

## СОДЕРЖАНИЕ

## ВВЕДЕНИЕ

Фотография - неотъемлемая составляющая процессов производства и потребления медиа контента. Данный формат контента является доминирующим в информационном пространстве. Он обладает рядом преимуществ перед другими видами представления информации: считывается раньше текста, может в качестве самостоятельного источника информации, а также дополнять другие виды представления информации, обладает более низким порогом вхождения для производства контента конкурентного качества и более широким распространением.

В данной сфере возрастаёт необходимость в качественных инструментах, позволяющих производителям контента сосредоточиться непосредственно на этапе производства, а не на организации производимого контента в хранилищах и на площадках, предназначенных для потребления контента.

Фотохостинг, как один из инструментов, участвующих в производстве контента — это сервис, позволяющий публиковать изображения в интернете с целью хранения и/или показа фотографий другим пользователям сети интернет.

Типичный порядок взаимодействия пользователя с фотохостингом:

- а) пользователь загружает готовую, или почти готовую фотографию в интернет-сервис;
- б) пользователь производит над фотографией операции по обработке, связанные с пред публикационным состоянием фотографии (такие, как обрезка, наложение фильтров, регулировка контраста);
- в) пользователь добавляет описание к фотографии при необходимости;
- г) пользователь вручную добавляет теги к фотографии, соответствующие классовой принадлежности фотографии;
- д) пользователь публикует фотографию в рамках фотохостинга, доступную к просмотру для всех пользователей сети интернет, а также к оцениванию и комментированию со стороны зарегистрированных и авторизованных пользователей фотохостинга;

- e) пользователь оценивает и комментирует фотографии других пользователей, загруженные на фотохостинг.

Цель работы – создание удобного инструмента для людей, так или иначе связанных с производством фотоконтента.

Главная задача программного обеспечения, так или иначе связанного с творчеством — уменьшить затраты пользователя на рутинные технические вещи, автоматизировать их, оставить только по-настоящему творческие задачи человеку. Поставлена задача разработать приложение, которое станет удобным инструментом для людей, связанных с производством фотоконтента в сети интернет. Приложение поможет пользователю организовать удобное хранение фотографий в автоматическом режиме, помечая фотографии тегами, исходя из содержимого фотографий, позволяя в дальнейшем осуществлять поиск фотографий по необходимым критериям, настраивать их приватность и публиковать в сети интернет при необходимости.

# 1 АНАЛИТИЧЕСКАЯ ЧАСТЬ

## 1.1 Постановка задачи

Конечная цель проектирования — разработка архитектуры программного решения, предназначенного для хранения и публикации фотографий в сети интернет.

Онлайн сервис для публикации фотографий должен обладать следующими характеристиками:

- возможность загрузки и хранения фотографий с возможностью просмотра и дальнейшего скачивания;
- организация хранилища фотографий пользователей в автоматическом или полуавтоматическом режиме с возможностью осуществления дальнейшего поиска по необходимым критериям;
- возможность публикации фотографий в сети интернет;
- индексирование загружаемых фотографий по цветам для осуществления возможности дальнейшего поиска фотографий по цветам;
- возможность комментирования и оценивания фотографий, загруженных в сервис;
- возможность обмена сообщениями с другими пользователями;
- автоматическая классификация фотографий по набору тегов;
- задание пользовательских тегов;
- поиск фотографии по кластерам цветов.

Для обеспечения безопасной и непрерывной работы пользователями программное решение должно отвечать следующим требованиям:

- Парольная аутентификация и разграничение прав доступа пользователей;
- Регистрация пользователей с подтверждением прохождения регистрации посредством email или смс;
- Протоколирование действий пользователей.

Для разработки фотохостинга необходима реализация следующих этапов:

- изучение и анализ предметной области;
- выбор технологий реализации;
- проектирование архитектуры приложения;
- обоснование выбора средств программной реализации;
- реализация продукта минимальной жизнедеятельности;
- запуск в эксплуатацию продукта минимальной жизнедеятельности;
- тестирование продукта минимальной жизнедеятельности на конечных пользователях;
- реализация продукта;
- запуск в эксплуатацию продукта.

## 1.2 Сравнительный анализ конкурирующих решений

На сегодняшний день существует большое количество решений, готовых предоставить услуги по хранению фотографий в сети. Данная услуга имеет массу плюсов для конечных пользователей, и самый главный - возможность представить фотографии в виде Web-альбома, созданного с помощью соответствующего решения, а не просто в виде бессистемного набора изображений. Но подобный вариант автоматически накладывает определенные сложности. Это относится к тому случаю, когда пользователь предназначает созданный фотоальбом не только для того, чтобы альбом просматривали, знающие его Web-адрес, но и для расширенного круга посетителей, например для выяснения мнения профессионалов по поводу качества изображений. В этом случае не избежать стандартной процедуры регистрации и раскрутки сайта, поскольку сделать сайт посещаемым — это отдельная и серьезная работа, которая потребует немало времени и специальных знаний. Каждый день появляются новые сервисы для хранения фотографий, сильно похожие на существующие аналоги. Сервисы соревнуются в типовых характеристиках, таких, как максимальное разрешение загружаемой фотографии, максимально возможное количество загруженных фотографий, тем самым они не предлагают пользователям нового

функционала, связанного с организацией хранилища фотографий. Сравнение ведущих решений для хранения фотографий представлены в таблице ??

Таблица 1.1 – Функциональность конкурирующих продуктов

Сравнение особенностей	Конкурент А фотохостинг	Конкурент В фотохостинг	Конкурент С фотохостинг	Конкурент D фотохостинг	Конкурент Е фотохостинг
URL компании	flickr.com	500px.com	photos.google.com	disk.yandex.ru	apple.com
Классификация продукта	Фотохостинг-соцсеть	Фотохостинг-соцсеть	Фотохостинг	Фотохостинг	Локальный фотохостинг
Варианты клиентов	Android, iOS, web	Android, iOS, web	Android, iOS, web	Android, iOS, web	OSX
Объем бесплатного хранилища	1 tb	7 фото в неделю	∞ if size <16Mp	10 gb	Локальное хранилище
Загрузка исходников фотографии	-	-	+	+	+
Теги	+	+	+	-	-
Настройки приватности для фотографии	+	-	+	+	-
Комментирование	+	+	-	-	-
Сохранение фотографий других людей	+	+	-	-	-
Скачивание оригинала фотографии	+	-	+	+	+
Авторасстановка тегов	-	-	+	-	-
Распознавание лиц	-	-	+	-	+
Распознавание разных людей	-	-	-	-	+
Чтение информации из exif	+	+	-	-	+
Суммарное количество особенностей на	15	11	9	5	7

### 1.3 Организация хранилища фотографий

Большинство фотографов хранят исходники или обработанные фотографии на локальных носителях. Данный способ хранения имеет ряд существенных недостатков, как например, ненадежность массово используемых решений и трудность организации фотографий стандартными средствами ОС. А инструменты, предоставляющие хранение фотографий в сети сильно ограничены. Одной из функций, улучшающих опыт использования от сервиса была бы возможность в автоматическом, или полуавтоматическом режиме организовывать хранилище фотографий, тем самым снимая данную нагрузку с пользователя. Это возможно благодаря индексации фотографий в сервисе сразу после их загрузки. Фотография классифицируется и помечается тегом принадлежности к набору классов. Также выделяются цветовые кластеры на фотографии для дальнейшей возможности поиска фотографии по набору преобладающих на ней цветов. Предполагается возможность формирования альбомов с фотографиями "на лету", после ввода пользователем общих критериев, объединяющих сразу несколько фотографий по проиндексированным при загрузке признакам.

