общие точки отказа. и предложены способы устранения. В таблице 6 приведено описание точек отказа и способов их устранения.

Таблица 6. Устранение общих точек отказа

Точка отказа	Способ устранения
Узел	Использование нескольких узлов
Источник питания	Использование ИБП или отдельных линий электропитания
Сетевой адаптер	Использование резервных сетевых адаптеров
Сеть	Использование резервных сетей для связи между узлами
Диск	Использование резервных дисков и RAID-технологий
Приложение	Использование мониторинга приложений и автоматического подхвата приложения резервным узлом

На основании проведенного анализа предлагается трехзвенная архитектура.

Преимущества выбранного решения:

- при изменении бизнес-логики нет необходимости изменять клиентские приложения и обновлять их у всех пользователей;
- максимально снижаются требования к аппаратуре пользователей;
- резервные блоки питания для подсистемы хранения данных.

Если какой-либо компонент такого решения выйдет из строя, резервный компонент подхватит его работу.

Технические решения по обеспечению времени восстановления после сбоя

Для обеспечения времени восстановления после сбоя предлагаются следующие меры:

- разработан план мероприятий по восстановлению после сбоя;
- обеспечено резервное копирование данных БД в оперативном режиме без остановки работы системы;
- использование резервного сервера БД.

3.7. Состав функций, реализуемых системой (подсистемой)

Описание функций Системы представлено в таблицах 7-9.

Таблица 7 – функции подсистемы работы с требованиями

№	Функция	Описание
1	Внесение атомарных требований	<p>Аналитик в системе может создать требование. Для этого ему необходимо заполнить следующие поля:</p> <ul style="list-style-type: none"> • Имя требования; • Описание требования; • Статус требования (по умолчанию создается со статусом «Новое»); • Исполнитель требования (может быть указан позже); • Спецификация, в которую данное требование входит (может быть указана позже); • Тип требования; • Связанное требование (при необходимости); • Тип связи (при необходимости); <p>У требования могут быть следующие статусы:</p> <ul style="list-style-type: none"> • Новое; • Отвергнуто; • Согласовано; • Отменено; • Реализовано; • Нереализовано. <p>Требование может иметь следующие типы:</p> <ul style="list-style-type: none"> • Функциональное; • Нефункциональное. <p>У требования могут быть следующие типы связи:</p> <ul style="list-style-type: none"> • Иерархия; • Зависимость.
2	Модификация требований	При модификации требования в системе может быть изменён его статус, имя, описание, тип, исполнитель,
3	Просмотр списка требований	Возможность просматривать наборы требований, сгруппированных по различным правилам (Принадлежность к конкретной спецификации/релизу, дата, исполнитель, тип, статус)
4	Поиск требований	Возможность получить запрошенное требование по части его имени или описания.
5	Установка отметки о выполнении требования	Требование, выполнение которого подтверждено командой тестирования может быть отмечено в системе как выполненное

Таблица 8 – функции подсистемы работы со спецификациями

№	Функция	Описание
1	Создание спецификации	<p>Аналитик в системе может создать спецификацию. Для этого ему необходимо заполнить следующие поля:</p> <ul style="list-style-type: none"> • Версия спецификации (автоматически подтягивается из Релиза); • Список требований; • Статус спецификации (по умолчанию создается со статусом «Не согласована»); • Создатель спецификации (добавляется автоматически). <p>У спецификации могут быть следующие статусы:</p> <ul style="list-style-type: none"> • Не согласована; <p>Согласована.</p>
2	Редактирование спецификации	<p>Аналитик может редактировать спецификацию до её согласования. Редактирование включает добавление требований в спецификацию, удаление требований из спецификации. Изменение описания и имени спецификации</p>
3	Согласование спецификации	<p>Статус спецификации может быть изменён на «Согласована» при условии проверки её Архитектором и Главным Тестирующим.</p>
4	Согласование Руководителем	<p>При утверждении спецификации руководителем из неё автоматически создаётся Релиз, в который копируются все требования из спецификации</p>

Таблица 9 – функции подсистемы интеграции

№	Функция	Описание
1	Получение данных о проектах из внешней системы	Загрузка в систему данных о проектах из внешней системы.
2	Синхронизация данных о проектах с внешней системой	Информация о проекте в системе может быть обновлена с учётом новых данных во внешней системе.
3	Выгрузка данных о проектах во внешнюю систему	Внешняя система может запросить данные о проекте (спецификации, релизы, списки требований)

3.8. Решения по комплексу технических средств, его размещению на объекте

Для корректного функционирования Системы необходимы следующие технические средства:

- сервер баз данных;
- сервер приложений;
- рабочие станции (для клиента).

Требования к аппаратному обеспечению клиента:

- ОС: любая ОС, имеющая графический интерфейс и поддерживающая работу клиентского ПО, приведенного в 4.3.3.

- Процессор: Intel Core i3, а также более современные
- Оперативная память: 4 GB ОЗУ
- Сеть: Широкополосное подключение к интернету
- Место на диске: 5 GB

Требования к аппаратному обеспечению сервера приложений:

- Операционная система: 64-разрядная; семейства UNIX – Centos 7, Debian
- Процессор: Intel Core i5-4430 / AMD FX-6300, а также более современные
- Оперативная память: не менее 8 GB ОЗУ
- Сеть: Широкополосное подключение к интернету: не менее 100 МБит
- Место на диске: 500 GB

3.9. Решения по составу информации, объему, способам ее организации, видам машинных носителей, входным и выходным документам и сообщениям, последовательности обработки информации и другим компонентам

Логическая модель хранимых данных и ее описание представлены в Приложении В.

3.10. Решения по составу программных средств, языкам программирования, алгоритмам процедур и операций и методам их реализации

Используемое при разработке программное обеспечение и библиотеки программных кодов должны иметь широкое распространение, быть общедоступными и использоваться в промышленных масштабах.

Браузер на стороне клиента: Google Chrome или Mozilla Firefox.

Требования к ПО сервера приложений: Python.

Требования к ПО сервера базы данных: MySQL.

3.11. Решения по обеспечению информационной безопасности

3.11.1. Угрозы информационной безопасности и точки возникновения угроз

Модель угроз и модель нарушителя информационной безопасности Системы представлены в соответствующем документе «Модель угроз и нарушителя информационной безопасности».

4. МЕРОПРИЯТИЯ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СИСТЕМЫ В ДЕЙСТВИЕ

4.1. Мероприятия по приведению информации к виду, пригодному для обработки на ЭВМ

Мероприятия по приведении информации к виду, пригодному для обработки ЭВМ не проводятся.

4.2. Мероприятия по обучению и проверке квалификации персонала

Необходимо составить следующие программы обучения:

- для пользователя системы;
- для администратора системы.

Для пользователей системы необходимо провести обучение по следующим дисциплинам:

- описание общей концепции «Подсистемы управления требованиями»;
- описание структуры;
- ввод данных в систему.

Для администратора системы необходимо провести обучение по следующим дисциплинам:

- описание общей концепции «Подсистемы управления требованиями»;
- описание схема БД;
- администрирование «Подсистемы управления требованиями».

4.3. Мероприятия по созданию необходимых подразделений и рабочих мест

Специальные мероприятия по созданию подразделений и рабочих мест не требуются, поскольку система должна быть развернута на имеющихся рабочих местах.