В настоящий момент на рынке не так много решений по хранению фотографий, классифицирующих или категоризирующих изображения. Подобных решений по хранению фотографий непосредственно в сети еще меньше. Одними из немногих и самым популярным среди таковых является сервис Google Photo. В Google Photo можно бесплатно загружать фотографии, размер которых не превышает 16 МПикс в формате jpeg. Сразу после загрузки фотографии индексируются для дальнейшего поиска по ключевым словам. При этом результаты индексирования остаются полностью скрытыми от пользователя. В таком случае, если нейронная сеть ошиблась, пользователь никогда об этом не узнает, или по крайней мере, никак не сможет на это повлиять. Например, нейронная сеть может распознать класс там, где его на самом деле нет или не распознать класс там, где он присутствует.

## 2 ПРОЕКТИРОВАНИЕ

### 2.1 Применение нейронной сети для задачи классификации

Для задач классификации изображений наилучшие результаты показывает Convolutional Neural Network или сверточная нейронная сеть, которая является логическим развитием идей таких архитектур нейронных сетей как когнитрона и неокогнитрона. Успех обусловлен возможностью учета двумерной связности изображения, в отличие от многослойного персептрана [?].

Сверточные нейронные сети обеспечивают частичную устойчивость к изменениям масштаба, смещениям, поворотам, смене ракурса и прочим искажениям. Сверточные нейронные сети объединяют три архитектурных идеи, для обеспечения инвариантности к изменению масштаба, повороту сдвига и пространственным искажениям:

- локальные рецепторные поля (обеспечивают локальную двумерную связность нейронов);
- общие синаптические коэффициенты (обеспечивают детектирование некоторых черт в любом месте изображения и уменьшают общее число весовых коэффициентов);
- иерархическая организация с пространственными подвыборками.

На данный момент сверточная нейронная сеть и ее модификации считаются лучшими по точности и скорости алгоритмами нахождения объектов на сцене. Начиная с 2012 года, сверточные нейронные сети занимают первые места на известном международном конкурсе по распознаванию образов ImageNet.

Именно поэтому принято решение о дальнейшем использовании сверточных нейронных сетей. Наиболее интересными представителями класса сверточных нейронных сетей являются сети «GoogleNet», «InceptionV3» и «VGG16».

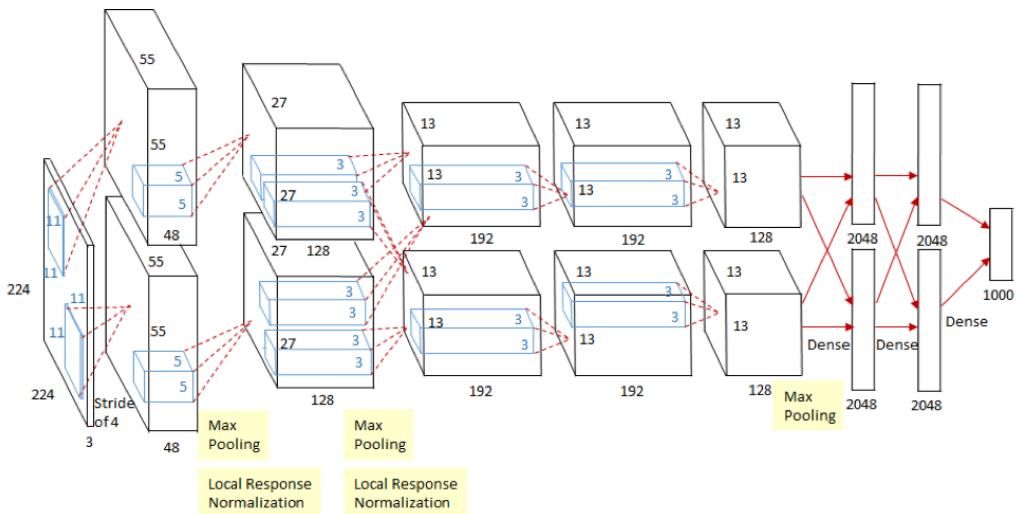


Рис. 2.1 – Структура нейронной сети AlexNet

VGG16 — модель сверточной нейронной сети, предложенная K. Simonyan и A. Zisserman из Оксфордского университета [?]. Модель достигает точности 92.7% — топ-5, при тестировании на подмножестве данных ILSVRC-2014 (ImageNet Large Scale Visual Recognition Challenge — Кампания по широкомасштабному распознаванию образов в ImageNet) множества ImageNet в задаче распознавания объектов на изображении.

Топ 5 — метрика, в которой алгоритм может выдать 5 вариантов класса картинки. Ошибка засчитывается, если среди всех этих вариантов нет правильного. В тестовом наборе данных 150 тысяч картинок и 1000 категорий, то есть задача крайне нетривиальна.

Это одна из самых известных моделей сверточной нейронной сети, которая была отправлена на соревнование ILSVRC-2014. Она является улучшенной версией нейронной сети AlexNet, которая была первой сверточной нейронной сетью, победившей в ILSVRC[?].

В VGG16 по сравнению с сетью AlexNet были заменены большие фильтры (размера 11 и 5 в первом и втором сверточном слое, соответственно) на несколько фильтров размера 3x3, следующих один за другим. Сеть VGG16 для конкурса обучалась на протяжении нескольких недель при использовании видеокарт NVIDIA TITAN BLACK.