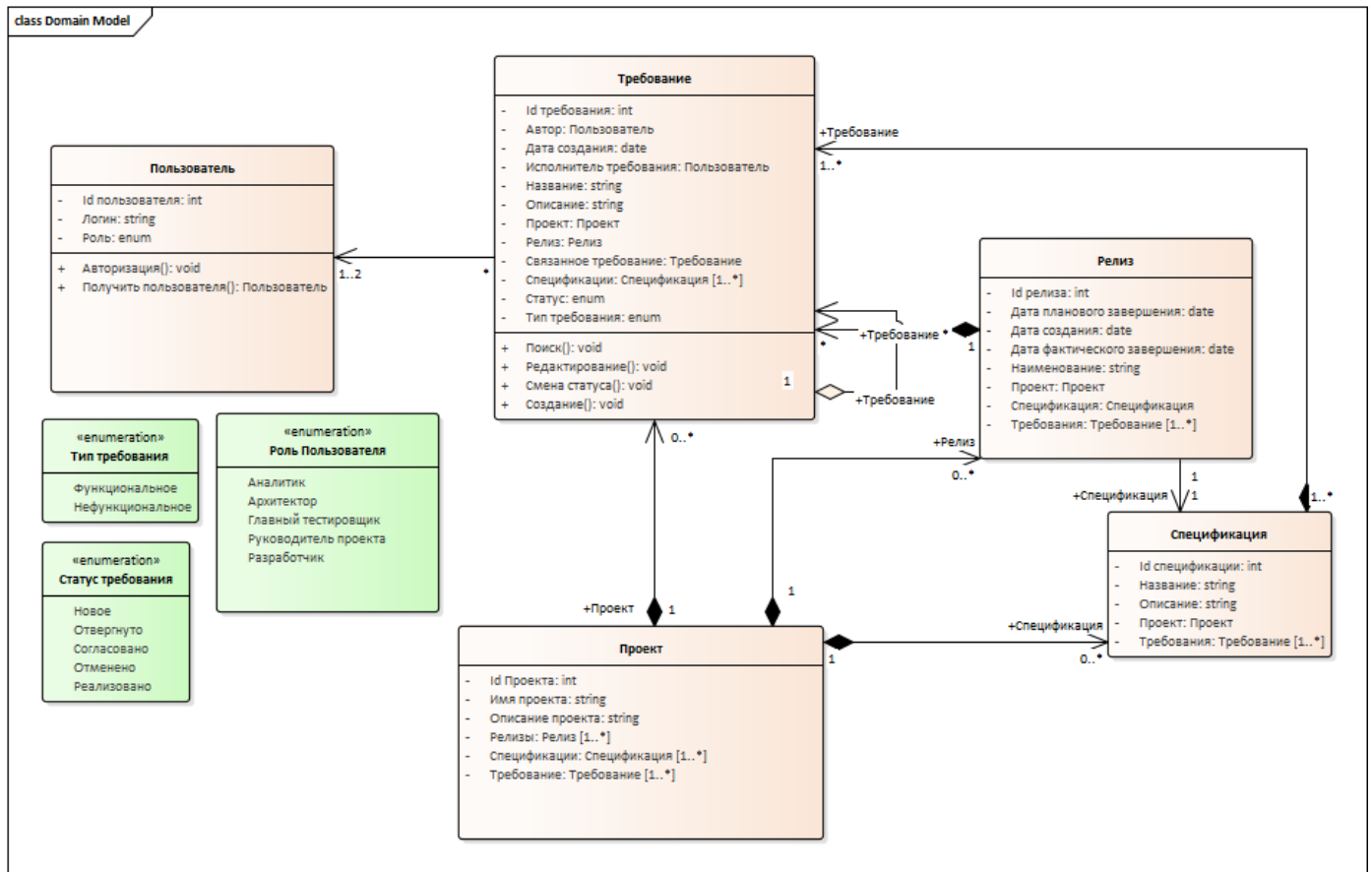
4.4. Мероприятия по изменению объекта автоматизации

Мероприятия по изменению объекта автоматизации не планируются.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

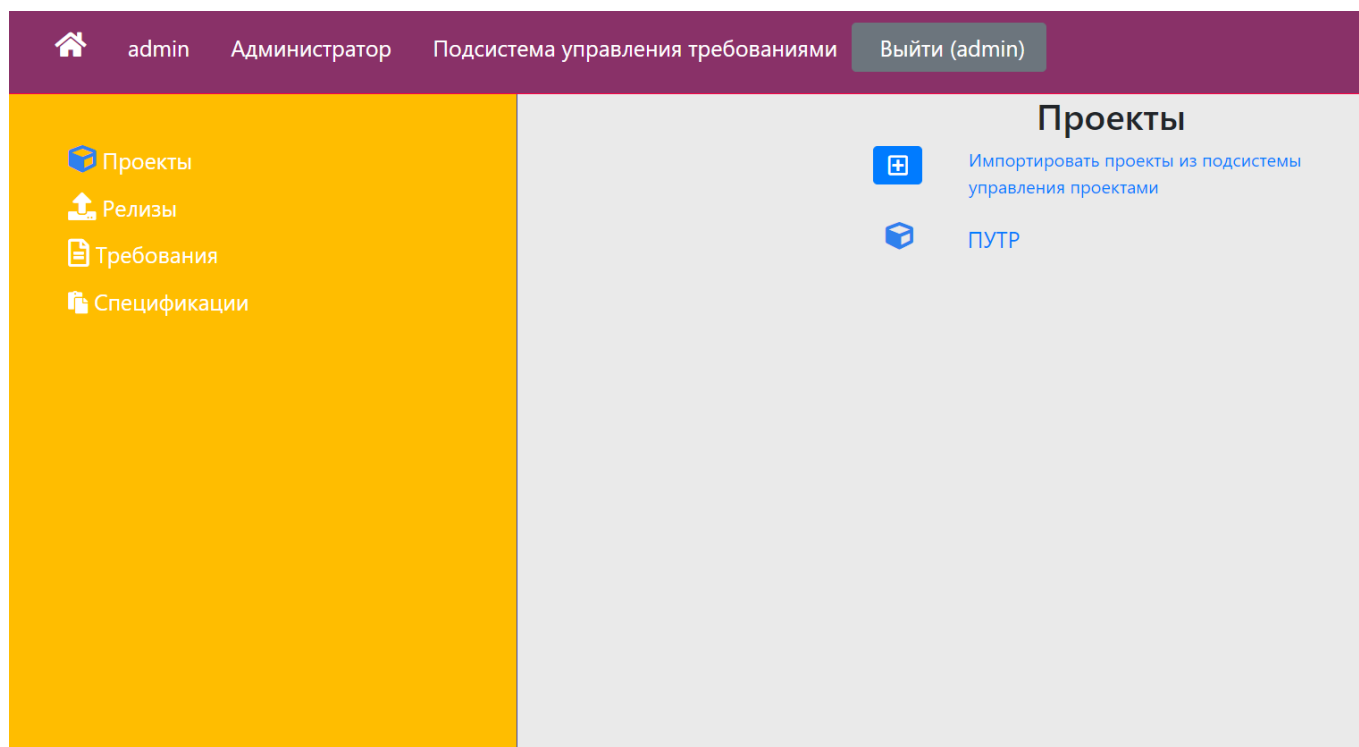
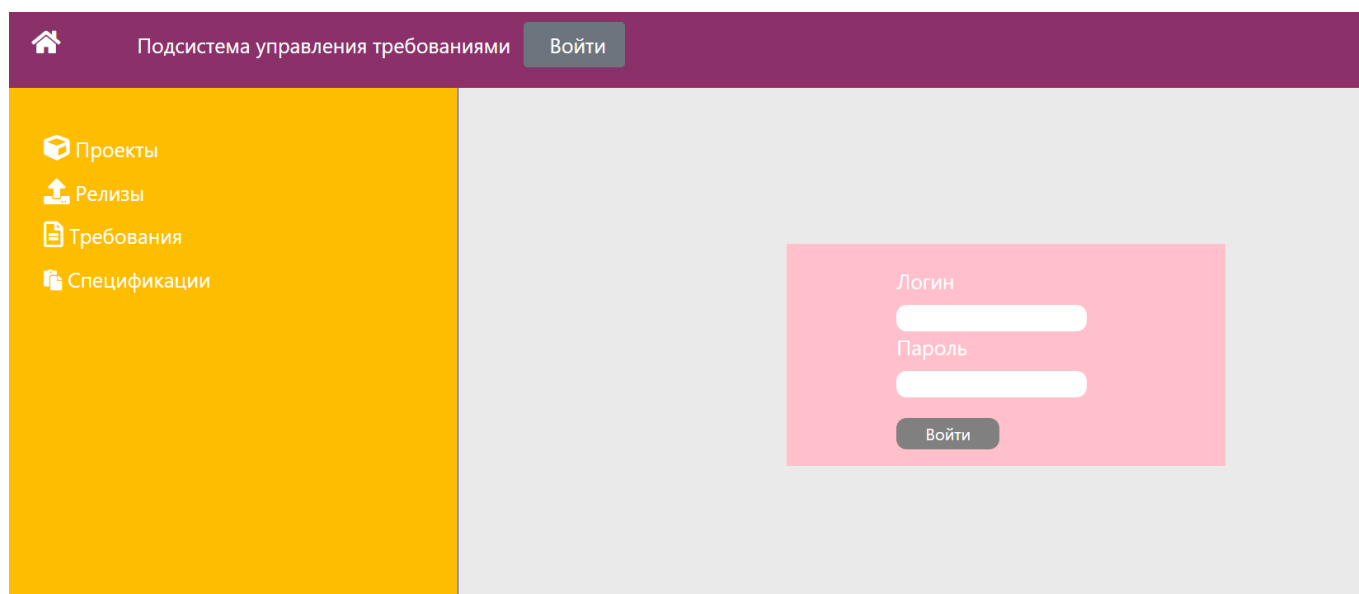
1. ГОСТ 2.105-95 Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам.
2. РД 50-34.698-90 Автоматизированные системы. Требования к содержанию документов