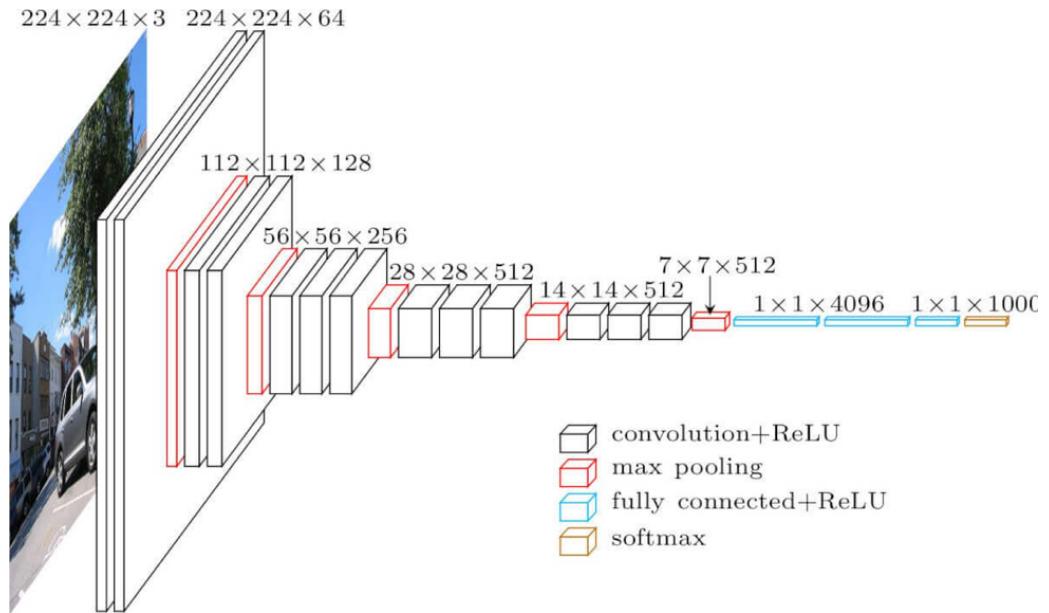


Рис. 2.2 – Структура нейронной сети VGG16

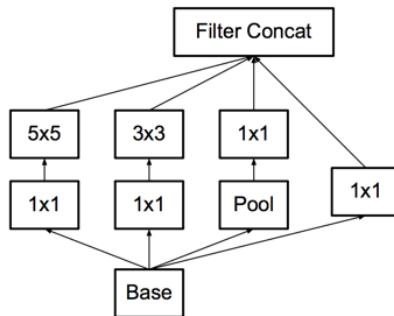


Рис. 2.3 – Структура блока inception сети GoogLeNet

GoogLeNet – сверточная нейронная сеть, спроектированная компанией Google и выигравшая ILSVRC-2014 с результатом точности 93,33% топ 5 [?]. Сеть AlexNet, победившая в 2012 году не помещалась в память одного графического ускорителя, объем памяти которого составлял 3GB. Одной из главных идей GoogLeNet была эффективность вычислений при небольшом размере модели и небольшом количестве самих вычислений, например, чтобы можно было использовать нейронную сеть на носимых устройствах.

При проектировании сети GoogLeNet также учитывались недостатки нейронной сети AlexNet.

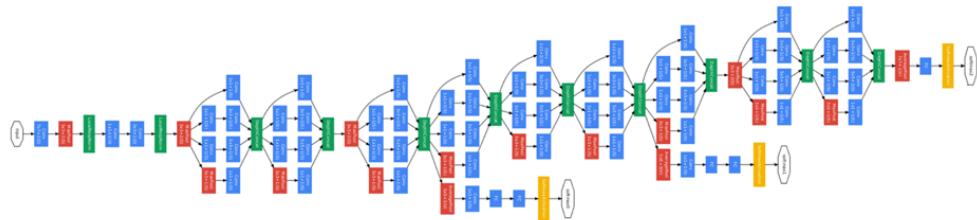


Рис. 2.4 – Структура нейронной сети GoogLeNet

В структуре AlexNet производились большие свертки, которые требуют много параметров, в GoogLeNet свертки стали меньше, однако увеличилось количество слоев в свертках.

После чего было произведено сильное уменьшение количества измерений, чтобы компенсировать более толстые слои. Данная операция производилась с помощью слоя, выполняющего роль линейного фильтра, примененного по всему изображению, чтобы линейно смешать текущее количество измерений в меньшее.

На каждом из уровней использовалось одновременно несколько подобных фильтров разного размера. Это делалось для того, чтобы улавливать градиентные участки изображения разного масштаба.

В GoogLeNet отсутствуют полно связные слои, так как в них слишком много параметров. Вместо этого на последнем уровне выполняется операция субдескрайтизации, после которой информация подается непосредственно на выходной слой.

Данные манипуляции позволили примерно в 10 раз сократить количество параметров нейронной сети по сравнению в AlexNet, как следствие и количество вычислений, производимых при обучении и непосредственной работе нейронной сети.

InceptionV3 – дальнейшее развитие идеи эффективных сверточных нейронных сетей от Google. Данная нейронная сеть достигает точности 92,8% топ 5 на ILSVRC-2015 [?].

При проектировании InceptionV3, в отличие от первой версии, были сформулированы основные принципы построения архитектуры:

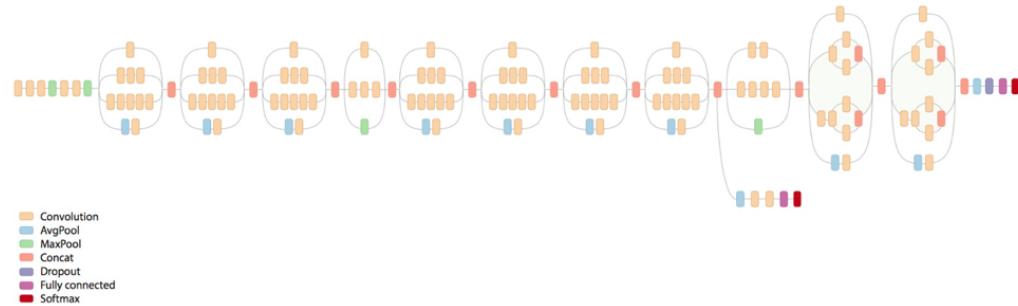


Рис. 2.5 – Структура нейронной сети InceptionV3

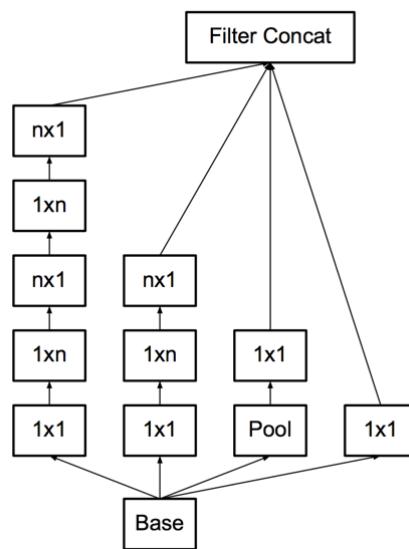


Рис. 2.6 – Структура блока inception нейронной сети InceptionV3

- Большое количество сигналов расположены в непосредственной близости друг от друга. Это можно использовать, чтобы делать свертки меньшего размера. Соседние сигналы часто коррелируют, следовательно, можно уменьшить размерность перед сверткой без потери информации.
- При увеличении свободного количества ресурсов для их эффективного использования, необходимо увеличивать и глубину и ширину сети одновременно.
- Неэффективно использовать слои, резко уменьшающие количество параметров, особенно в начале нейронной сети.
- «Широкие» слои быстрее обучаются, что особенно важно на высоких уровнях (но локально, т.е. можно после них уменьшать размерность)

В качестве структуры нейронной сети для дальнейшей работы выбрана InceptionV3, так как она показывает наилучшие результаты по сравнению с другими вышенназванными сверточными нейронными сетями, а также имеет один из лучших показателей эффективности.