ПРИЛОЖЕНИЕ А. **СХЕМА КОМПОНЕНТОВ СИСТЕМЫ**





ПРИЛОЖЕНИЕ Б.


СХЕМА ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА




 admin Администратор Подсистема управления требованиями Выйти (admin)

 Проекты

 Релизы

 Требования

 Спецификации

Проект ПУТР

Описание: Подсистема управления требованиями

Релизы:

[Путр_0.01](#)

[Путр_0.02](#)

Спецификации:

[Путр_1.0](#)

[Путр_1.1](#)

Требования:


[Создание требования](#)


[Создание проекта](#)


[Создание спецификации](#)


[Вход в систему](#)


Удалить Редактировать

 admin Администратор Подсистема управления требованиями Выйти (admin)

 Проекты

 Релизы

 Требования

 Спецификации

Создание проекта

Название проекта:

Описание:

Описание

Создать проект

admin Администратор Подсистема управления требованиями Выйти (admin)

Проекты

Релизы

Требования

Спецификации

Релизы

Путр_0.01 (Проект [ПУТР](#), Спецификация [Путр_1.0](#))

Путр_0.02 (Проект [ПУТР](#), Спецификация [Путр_1.1](#))

admin Администратор Подсистема управления требованиями Выйти (admin)

Проекты

Релизы

Требования

Спецификации

Создание релиза

Версия:

Версия релиза

Проект:

▼

Спецификация:

▼

Время начала:

Время старта

Время окончания:

Время окончания

Описание:

Описание

Создать релиз

admin Администратор Подсистема управления требованиями Выйти (admin)

Проекты

Релизы

Требования

Спецификации

Требования

Вход в систему (Спецификация Путр_1.1)

Создание требования (Спецификация Путр_1.0)

Создание проекта (Спецификация Путр_1.0)

Создание спецификации (Спецификация Путр_1.0)

admin Администратор Подсистема управления требованиями Выйти (admin)

Проекты

Релизы

Требования

Спецификации

Создание требования

Имя:

Описание:

Статус:

Тип требования:

Исполнитель:


Спецификация:


Связанные требования:


Вход в систему
Создание требования
Создание проекта
Создание спецификации


Тип связи:


Создать требование


 admin Администратор Подсистема управления требованиями [Выйти \(admin\)](#)


 Проекты


 Релизы


 Требования


 Спецификации


Спецификации 


 Путр_1.0


 Путр_1.1

 admin Администратор Подсистема управления требованиями [Выйти \(admin\)](#)

 Проекты

 Релизы

 Требования

 Спецификации

Спецификация Путр_1.0

Требования:

[Создание требования](#)

[Создание проекта](#)

[Создание спецификации](#)

Дата создания: 18 января 2022 г. 1:19

Создал: admin

Статус: Несогласовано

[Удалить](#) [Редактировать](#)



admin

Администратор

Подсистема управления требованиями

Выйти (admin)



Проекты



Релизы



Требования



Спецификации

Создание спецификации

Версия:

Статус:



Создать спецификацию

ПРИЛОЖЕНИЕ В.

ЛОГИЧЕСКАЯ МОДЕЛЬ ДАННЫХ



СПИСОК ИЗМЕНЕНИЙ

Дата	Версия	Описание изменений	Автор

ПОДСИСТЕМА УПРАВЛЕНИЯ ТРЕБОВАНИЯМИ
МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Версия 1.0

СОГЛАСОВАНО

Должность

Х.

Х. XXXX

(личная подпись)
(расшифровка подписи)

«__» _____ 2021 г

Представители организации
Разработчика

Должность

Х.

Х. XXXX

(личная подпись)
(расшифровка подписи)

«__» _____ 2021 г

2021

КАФЕДРА КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ (№ 12)

**ПРОЕКТИРОВАНИЕ ПОДСИСТЕМЫ УПРАВЛЕНИЯ
ТРЕБОВАНИЯМИ**

**МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЕЙ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Листов 23

Версия 1.0

Москва, 2021

Аннотация

В документе «Модель угроз информационной безопасности» определены необходимые меры и средства по предотвращению реализации нарушителем угроз информационной безопасности в отношении ресурсов подсистемы «*Управление требованиями*». (ПУТР)

Модель угроз информационной безопасности является основой для определения состава необходимых режимных, организационно-технических и технических мер защиты ПУТР.

Модель угроз информационной безопасности ПУТР содержит:

- описание ПУТР;
- описание модели нарушителя информационной безопасности ПУТР;
- перечень угроз информационной безопасности (с привязкой к потенциальным нарушителям) ПУТР;
- меры по противодействию угрозам информационной безопасности в ПУТР.

Содержание

Термины и определения	7
1. Общие положения.....	9
1.1. Цели создания модели угроз и модели нарушителя информационной безопасности	9
1.2. Область применения	9
1.3. Общие принципы формирования	9
1.4. Правила пересмотра	9
2. Описание ПУТР	10
2.1. Наименование информационной системы	10
2.2. Цели создания и назначение ПУТР	10
2.3. Общее описание архитектуры ПУТР	10
2.4. Физические лица, имеющие доступ к компонентам ПУТР	11
2.5. Информация, обрабатываемая в ПУТР	12
Персональные данные.....	12
Конфиденциальная информация	13
Общедоступная информация	13
2.6. Объекты защиты.....	13
3. Модель нарушителя информационной безопасности.....	13
3.1. Общие положения	13
3.2. Описание нарушителей.....	13
3.3. Предположения об имеющихся у нарушителей средствах атак	14
3.4. Предположения об имеющихся у нарушителей средствах атак	16
3.5. Описание каналов атак	17

4. Модель угроз	17
4.1. Общие положения	17
5. Меры по противодействию угрозам ИБ	17
6. Заключение	23

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

БД	–	База данных
ЖЦ	–	Жизненный цикл
ИБ	–	Информационная безопасность
ИС	–	Информационная система управления правами на результаты интеллектуальной деятельности
ИТ	–	Информационные технологии
НСД	–	Несанкционированный доступ
ПДн	–	Персональные данные
ПО	–	Программное обеспечение
СВТ	–	Средства вычислительной техники
СЗИ	–	Система защиты информации
СОИБ	–	Система обеспечения информационной безопасности
СрЗИ	–	Средство защиты информации
ТС	–	Техническое средство
ПУТР	–	Подсистема управления требованиями