## 2.2 Выделение цветовых кластеров на изображении

Для выделения цветовых кластеров на фотографии, при их загрузке на фотохостинг, пиксели на фотографии необходимо кластеризовать. Так, как заранее не известно количество цветовых кластеров на фотографии, необходимо использовать адаптивный алгоритм, определяющий количество кластеров в процессе работы, также устойчивый к выбросам. Таким алгоритмом является DBSCAN (Основанная на плотности пространственная кластеризация для приложений с шумами) [?].

Алгоритм DBSCAN может быть разложен на следующие шаги:

- а) найти точки в  $\epsilon$ -окрестности каждой точки и выделить основные точки с более чем  $minPts$  соседями;
- б) найти связные компоненты основных точек на графике соседей, игнорируя все неосновные точки;
- в) назначить каждую неосновную ближайшему кластеру, если кластер является  $\epsilon$ -соседним, в противном случае считать точку шумом.

Хорошой практикой является выбор значения  $minPts$  равному размерности данных, увеличенной на единицу. Величину  $\epsilon$  можно выбрать из графа  $k$ -расстояний[?]:

- а) вычислить средние расстояния по  $minPts$  ближайшим соседям для каждой точки;
- б) отсортировать полученные значения;
- в) выбрать  $\epsilon$  в точке колена получившегося графика.

Так, как данный алгоритм в результате работы не находит центр кластера, необходимо вычислить геометрическую медиану полученных кластеров. Выполнить данную операцию можно почти за линейное время, используя

алгоритм Коэна, Ли, Миллера и Пачоки [?]. В результате работы алгоритма получаем данные о цветовых характеристиках изображения.

### 2.3 Функциональные требования

Программа должна обеспечивать возможность выполнения перечисленных ниже функций:

- Загрузка и хранение фотографий с возможностью просмотра и дальнейшего скачивания;
- Разграничение прав доступа, регистрация пользователей с подтверждением прохождения регистрации посредством email или смс, авторизация пользователей;
- Организация хранилища фотографий пользователей в автоматическом или полуавтоматическом режиме с возможностью осуществления дальнейшего поиска по необходимым критериям;
- Возможность публикации фотографий в сети интернет;
- Возможность комментирования и оценивания фотографий, загруженных в сервис;
- Индексирование загружаемых фотографий по цветам для осуществления возможности дальнейшего поиска фотографий по цветам;
- Классификация фотографий с использованием нейронных сетей и индексирование результатов с целью возможности дальнейшего поиска фотографий по данному критерию;

### 2.4 Общее описание

### 2.5 Варианты использования

Перечень вариантов использования системы приведена в таблице ???. Диаграмма вариантов использования на рисунке ?? показывает варианты использования системы и связанные с ними действующие лица.

Таблица 2.1 – Варианты использования системы хранения фотографий

Основное действующее лицо	Вариант использования
Посетитель	<ol style="list-style-type: none"> <li>1. Пройти регистрацию</li> <li>2. Просмотреть ленту популярных фотографий</li> <li>3. Просмотреть фотографии пользователя</li> <li>4. Просмотреть информацию о фотографии</li> <li>5. Осуществить поиск фотографии по необходимым критериям</li> <li>6. Авторизоваться</li> </ol>
Пользователь	<ol style="list-style-type: none"> <li>1. Привязать популярные соц сети</li> <li>2. Создать пост в соц сетях</li> <li>3. Настроить приватность фотографии</li> <li>4. Настроить защиту от копирования</li> <li>5. Оценить фотографию</li> <li>6. Прокомментировать фотографию</li> <li>7. Просмотреть статистику</li> <li>8. Сохранить в избранное</li> <li>9. Подписаться на публикации других пользователей</li> <li>10. Опубликовать фотографию</li> </ol>

Таблица 2.2 – Вариант использования - 1 – Пройти регистрацию

№ варианта использования:	Вариант использования - 1
Название варианта использования:	Пройти регистрацию
Действующие лица:	Посетитель
Описание:	Посетитель заполняет форму со своими данными для последующей авторизации и подтверждает регистрацию
Предварительные условия:	Нет
Выходные условия:	Нет
Нормальное направление:	<p>1.0 Пройти регистрацию</p> <p>1. Пользователь заполняет форму с данными, основными являются логин, пароль и email или номер телефона</p> <p>2. Нажимает кнопку регистрации на форме</p> <p>3. Система создает в БД запись о пользователе и генерирует токен для подтверждения учетной записи. Токен отправляется посредством email или смс</p> <p>4. Пользователь получает токен для подтверждения прохождения регистрации</p> <p>5. Подтверждает регистрацию на сайте</p> <p>6. Система отмечает, что пользователь успешно зарегистрирован и авторизовывает его. Посетитель становится пользователем.</p>
Альтернативные направления:	

Таблица 2.3 – Вариант использования - 2 – Просмотреть ленту популярных фотографий

<b>№ варианта использования:</b>	<b>Вариант использования - 2</b>
Название варианта использования:	Просмотреть ленту популярных фотографий
Действующие лица:	Посетитель
Описание:	Посетитель открывает веб страницу, на которой содержатся все популярные фотографии за определенный промежуток времени
Предварительные условия:	В сервисе загружены фотографии, доступ к которым разрешен всем
Выходные условия:	Нет
Нормальное направление:	<p>2.0 Просмотреть ленту популярных фотографий</p> <p>1. Посетитель открывает страницу с популярными фотографиями</p> <p>2. Сервис формирует список популярных фотографий, доступных всем, за определенный промежуток времени и отправляет посетителю</p> <p>3. Посетитель путем скроллинга веб страницы осуществляет просмотр популярных фотографий</p>
Альтернативные направления:	
Исключения:	<p>2.0.И.1 Отсутствуют фотографии, доступные всем</p> <p>1. Сообщение об ошибке на странице просмотра фотографий</p>
Включает:	
Приоритет:	Низкий
Особые требования:	

Таблица 2.4 – Вариант использования - 3 – Просмотреть ленту популярных фотографий