Термины и определения

Атака	Целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой информации или с целью создания условий для этого.
Безопасность информации (данных)	Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.
Защищаемая информация	Информация, для которой обладателем информации определены характеристики ее безопасности.
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
Информация	Сведения (сообщения, данные) независимо от формы их представления
Канал атаки	Среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки.
Конфиденциальная информация	Информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.
Конфиденциальность информации	Обязательное для выполнения требование не передавать такую информацию третьим лицам без согласия ее обладателя лицом, получившим доступ к определенной информации.
Модель нарушителя	Предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.
Модель угроз	Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Нарушитель (субъект атаки)	Лицо (или иницируемый им процесс), проводящее (проводящий) атаку.
Регистрация данных	Ввод данных пользователем в формы, предоставляемые интерфейсом пользователя ИС.
Роль	Совокупность функциональных возможностей (привилегий) пользователя ИС, позволяющая разграничивать доступ к различным функциям ИС. Соответствие ролям пользователей определенных функциональных возможностей определяется моделью определения прав доступа.
Средство защиты информации	Техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.
Угроза информационной безопасности организации	Совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации.

1. Общие положения

1.1. Цели создания модели угроз и модели нарушителя информационной безопасности

Целью создания модели угроз ИБ и модели нарушителя ИБ ПУТР является формирование единого перечня угроз и мер по противодействию им в рамках ПУТР.

1.2. Область применения

Настоящая модель угроз ИБ и модель нарушителя ИБ предназначена для определения состава мер по защите информации в ПУТР.

Модель угроз ПУТР должна учитываться при построении СЗИ ПУТР.

1.3. Общие принципы формирования

Разработка модели угроз ИБ ПУТР основывается на следующих принципах:

- При формировании модели угроз необходимо учитывать угрозы, осуществляющие нарушение безопасности информации (далее по тексту – прямая угроза), а также угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы).
- Защищаемая информация обрабатывается и хранится в ПУТР с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

1.4. Правила пересмотра

Настоящая модель угроз ИБ и модель нарушителя ИБ может уточняться, дополняться или изменяться в соответствии с установленным порядком. Основанием для пересмотра настоящего документа служат:

- Изменения законодательства РФ в области защиты информации.
- Изменения в информационной системе.

2. Описание ПУТР

2.1. Наименование информационной системы

Наименование проекта: Подсистема управления требованиями

Условное обозначение: ПУТР

2.2. Цели создания и назначение ПУТР

Подсистема управления требованиями предназначена для контроля действий разработки программного обеспечения.

ПУТР предназначена для:

- Управления контролем выполнения требований.
- Контроля качества выполняемых требований, сроков их выполнения.
- Изменения требований.
- Аналитики и принятия решений.

Цели создания ПУТР:

- Сокращение времени анализа требований для аналитика;
- Сокращение времени анализа требований для тестировщика;
- В рамках подсистемы требований разработать функциональность для установки статуса требований пользователем;
- В рамках подсистемы требований разработать функциональность для изменения требований пользователем;

2.3. Общее описание архитектуры ПУТР

ПУТР является многопользовательской ИС. По виду автоматизируемой деятельности ПУТР относится к системам управления, сбора, хранения, обработки и передачи информации.

Технические средства (ТС) ПУТР включает сервера БД, серверы приложений.

Информация, обрабатываемая в ПУТР, передается по защищенным каналам связи, в том числе при взаимодействии с пользователями, участвующими в процессе обработке защищаемой информации. ПУТР имеет подключение к сети Интернет.

ПУТР реализована в виде клиент-серверного приложения. Инфраструктура приложения может функционировать как на серверах Заказчика, так и на бесплатных хост серверах. Территориальное расположение серверов не представляет особой значимости, главным фактором является их доступность.

ПУТР разработан с использованием фреймворка Django на языке Python3.

Архитектура ПУТР опирается на следующие требования для функционирования сервера приложений:

- Операционная система сервера: 64-разрядная; Centos 7, Debian и более современные
- Процессор: Intel Core i5-4430 / AMD FX-6300, а также более современные
- Оперативная память: 8 GB ОЗУ
- Сеть: Широкополосное подключение к интернету
- Место на диске: 500 GB

А также требования к аппаратному обеспечению клиента:

- Операционная система на стороне клиента: Любая.
- Процессор: Intel Core i3, а также более современные
- Оперативная память: 4 GB ОЗУ
- Сеть: Широкополосное подключение к интернету
- Место на диске: 5 GB

2.4. Физические лица, имеющие доступ к компонентам ПУТР

Возможности пользователя по взаимодействию с Системой и доступу к информации определяются интерфейсом, разработанным для каждой роли пользователей. В таблице 1 представлены категории ролей пользователей системы, имеющих доступ к ее ресурсам.

Таблица 1 – Перечень ролей пользователей, имеющих доступ к ресурсам Системы

Категория	Тип доступа	Описание
Системный администратор	Доступ к серверным компонентам средствам ПУТР Имеет полный доступ к функциональности и информационным ресурсам Системы.	Сотрудники организации, обеспечивающие функционирование сервера системы ПУТР.
Администратор баз данных	Имеет полный доступ к данным, обрабатываемым системой.	Сотрудники организации, осуществляющие выполнение работ по установке, настройке и администрированию используемых в АС СУБД.
Пользователь	Имеют ограниченный доступ	

Категория	Тип доступа	Описание
	к web-интерфейсу системы и предоставляемым им функциям.	
Пользователи смежных систем	Имеют доступ к полной информации по требованиям к проектам.	

2.5.Информация, обрабатываемая в ПУТР

В ПУТР обрабатывается информация следующих категорий:

- Иные категории персональных данных (ПДн), не отнесенные к специальным, биометрическим или общедоступным, в соответствии с пунктом 5 Постановления Правительства Российской Федерации № 1119 от 01.11.2012 г.

Постановление Правительства Российской Федерации от 13 февраля 2019 г. № 146 "Об утверждении правил организации и осуществления государственного контроля и надзора за обработкой персональных данных"

- информация, составляющая коммерческую тайну;
- сведения, составляющие служебную информацию ограниченного распространения (служебная тайна);

В ПУТР обработка речевой и видео информации не осуществляется.

Персональные данные

Персональные данные включают в себя, в частности следующую информацию:

- Фамилию, имя, отчество (ФИО).
- Имя учетной записи пользователя.
- Адрес электронной почты.
- Должность.

Конфиденциальная информация

К конфиденциальной информации, обрабатываемой в ПУТР, относятся сведения о проектах, релизах, спецификациях, требованиях.

Общедоступная информация

В ПУТР не хранится общедоступная информация.

2.6. Объекты защиты

Защищаемыми ресурсами Системы являются:

- обрабатываемая и защищаемая в системе информация (файлы, записи БД);
- системное и прикладное ПО;
- технические средства обработки (клиентская рабочая станция пользователя, серверные машины и коммутационное оборудование);
- каналы связи, используемые для взаимодействия компонентов системы;

3. Модель нарушителя информационной безопасности

3.1. Общие положения

Модель нарушителя ИБ содержит описание предположений о возможностях нарушителя, которые он может использовать для разработки и проведения атак на компоненты ПУТР, а также об ограничениях на эти возможности.

3.2. Описание нарушителей

По отношению к месту проведения атак потенциальные нарушители подразделяются на два типа:

- Внешние – нарушители, осуществляющие атаки не имевшие и/или не имеющие авторизованного доступа к системе.
- Внутренние – нарушители из категорий I–IV, осуществляющие атаки имея определенный авторизованный доступ к системе.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию для целей нарушения безопасности ПДн, так как состав информации, хранимой и обрабатываемой в Системе, не представляет интереса для внешнего нарушителя.