№ варианта использования:	Вариант использования - 3
Название варианта использования:	Просмотреть фотографии пользователя
Действующие лица:	Посетитель
Описание:	Посетитель просматривает фотографии пользователя, доступные всем
Предварительные условия:	Пользователь, фотографии которого пытается просмотреть посетитель, существует и загрузил хотя бы одну фотографию, доступную для просмотра всем
Выходные условия:	Нет
Нормальное направление:	3.0 Просмотреть фотографии пользователя 1. Посетитель открывает страницу в профиле пользователя с фотографиями 2. Сервис формирует список фотографий пользователя, доступный всем 3. Посетитель путем скроллинга веб страницы осуществляет просмотр фотографий
Альтернативные направления:	

Таблица 2.5 – Вариант использования - 4 - Просмотреть информацию о фотографии

<b>№ варианта использования:</b>	<b>Вариант использования - 4</b>
Название варианта использования:	Просмотреть информацию о фотографии
Действующие лица:	Посетитель
Описание:	Посетитель просматривает информацию о фотографии, такую как метаданные фотографии, теги, количество пользователей, которым понравилась фотография и т.п.
Предварительные условия:	Фотография, информацию о которой пытается просмотреть посетитель, существует и доступна для просмотра всем
Выходные условия:	Нет
Нормальное направление:	4.0 Просмотреть информацию о фотографии 1. Посетитель открывает страницу с фотографией 2. Система находит фотографию и всю информацию о ней 3. Посетитель просматривает доступную информацию о фотографии
Альтернативные направления:	

Таблица 2.6 – Вариант использования - 5 – Осуществить поиск фотографии по необходимым критериям

№ варианта использования:	Вариант использования - 5
Название варианта использования:	Осуществить поиск фотографии по необходимым критериям
Действующие лица:	Посетитель
Описание:	Посетитель осуществляет поиск фотографий с необходимыми ему критериями, такими, как цвет на фотографии, содержимое фотографии и т.д.
Предварительные условия:	Хотя бы одна фотография загружена в сервис и проиндексирована для поиска
Выходные условия:	Нет
Нормальное направление:	<p>5.0 Осуществить поиск фотографии по необходимым критериям</p> <p>1. Посетитель открывает страницу поиска фотографий</p> <p>2. Вводит необходимые ему критерии</p> <p>3. Система формирует список фотографий</p> <p>4. Посетитель путем скроллинга веб страницы просматривает список найденных фотографий</p>
Альтернативные направления:	
Исключения:	<p>5.0.И.1 Фотографии с заданными критериями поиска не найдены</p> <p>1. Сообщение об ошибке на странице поиска фотографий</p>
Включает:	
Приоритет:	Высокий
Особые требования:	

Таблица 2.7 – Вариант использования - 6 – Авторизоваться

№ варианта использования:	Вариант использования - 6
Название варианта использо- вания:	Авторизоваться
Действующие лица:	Посетитель
Описание:	Посетитель вводит логин и пароль от принад- лежащей ему учетной записи пользователя и авторизовывается
Предварительные условия:	Пользователь, данные которого вводятся, заре- гистрирован в системе
Выходные условия:	Нет
Нормальное направление:	<p>6.0 Авторизоваться</p> <p>1. Посетитель открывает страницу авториза- ции</p> <p>2. Вводит логин и пароль</p> <p>3. При включенной у учетной записи пользова- теля двухфакторинговой авторизации вводит дополнительные данные для входа</p> <p>4. Система. Авторизует пользователя и перена- правляет на главную страницу</p>
Альтернативные направле- ния:	
Исключения:	
Включает:	
Приоритет:	Высокий
Особые требования:	

Таблица 2.8 – Вариант использования - 7 - Привязать популярные соц сети

№ варианта использования:	Вариант использования - 7
Название варианта использования:	Привязать популярные соц сети
Действующие лица:	Пользователь
Описание:	Пользователь привязывает аккаунт соц сети с целью дальнейшего создания постов и публикации фотографий в соц сети
Предварительные условия:	Пользователь авторизован
Выходные условия:	Нет
Нормальное направление:	<p>7.0 Привязать популярные соц сети</p> <p>1. Пользователь открывает страницу своего профиля</p> <p>2. Выбирает необходимую ему социальную сеть из списка предложенных</p> <p>3. Система перенаправляет пользователя на страницу социальной сети для авторизации</p> <p>4. Пользователь авторизуется в соц сети</p> <p>5. Соц сеть перенаправляет пользователя обратно в систему</p> <p>6. Система привязывает переданный соц сетью токен к пользователю</p>
Альтернативные направления:	
Исключения:	
Включает:	
Приоритет:	Низкий
Особые требования:	

Таблица 2.9 – Вариант использования - 8 – Создать пост в соц сетях

№ варианта использования:	Вариант использования - 8
Название варианта использования:	Создать пост в соц сетях
Действующие лица:	Пользователь
Описание:	Пользователь при создании поста отмечает о необходимости его публикации в социальных сетях. Пост автоматически публикуется во всех отмеченных соц сетях
Предварительные условия:	Пользователь авторизован и хотя бы один аккаунт социальной сети привязан к аккаунту пользователя
Выходные условия:	Нет
Нормальное направление:	<p>8.0 Создать пост в соц сетях</p> <p>1. Пользователь переходит на страницу создания поста</p> <p>2. Формирует пост для дальнейшей публикации</p> <p>3. Публикует внутри сервиса и при публикации отмечает о необходимости публикации в аккаунте социальной сети</p>
Альтернативные направления:	
Исключения:	
Включает:	
Приоритет:	Низкий
Особые требования:	

Таблица 2.10 – Вариант использования - 9 – Настроить приватность фотографии

№ варианта использования:	Вариант использования - 9
Название варианта использования:	Настроить приватность фотографии
Действующие лица:	Пользователь
Описание:	Пользователь настраивает доступ к фотографии определенному кругу лиц
Предварительные условия:	Пользователь авторизован и загрузил фотографию, доступ к которой хочет настроить
Выходные условия:	Нет
Нормальное направление:	<p>9.0 Настроить приватность фотографии</p> <p>1. Пользователь открывает страницу настроек фотографии</p> <p>2. Переходит к форме настройки листов доступа</p> <p>3. Выбирает тип доступа и настраивает листы доступа</p>
Альтернативные направления:	
Исключения:	
Включает:	
Приоритет:	Низкий
Особые требования:	

Таблица 2.11 – Вариант использования - 10 – Оценить фотографию

№ варианта использования:	Вариант использования - 10
Название варианта использования:	Оценить фотографию
Действующие лица:	Пользователь
Описание:	Пользователь оценивает понравившуюся ему фотографию
Предварительные условия:	Пользователь авторизован и имеет доступ к фотографии, которую хочет оценить
Выходные условия:	Нет
Нормальное направление:	10.0 Оценить фотографию 1. Пользователь открывает страницу фотографии 2. Нажимает кнопку оценки фотографии
Альтернативные направления:	
Исключения:	
Включает:	
Приоритет:	Низкий
Особые требования:	

Таблица 2.12 – Вариант использования - 11 – Прокомментировать фотографию

№ варианта использования:	Вариант использования - 11
Название варианта использования:	Прокомментировать фотографию
Действующие лица:	Пользователь
Описание:	Пользователь оставляет комментарий к фотографии или в ответ на другой комментарий
Предварительные условия:	Пользователь авторизован и имеет доступ к фотографии, к которой хочет оставить комментарий
Выходные условия:	Нет
Нормальное направление:	<p>11.0 Прокомментировать фотографию</p> <p>1. Пользователь открывает страницу фотографии</p> <p>2. Вводит комментарий в форму ввода под фотографией или необходимым комментарием и нажимает кнопку «отправить»</p>
Альтернативные направления:	
Исключения:	
Включает:	
Приоритет:	Низкий
Особые требования:	

Таблица 2.13 – Вариант использования - 12 – Просмотреть статистику

№ варианта использования:	Вариант использования - 12
Название варианта использо- вания:	Просмотреть статистику
Действующие лица:	Пользователь
Описание:	Пользователь просматривает глобальную статистику фотографий по сервису или статистику по одной из своих фотографий
Предварительные условия:	Пользователь авторизован
Выходные условия:	Нет
Нормальное направление:	<p>12.0 Просмотреть статистику</p> <p>1. Пользователь открывает страницу с глобальной статистикой</p> <p>2. Просматривает глобальную статистику фотографий по сервису</p>
Альтернативные направле- ния:	
Исключения:	
Включает:	
Приоритет:	Низкий
Особые требования:	

Таблица 2.14 – Вариант использования - 13 – Сохранить в избранное

№ варианта использования:	Вариант использования - 13
Название варианта использо- вания:	Сохранить в избранное
Действующие лица:	Пользователь
Описание:	Пользователь сохраняет понравившуюся фо- тографию в избранное внутри сервиса
Предварительные условия:	Пользователь авторизован и имеет доступ к фотографии, которую хочет сохранить в из- бранное
Выходные условия:	Нет
Нормальное направление:	13.0 Сохранить в избранное  1. Пользователь нажимает на кнопку «сохра- нить в избранное» рядом с понравившейся фо- тографией
Альтернативные направле- ния:	
Исключения:	
Включает:	
Приоритет:	Низкий
Особые требования:	

Таблица 2.15 – Вариант использования - 14 – Подписаться на публикации других пользователей

№ варианта использования:	Вариант использования - 14
Название варианта использования:	Подписаться на публикации других пользователей
Действующие лица:	Пользователь
Описание:	Пользователь добавляет в свою персональную ленту интересных публикаций и фотографий все фотографии и посты другого пользователя
Предварительные условия:	Пользователь авторизован
Выходные условия:	Нет
Нормальное направление:	<p>14.0 Подписаться на публикации других пользователей</p> <p>1. Пользователь переходит на страницу пользователя, на публикации которого он хочет подписаться</p> <p>2. Нажимает кнопку «подписаться»</p>
Альтернативные направления:	
Исключения:	
Включает:	
Приоритет:	Низкий
Особые требования:	

Таблица 2.16 – Вариант использования - 15 – Опубликовать фотографию

№ варианта использования:	Вариант использования - 15
Название варианта использо- вания:	Опубликовать фотографию
Действующие лица:	Пользователь
Описание:	Пользователь загружает фотографию в сервис
Предварительные условия:	Пользователь авторизован
Выходные условия:	Нет
Нормальное направление:	<p>15.0 Опубликовать фотографию</p> <p>1. Пользователь переходит на страницу загрузки фотографии</p> <p>2. Добавляет новую фотографию</p> <p>3. Настраивает доступ к фотографии и выставляет теги к фотографии из списка предложенных и/или самостоятельно</p>
Альтернативные направле- ния:	
Исключения:	
Включает:	
Приоритет:	Низкий
Особые требования:	



Рис. 2.7 – Диаграмма вариантов использования программного решения для хранения фотографий

## 2.6 Структура базы данных

На рисунке ?? представлена модель базы данных программного решения.