Перечень категорий внутренних нарушителей информационной безопасности и имеющейся у них информации об объектах реализации угроз Системы приведен в таблице.

Таблица 2 – Категории внутренних нарушителей безопасности информации

Категория	Описание	Имеющаяся у нарушителя информация об объектах реализации угроз
Категория I	Системный администратор	Информация о структуре данных,

	Системы	используемых в процессе коммуникациями со связанными подсистемами. Параметры сетевой конфигурации настоящей системы и идентификационные данные системы. Информационное обеспечение системы.
Категория II	Администратор баз данных	Полный доступ к данным, обрабатываемым системой. Доступ к идентификационным данным пользователей системы.
Категория III	Пользователь смежной системы	Полный доступ на чтение к данным проекта: Релизы, спецификации, требования
Категория IV	Пользователь	Информация о данных, обрабатываемых системой в соответствии с правами доступа, установленного для данного пользователя.

3.3.Предположения об имеющихся у нарушителей средствах атак

Внутренний нарушитель может использовать доступные в свободной продаже технические средства и ПО, специально разработанные технические средства и ПО.

Таблица 3 – Соответствие между ролями пользователей в системе и категориями нарушителей

Предположения о наличии информации	Категория нарушителя				
	Внешний	Внутренний			
		1	2	3	4
		Системный администратор	Администратор БД	Пользователи смежных систем	Пользователь
Части защищаемой информации, передаваемой по внутренним каналам	–	+	+	-	-
Имена учетных записей зарегистрированных пользователей (без паролей)	–	+	+	-	-
Не менее одной связки <имя, пароль УЗ> для доступа к подсистемам ИС	–	+	+	+	+
Полная информация о системном и прикладном ПО, используемом в ИС	–	+	+	-	-
Информация об алгоритмах и программах обработки защищаемой информации	+	+	+	+	+
Парольная информация для административного доступа к компонентам ИС	–	+	-	-	-
Сведения о линиях связи, по которым передается защищаемая информация	–	+	+	-	-
Журнал событий ИБ компонента ИС	–	+	-	-	-
Журнал событий СЗИ	–	+	+	-	-
Все проявляющиеся в ИС нарушения правил эксплуатации СЗИ	–	+	+	-	-

3.4.Предположения об имеющихся у нарушителей средствах атак

Потенциальные нарушители различных типов обладают различным уровнем доступа к компонентам ИС, а также различным уровнем квалификации. Таким образом, следует классифицировать нарушителей относительно имеющихся у них средств атак. Предположения об имеющихся у нарушителей средствах атак представлены в таблице **Error! Reference source not found..**

Таблица 4 – Предположения об имеющихся у нарушителей средствах атак

Предположения о наличии информации	Категория нарушителя				
	Внешний	Внутренний			
		1	2	3	4
		Системный администратор	Администратор БД	Пользователи смежных систем	Пользователь
Доступное в свободной продаже ПО	+	+	+	+	+
Специально разработанные технические средства и программное обеспечение (в том числе снифферы и программ анализа защищенности (сетевых сканеров безопасности))	+	+	+	-	-

3.5. Описание каналов атак

Для осуществления доступа к ресурсам Системы внутренний нарушитель может использовать следующие каналы атак:

- физический доступ к штатным программно-аппаратным средствам системы;
- носители информации, в том числе съемные.

Возможны следующие способы атак:

- негласное (скрытое) временное изъятие или хищение съемных носителей защищаемой информации, аутентифицирующей или ключевой информации;
- вызывание сбоев технических средств;
- внесение неисправностей в технические средства.

4. Модель угроз

4.1. Общие положения

В данном разделе содержится структурированный перечень угроз ИБ с привязкой к потенциальным нарушителям ИБ, способным реализовать эти угрозы.



Структурированный_
перечень_угроз_ИБ_Г

[Ссылка на таблицу с моделями угроз и нарушителями ИБ \(файл «Структурированный перечень угроз ИБ ПУТР.xls»\)](#)

5. Меры по противодействию угрозам ИБ

Перечень мероприятий для противодействия угрозам предполагает использование мер как технического, так и организационного порядка в отношении угроз, степень опасности которых не ниже высокой. Предлагаемые мероприятия направлены на обеспечение защиты ресурсов в целях снижения негативных последствий при реализации угроз.

Описание мероприятий по защите ресурсов представлено в таблице 5.

Таблица 5 - Описание мероприятий по защите ресурсов

№ п/п	Наименование угрозы	Меры по защите от угроз	
		Организационные	Технические
1.	Угроза анализа криптографических алгоритмов и их реализации	Использование актуальных версий сертифицированных средств криптографической защиты информации.	Своевременная установка обновлений программного обеспечения, направленного на устранение выявленных уязвимостей ПО
2.	Угроза доступа к локальным файлам сервера при помощи URL	Использование сертифицированного программного обеспечения и средств защиты информации. Мониторинг информации об обнаружении уязвимостей используемого ПО и выпуске соответствующих исправлений.	Своевременная установка обновлений программного обеспечения, направленного на устранение выявленных уязвимостей ПО
3.	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Инвентаризация и анализ установленного на серверах программного обеспечения на предмет наличия учетных записей «по умолчанию»	Блокирование встроенных учетных записей с администраторскими правами
4.	Угроза неправомерного ознакомления с защищаемой информацией	Определение перечня лиц, допущенных в помещение, где расположены компоненты ГИС. Использование плотных штор или жалюзи на окнах. Меры по получению доступа в помещение. Ручная блокировка экрана	Автоматическая блокировка экрана по достижении заданного времени не активности.
5.	Угроза неправомерных действий в каналах связи		Защита шифровальными (криптографическими) методами каналов передачи данных
6.	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Мониторинг состояния средств межсетевого экранирования и фильтрации сетевого трафика	Исключение средствами межсетевого экранирования доступа из внешних сетей к активному сетевому оборудованию, установка в

			настройках оборудования разрешения на администрирование устройств только с определенного пула адресов, принадлежащих внутренней сети организации
7.	Угроза несанкционированного удаления защищаемой информации	Определение перечня лиц, допущенных в помещение, где расположены компоненты ГИС	Минимизация прав пользователей в системе
8.	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Мониторинг состояния средств межсетевого экранирования и фильтрации сетевого трафика	
9.	Угроза обхода некорректно настроенных механизмов аутентификации	Использование сертифицированного программного обеспечения и средств защиты информации. Мониторинг информации об обнаружении уязвимостей используемого ПО и выпуске соответствующих исправлений.	Своевременная установка обновлений программного обеспечения, направленного на устранение выявленных уязвимостей ПО
10.	Угроза перехвата данных, передаваемых по вычислительной сети		Защита шифровальными (криптографическими) методами каналов передачи данных
11.	Угроза подмены действия пользователя путём обмана	Разработка инструкции по работе в системе, доведение ее до пользователей	Минимизация прав пользователей в системе
12.	Угроза включения в проект не достоверно испытанных компонентов	Использование сертифицированного программного обеспечения и средств защиты информации. Мониторинг информации об обнаружении уязвимостей используемого ПО и выпуске соответствующих исправлений.	
13.	Угроза заражения компьютера при посещении неблагонадёжных сайтов		Регулярное обновление вирусных дефиниций АВПО на серверах и АРМ пользователей, использование на сервере АВПО

			отличного по производителю от АВПО, установленного на АРМах пользователей.
14.	Угроза «кражи» учётной записи доступа к сетевым сервисам	Мониторинг состояния средств межсетевого экранирования и фильтрации сетевого трафика	Настройка соответствующих правил на межсетевом экране
15.	Угроза неправомерного шифрования информации		Регулярное обновление вирусных дефиниций АВПО на серверах и АРМ пользователей, использование на сервере АВПО отличного по производителю от АВПО, установленного на АРМах пользователей. Регулярное полное резервное копирование данных. Глубина копирования – не более одного дня.
16.	Угроза скрытного включения вычислительного устройства в состав бот-сети	Использование сертифицированного программного обеспечения	Регулярное обновление вирусных дефиниций АВПО на серверах и АРМ пользователей, использование на сервере АВПО отличного по производителю от АВПО, установленного на АРМах пользователей
17.	Угроза «фишинга»:	Информирование пользователей о методах и средствах «фишинга». Регламентация доступа пользователей к ресурсам сети Интернет	
18.	Угроза отказа подсистемы обеспечения температурного режима	Разработка инструкции по действиям сотрудников охраны в случае срабатывания датчика по превышению температуры в	Оснащение серверного помещения основным и резервным кондиционером,

		серверном помещении	установка сигнального датчика и вывод тревожного сигнала на пост охраны здания организации
19.	Угроза внедрения вредоносного кода через рекламу, сервисы и контент		Регулярное обновление вирусных дефиниций АВПО на серверах и АРМ пользователей, использование на сервере АВПО отличного по производителю от АВПО, установленного на АРМах пользователей
20.	Угроза подмены программного обеспечения	Использование сертифицированного программного обеспечения	
21.	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет:		Регулярное обновление вирусных дефиниций АВПО на серверах и АРМ пользователей, использование на сервере АВПО отличного по производителю от АВПО, установленного на АРМах пользователей
22.	Угроза использования уязвимых версий программного обеспечения	Использование сертифицированного программного обеспечения и средств защиты информации. Мониторинг информации об обнаружении уязвимостей используемого ПО и выпуске соответствующих исправлений	Своевременная установка обновлений программного обеспечения, направленного на устранение выявленных уязвимостей ПО
23.	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Мониторинг информации об обнаружении уязвимостей используемого ПО и выпуске соответствующих исправлений Использование официальных источников обновлений.	Регулярное резервное копирование данных.
24.	Угроза перехвата управления информационной системой	Использование сертифицированного	Своевременная установка

		программного обеспечения и средств защиты информации. Мониторинг информации об обнаружении уязвимостей используемого ПО и выпуске соответствующих исправлений.	обновлений программного обеспечения, направленного на устранение выявленных уязвимостей ПО. Регулярное обновление вирусных дефиниций АВПО на серверах. Защита шифровальными (криптографическими) методами каналов передачи данных.
25.	Угроза воздействия на программы с высокими привилегиями	Инвентаризация и анализ установленного на серверах программного обеспечения на предмет наличия учетных записей «по умолчанию»	Блокирование встроенных учетных записей с администраторскими правами
26.	Угроза искажения вводимой и выводимой на периферийные устройства информации	Мониторинг состояния средств межсетевого экранирования и фильтрации сетевого трафика	Исключение средствами межсетевого экранирования доступа из внешних сетей к активному сетевому оборудованию, установка в настройках оборудования разрешения на администрирование устройств только с определенного пула адресов, принадлежащих внутренней сети организации

6. Заключение

Представленная в данном документе Модель угроз и нарушителей информационной безопасности ИС должна использоваться при реализации системы, в ходе ее внедрения и эксплуатации.

В соответствии порядком ввода и обработки информации, реализуемом в ИС, на протяжении опытной и промышленной эксплуатации в ИС будет обрабатываться и храниться информация, составляющая:

- Персональные данные, не отнесенные к специальным, биометрическим или общедоступным;
- Коммерческую тайну;
- Служебную информацию ограниченного распространения и ей организаций.

На протяжении опытной и постоянной эксплуатации в ИС не должна образовываться и содержаться информация:

- Подлежащая засекречиванию.
- Отнесенная к выполнению заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд (раскрывающая государственные заказы).

Для обеспечения конфиденциальности, целостности и доступности указанной информации необходимо принятие мер по обеспечению безопасности информации, предусмотренных законодательством РФ и нормативными документами.

В V главе приведены примеры с возможными способами их предотвращения или эскалации, для полной информации обо всех возможных угрозах для данной ИС следует посмотреть банк угроз.

ID	Нарушители	Категория нарушителя	Потенциал нарушителя
1	Неустановленные внешние субъекты (физические лица)	Внешний нарушитель	с низким потенциалом
2	Бывшие работники (пользователи)	Внешний нарушитель	с низким потенциалом
5	Пользователи информационной системы	Внутренний нарушитель	с низким потенциалом

6	Администраторы информационной системы и администраторы безопасности	Внутренний нарушитель	со средним потенциалом
9	Конкурирующие организации	Внешний нарушитель	со средним потенциалом

10	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний нарушитель	со средним потенциалом
----	---	--------------------	------------------------

Возможная мотивация	Предполагаемые возможности
<p>Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.</p>	<p>Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему.</p>
<p>Причинение имущественного ущерба путем мошенничества или иным преступным путем. Мсть за ранее совершенные действия.</p>	<p>Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему</p>
<p>Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Мсть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия.</p>	<p>Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования</p>

<p>Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.</p>	<p>Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования</p>
<p>Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием</p>	<p>Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы</p>

<p>Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.</p>	<p>Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны</p> <p>Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках</p> <p>Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему</p> <p>Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа.</p> <p>Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения.</p> <p>Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы</p> <p>Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)</p> <p>Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)</p>
---	---

Общая информац

Идентификатор УБИ	Наименование УБИ	Описание
3	Угроза использования слабостей криптографии	Угроза заключается в возможн
6	Угроза внедрения кода или данных	Угроза заключается в возможн
7	Угроза воздействия на программы с высокими	Угроза заключается в возможн
8	Угроза восстановления и/или повторного испо	Угроза заключается в возможн
12	Угроза деструктивного изменения конфигурац	Угроза заключается в возможн
14	Угроза длительного удержания вычислительн	Угроза заключается в возможн
15	Угроза доступа к защищаемым файлам с испо	Угроза заключается в возможн
16	Угроза доступа к локальным файлам сервера п	Угроза заключается в возможн
17	Угроза доступа/перехвата/изменения HTTP со	Угроза заключается в возможн
19	Угроза заражения DNS-кеша	Угроза заключается в возможн
20	Угроза злоупотребления возможностями, пред	Угроза заключается в возможн
21	Угроза злоупотребления доверием потребите	Угроза заключается в возможн
22	Угроза избыточного выделения оперативной п	Угроза заключается в возможн
23	Угроза изменения компонентов информацион	Угроза заключается в возможн
25	Угроза изменения системных и глобальных пе	Угроза заключается в возможн
26	Угроза искажения XML-схемы	Угроза заключается в возможн
27	Угроза искажения вводимой и выводимой на	Угроза заключается в возможн
28	Угроза использования альтернативных путей д	Угроза заключается в возможн
30	Угроза использования информации идентифи	Угроза заключается в возможн
31	Угроза использования механизмов авторизаци	Угроза заключается в возможн
33	Угроза использования слабостей кодирования	Угроза заключается в возможн
34	Угроза использования слабостей протоколов с	Угроза заключается в возможн
36	Угроза исследования механизмов работы про	Угроза заключается в возможн
37	Угроза исследования приложения через отчёт	Угроза заключается в возможн
40	Угроза конфликта юрисдикций различных стра	Угроза заключается в возможн
41	Угроза межсайтового скриптинга	Угроза заключается в возможн
42	Угроза межсайтовой подделки запроса	Угроза заключается в возможн
43	Угроза нарушения доступности облачного сер	Угроза заключается в возможн
49	Угроза нарушения целостности данных кеша	Угроза заключается в возможн
51	Угроза невозможности восстановления сессии	Угроза заключается в возможн
54	Угроза недобросовестного исполнения обязат	Угроза заключается в возможн
55	Угроза незащищённого администрирования о	Угроза заключается в возможн