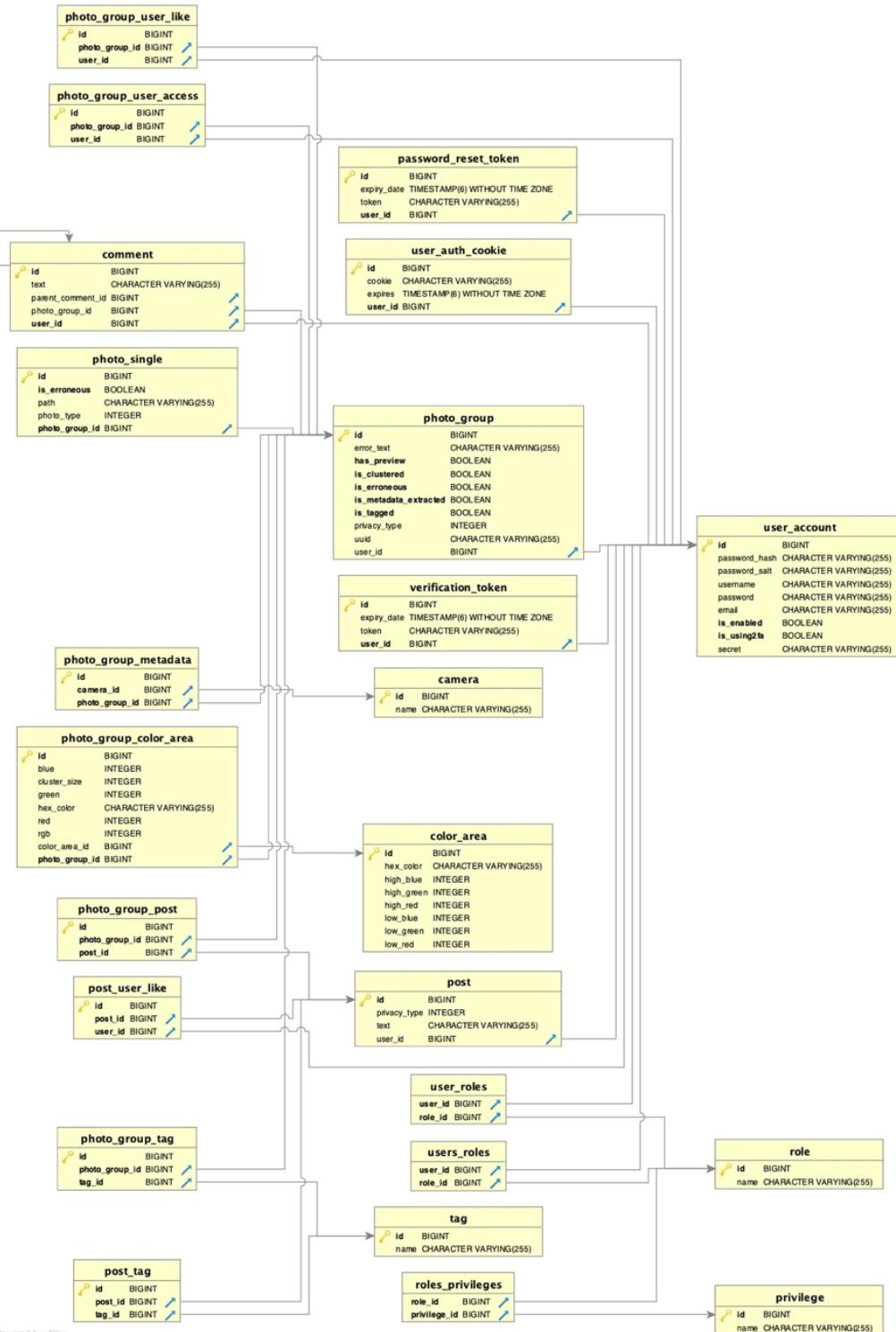


Рис. 2.8 – Модель базы данных программного решения для хранения фотографий

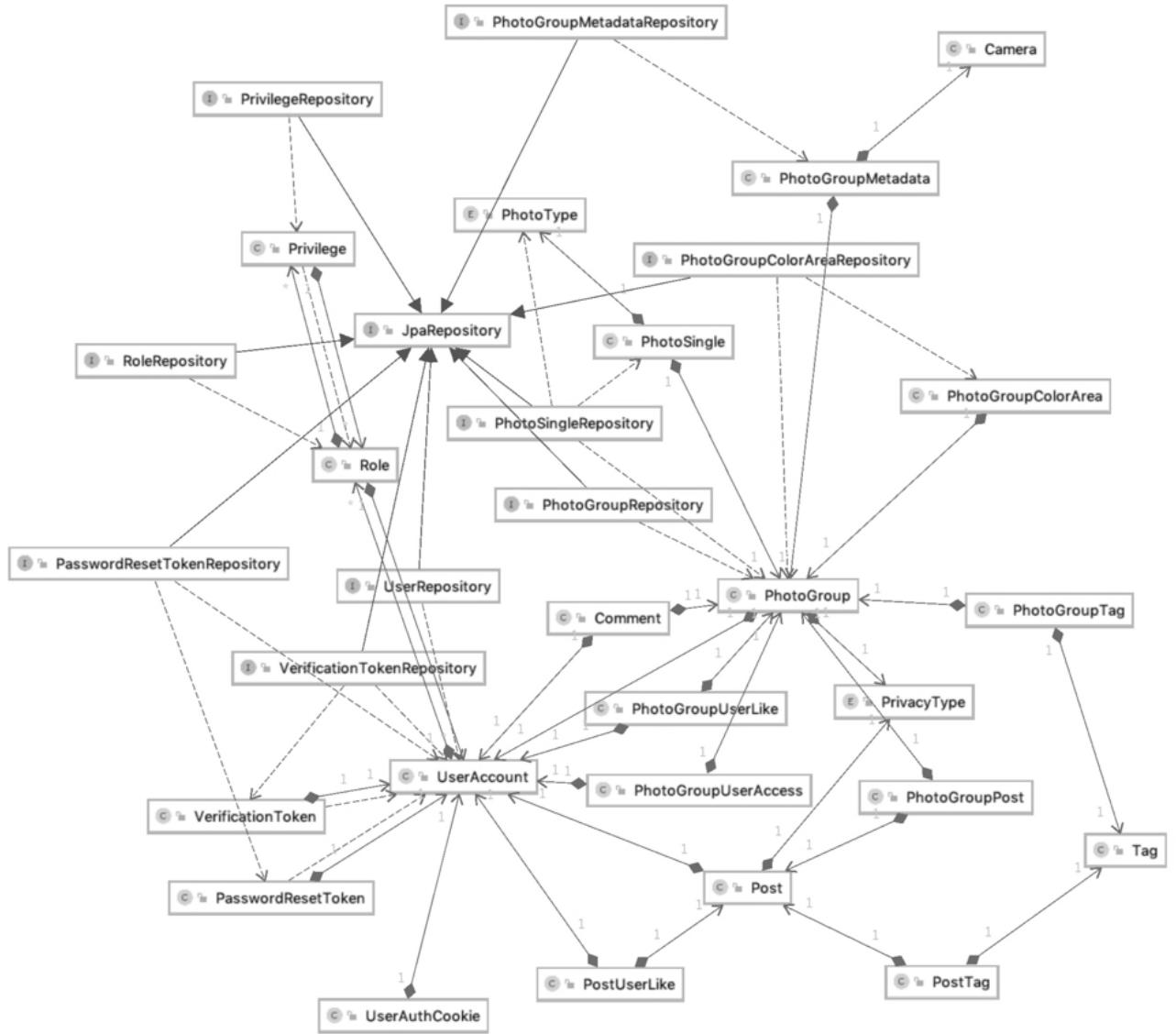


Рис. 2.9 – Диаграмма классов сущностей и репозиториев программного решения для хранения фотографий

## 2.7 Диаграмма классов

На рисунках ?? и ?? представлены диаграммы классов программного решения.