56	Угроза некачественного переноса инфраструкт	Угроза заключается в возможн
61	Угроза некорректного задания структуры данн	Угроза заключается в возможн
62	Угроза некорректного использования прозрач	Угроза заключается в возможн
63	Угроза некорректного использования функций	Угроза заключается в возможн
64	Угроза некорректной реализации политики ли	Угроза заключается в возможн
65	Угроза неопределённости в распределении от	Угроза заключается в возможн
66	Угроза неопределённости ответственности за	Угроза заключается в возможн
67	Угроза неправомерного ознакомления с защи	Угроза заключается в возможн
68	Угроза неправомерного/некорректного испол	Угроза заключается в возможн
69	Угроза неправомерных действий в каналах свя	Угроза заключается в возможн
70	Угроза непрерывной модернизации облачной	Угроза заключается в возможн
71	Угроза несанкционированного восстановления	Угроза заключается в возможн
74	Угроза несанкционированного доступа к аутен	Угроза заключается в возможн
86	Угроза несанкционированного изменения ауте	Угроза заключается в возможн
88	Угроза несанкционированного копирования за	Угроза заключается в возможн
89	Угроза несанкционированного редактирования	Угроза заключается в возможн
90	Угроза несанкционированного создания учётн	Угроза заключается в возможн
91	Угроза несанкционированного удаления защи	Угроза заключается в возможн
93	Угроза несанкционированного управления бу	Угроза заключается в возможн
94	Угроза несанкционированного управления син	Угроза заключается в возможн
95	Угроза несанкционированного управления ука	Угроза заключается в возможн
96	Угроза несогласованности политик безопаснос	Угроза заключается в возможн
98	Угроза обнаружения открытых портов и иденти	Угроза заключается в возможн
99	Угроза обнаружения хостов	Угроза заключается в возможн
100	Угроза обхода некорректно настроенных меха	Угроза заключается в возможн
101	Угроза общедоступности облачной инфраструкт	Угроза заключается в возможн
102	Угроза опосредованного управления группой	Угроза заключается в возможн
103	Угроза определения типов объектов защиты	Угроза заключается в возможн
104	Угроза определения топологии вычислительн	Угроза заключается в возможн
109	Угроза перебора всех настроек и параметров п	Угроза заключается в возможн
111	Угроза передачи данных по скрытым каналам	Угроза заключается в возможн
113	Угроза перезагрузки аппаратных и программн	Угроза заключается в возможн
114	Угроза переполнения целочисленных перемен	Угроза заключается в возможн
115	Угроза перехвата вводимой и выводимой на п	Угроза заключается в возможн

116	Угроза перехвата данных, передаваемых по вы	Угроза заключается в возможн
117	Угроза перехвата привилегированного потока	Угроза заключается в возможн
118	Угроза перехвата привилегированного процес	Угроза заключается в возможн
121	Угроза повреждения системного реестра	Угроза заключается в возможн
122	Угроза повышения привилегий	Угроза заключается в возможн
124	Угроза подделки записей журнала регистрации	Угроза заключается в возможн
127	Угроза подмены действия пользователя путём	Угроза заключается в возможн
128	Угроза подмены доверенного пользователя	Угроза заключается в возможн
130	Угроза подмены содержимого сетевых ресурс	Угроза заключается в возможн
131	Угроза подмены субъекта сетевого доступа	Угроза заключается в возможн
132	Угроза получения предварительной информац	Угроза заключается в возможн
134	Угроза потери доверия к поставщику облачны	Угроза заключается в возможн
135	Угроза потери и утечки данных, обрабатываем	Угроза заключается в возможн
138	Угроза потери управления собственной инфра	Угроза заключается в возможн
139	Угроза преодоления физической защиты	Угроза заключается в возможн
140	Угроза приведения системы в состояние «отка	Угроза заключается в возможн
141	Угроза привязки к поставщику облачных услуг	Угроза заключается в возможн
142	Угроза приостановки оказания облачных услуг	Угроза заключается в возможн
143	Угроза программного выведения из строя сред	Угроза заключается в возможн
145	Угроза пропуска проверки целостности програ	Угроза заключается в возможн
149	Угроза сбоя обработки специальным образом	Угроза заключается в возможн
151	Угроза сканирования веб-сервисов, разработа	Угроза заключается в возможн
152	Угроза удаления аутентификационной информ	Угроза заключается в возможн
153	Угроза усиления воздействия на вычислительн	Угроза заключается в возможн
155	Угроза утраты вычислительных ресурсов	Угроза заключается в возможн
156	Угроза утраты носителей информации	Угроза заключается в возможн
157	Угроза физического выведения из строя средс	Угроза заключается в возможн
158	Угроза форматирования носителей информац	Угроза заключается в возможн
159	Угроза «форсированного веб-браузинга»	Угроза заключается в возможн
160	Угроза хищения средств хранения, обработки	Угроза заключается в возможн
162	Угроза эксплуатации цифровой подписи прогр	Угроза заключается в возможн
163	Угроза перехвата исключения/сигнала из прив	Угроза заключается в возможн
164	Угроза распространения состояния «отказ в об	Угроза заключается в возможн
165	Угроза включения в проект не достоверно исп	Угроза заключается в возможн

166	Угроза внедрения системной избыточности	Угроза заключается в возможн
168	Угроза «кражи» учётной записи доступа к сете	Угроза заключается в возможн
169	Угроза наличия механизмов разработчика	Угроза заключается в возможн
170	Угроза неправомерного шифрования информа	Угроза заключается в возможн
172	Угроза распространения «почтовых червей»	Угроза заключается в возможн
173	Угроза «спама» веб-сервера	Угроза заключается в возможн
174	Угроза «фарминга»	Угроза заключается в возможн
175	Угроза «фишинга»	Угроза заключается в возможн
177	Угроза неподтверждённого ввода данных опе	Угроза заключается в возможн
178	Угроза несанкционированного использования	Угроза заключается в возможн
179	Угроза несанкционированной модификации з	Угроза заключается в возможн
181	Угроза перехвата одноразовых паролей в реж	Угроза заключается в возможн
182	Угроза физического устаревания аппаратных к	Угроза заключается в возможн
185	Угроза несанкционированного изменения пар	Угроза заключается в возможн
187	Угроза несанкционированного воздействия на	Угроза заключается в возможн
188	Угроза подмены программного обеспечения	Угроза заключается в возможн
189	Угроза маскирования действий вредоносного	Угроза заключается в возможн
191	Угроза внедрения вредоносного кода в дистри	Угроза заключается в возможн
192	Угроза использования уязвимых версий прогр	Угроза заключается в возможн
193	Угроза утечки информации за счет применени	Угроза заключается в возможн

Угрозы	Объект воздействия	Последствия	
		Нарушение конфиденциальности	Нарушение целостности
Внешний нарушитель со средним потенциалом	Метаданные, системное программное обеспечение	1	1
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, приложения	1	1
Внешний нарушитель со средним потенциалом	Информационная система, виртуальная машина	1	1
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, микропроцессор	1	0
Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, приложения	1	1
Внешний нарушитель с низким потенциалом	Информационная система, сетевой узел, носитель информации	0	0
Внешний нарушитель с низким потенциалом	Объекты файловой системы	1	0
Внешний нарушитель со средним потенциалом	Сетевое программное обеспечение	1	0
Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение	1	0
Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	1	0
Внутренний нарушитель с низким потенциалом	Облачная система, виртуальная машина	1	1
Внешний нарушитель с низким потенциалом	Облачная система	1	1
Внешний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение	0	0
Внутренний нарушитель с низким потенциалом	Информационная система, сервер, рабочая станция	1	1
Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, приложения	1	1
Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение	0	1
Внешний нарушитель с высоким потенциалом	Системное программное обеспечение, приложения	0	1
Внешний нарушитель с низким потенциалом	Сетевой узел, объекты файловой системы, приложения	1	0
Внутренний нарушитель с низким потенциалом	Средства защиты информации, системное программное обеспечение	1	1
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, приложения	1	0
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, приложения	0	1
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое программное обеспечение	1	1
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, приложения	1	0
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, приложения	1	0
Внешний нарушитель с низким потенциалом	Облачная система	0	0
Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	1	1
Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение	1	1
Внешний нарушитель с низким потенциалом	Облачная система, облачный сервер	0	0
Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	0	1
Внутренний нарушитель с низким потенциалом	Рабочая станция, носитель информации, системное программное обеспечение	0	1
Внешний нарушитель с низким потенциалом	Информационная система, сервер, носитель информации	1	1
Внешний нарушитель с низким потенциалом	Облачная система, рабочая станция, сетевое программное обеспечение	1	1

Внешний нарушитель с низким потенциалом	Информационная система, иммигрированная в Интернет	1	1
Внутренний нарушитель со средним потенциалом	Сетевой трафик, база данных, сетевое программное обеспечение	0	1
Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	1	0
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, приложения	1	1
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, приложения	0	0
Внешний нарушитель с низким потенциалом	Системное программное обеспечение	1	1
Внешний нарушитель с низким потенциалом	Облачная система	1	1
Внутренний нарушитель с низким потенциалом	Аппаратное обеспечение, носители информации	1	0
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, приложения	1	1
Внешний нарушитель с низким потенциалом	Сетевой трафик	1	1
Внутренний нарушитель со средним потенциалом	Облачная инфраструктура	0	1
Внешний нарушитель с низким потенциалом	Машинный носитель информации	1	0
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, объекты файловой системы	1	0
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, объекты файловой системы	0	1
Внешний нарушитель с низким потенциалом	Объекты файловой системы, машинный носитель информации	1	0
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, использование Интернета	1	1
Внешний нарушитель с низким потенциалом	Системное программное обеспечение	1	1
Внешний нарушитель с низким потенциалом	Метаданные, объекты файловой системы, реестр	0	0
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, приложения	1	1
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, приложения	0	1
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, приложения	1	1
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, облачные сервисы	1	1
Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	1	0
Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	1	0
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, сетевые ресурсы	1	1
Внешний нарушитель со средним потенциалом	Объекты файловой системы, аппаратное обеспечение	1	1
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, приложения	0	1
Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	1	0
Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	1	0
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, приложения	0	1
Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение	1	0
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, аппаратное обеспечение	0	1
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, приложения	1	1
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, приложения	1	0

Внешний нарушитель с низким потенциалом	Сетевой узел, сетевой трафик	1	0
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное	1	1
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное	1	1
Внешний нарушитель с низким потенциалом	Объекты файловой системы, реестр	0	1
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, сетевое	1	1
Внешний нарушитель с низким потенциалом	Системное программное обеспечение	0	1
Внешний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое	1	1
Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	1	0
Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое	1	0
Внешний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое	1	1
Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение	1	0
Внутренний нарушитель со средним потенциалом	Объекты файловой системы, информационная система	1	1
Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, метаданные	1	1
Внутренний нарушитель со средним потенциалом	Информационная система, иммигрированная в сеть	1	1
Внешний нарушитель со средним потенциалом	Сервер, рабочая станция, носитель информации	1	1
Внешний нарушитель с низким потенциалом	Информационная система, сетевой узел, системное	0	0
Внутренний нарушитель с низким потенциалом	Информационная система, иммигрированная в сеть	0	0
	Системное программное обеспечение, аппаратное	0	0
Внешний нарушитель со средним потенциалом	Носитель информации, микропрограммное обеспечение	0	1
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное	0	1
Внешний нарушитель со средним потенциалом	Метаданные, объекты файловой системы, системное	1	1
Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение, сетевой узел	1	0
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, микропрограммное	1	1
Внешний нарушитель с низким потенциалом	Информационная система, сетевой узел, системное	0	0
Внешний нарушитель с низким потенциалом	Информационная система, сетевой узел, носитель информации	0	0
Внутренний нарушитель с низким потенциалом	Носитель информации	1	0
Внешний нарушитель с низким потенциалом	Сервер, рабочая станция, носитель информации	0	1
Внешний нарушитель с низким потенциалом	Носитель информации	0	1
Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	1	0
Внешний нарушитель с низким потенциалом	Сервер, рабочая станция, носитель информации	1	0
Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное	1	1
Внешний нарушитель со средним потенциалом	Системное программное обеспечение	1	1
Внешний нарушитель с низким потенциалом	Облачная инфраструктура, созданная с использованием	1	1
Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство	1	1

Внутренний нарушитель со средним потенциалом	Программное обеспечение, информационная система	0	0
Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	1	0
Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство	1	1
Внешний нарушитель с низким потенциалом	Объект файловой системы	0	0
Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	1	1
Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	0	0
Внешний нарушитель с низким потенциалом	Рабочая станция, сетевое программное обеспечение	1	0
Внешний нарушитель с низким потенциалом	Рабочая станция, сетевое программное обеспечение	1	0
Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое	0	1
Внешний нарушитель с низким потенциалом	Системное программное обеспечение	1	1
Внешний нарушитель с низким потенциалом	Объекты файловой системы	0	1
Внешний нарушитель со средним потенциалом	Сетевое программное обеспечение	0	1
Внутренний нарушитель с низким потенциалом	Аппаратное средство	0	0
Внешний нарушитель с низким потенциалом	Средство защиты информации	1	1
Внешний нарушитель со средним потенциалом	Средство защиты информации	1	1
Внутренний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое	1	1
Внешний нарушитель со средним потенциалом	Системное программное обеспечение, сетевое	0	1
Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое	1	1
Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое	1	1
Внешний нарушитель со средним потенциалом	Информационные ресурсы, объекты файловой	1	0

	Дополнительно	
нарушение доступности	включения угрозы в БНД	последнего изменения данных
0	20.03.2015	29.11.2020
1	20.03.2015	08.02.2019
0	20.03.2015	08.02.2019
0	20.03.2015	15.11.2019
1	20.03.2015	08.02.2019
1	20.03.2015	08.02.2019
0	20.03.2015	08.02.2019
0	20.03.2015	08.02.2019
1	20.03.2015	08.02.2019
0	20.03.2015	08.02.2019
1	20.03.2015	08.02.2019
0	20.03.2015	08.02.2019
1	20.03.2015	08.02.2019
1	20.03.2015	15.11.2019
1	20.03.2015	08.02.2019
1	20.03.2015	08.02.2019
0	20.03.2015	08.02.2019
0	20.03.2015	08.02.2019
1	20.03.2015	25.11.2020
0	20.03.2015	08.02.2019
1	20.03.2015	08.02.2019
1	20.03.2015	15.11.2019
1	20.03.2015	08.02.2019
0	20.03.2015	08.02.2019
1	20.03.2015	08.02.2019
1	20.03.2015	08.02.2019
1	20.03.2015	08.02.2019
1	20.03.2015	08.02.2019
1	20.03.2015	08.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019

1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
0	20.03.2015	21.05.2019
0	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019

0	20.03.2015	25.11.2020
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	12.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	12.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
0	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	20.03.2015	11.02.2019
1	31.03.2015	11.02.2019
1	31.03.2015	11.02.2019
1	25.05.2015	11.02.2019

1	25.05.2015	11.02.2019
1	25.05.2015	11.02.2019
1	25.05.2015	11.02.2019
1	25.05.2015	11.02.2019
1	25.05.2015	11.02.2019
1	25.05.2015	11.02.2019
0	25.05.2015	11.02.2019
0	25.05.2015	11.02.2019
1	18.08.2015	11.02.2019
1	18.08.2015	11.02.2019
0	18.08.2015	11.02.2019
0	18.08.2015	11.02.2019
1	18.08.2015	11.02.2019
1	23.06.2016	11.02.2019
1	21.10.2016	11.02.2019
1	21.10.2016	11.02.2019
1	21.10.2016	08.02.2019
1	21.10.2016	11.02.2020
1	21.10.2016	25.11.2020
0	01.12.2016	20.05.2020