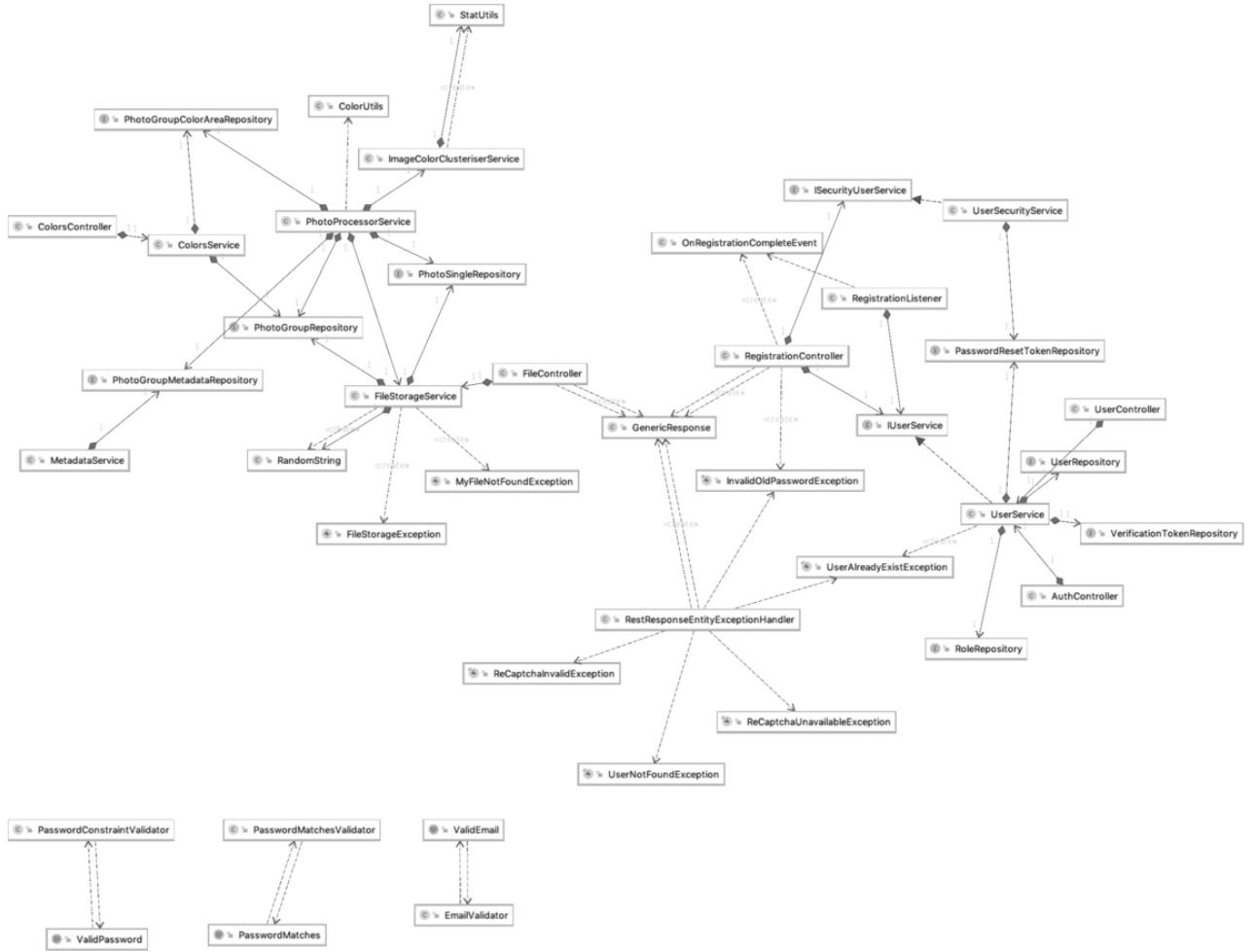


Рис. 2.10 – Диаграмма классов контроллеров программного решения для хранения фотографий

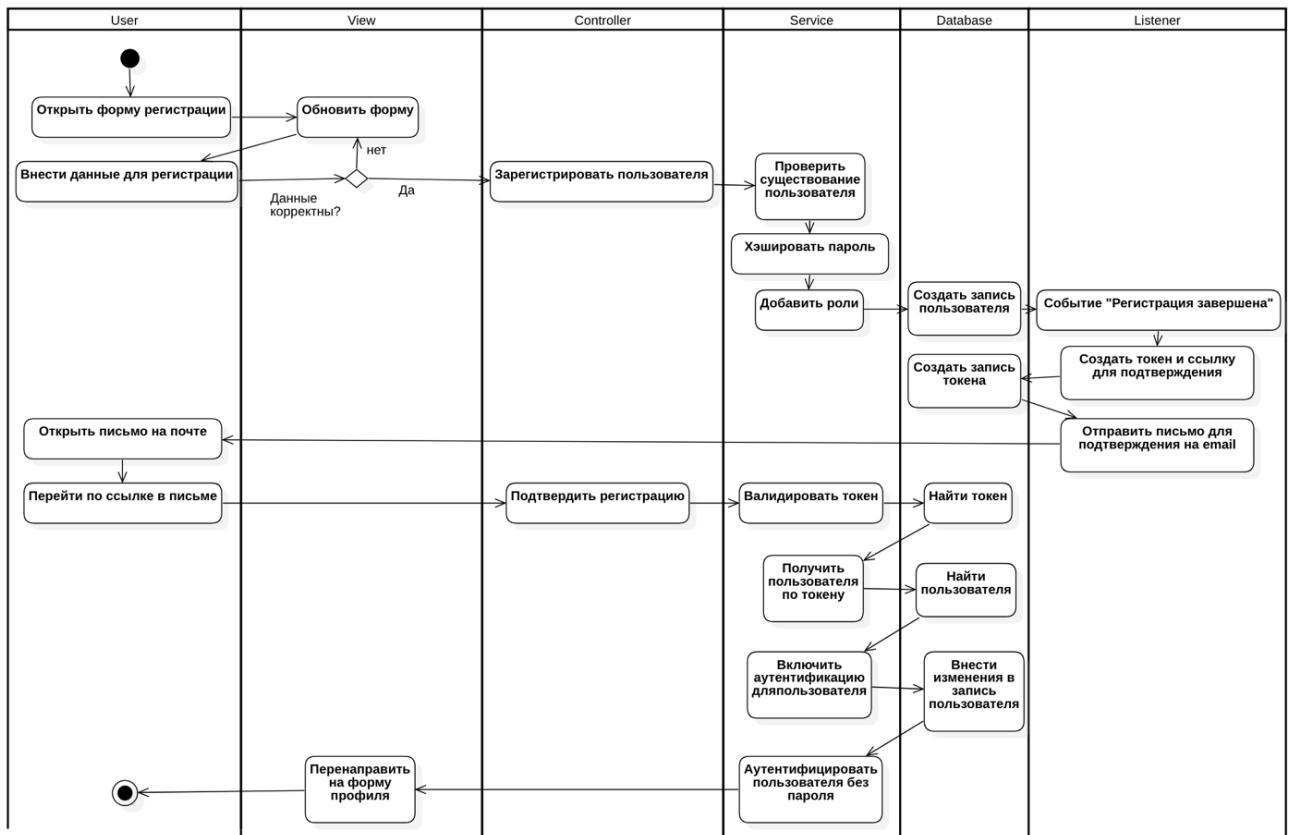


Рис. 2.11 – Диаграмма активностей процесса регистрации пользователя

## 2.8 Диаграмма активностей

На рисунке ?? представлена диаграмма активностей процесса регистрации пользователя.

### 3 ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ПРОГРАММНОЙ РЕАЛИЗАЦИИ

В рамках работы было принято разработать продукт минимальной жизнедеятельности по подготовленному проекту. Учитывая возможности имеющегося оборудования и программного обеспечения, необходимо создать работоспособный прототип программного продукта, избегая таких недостатков, как высокая стоимость и длительные этапы внедрения. Необходимо особое внимание уделить серверной части приложения, так как именно ее функционал отличает реализуемый программный продукт от аналогичной продукции, функционирующей на рынке.

#### 3.1 PostgreSQL

Для разработки базы данных для продукта была выбрана свободная к распространению система управления базами данных с открытым исходным кодом - PostgreSQL[?]. PostgreSQL - реляционная СУБД, это значит, что данные в ней хранятся в виде логически связанных между собой таблиц, представляющих в общем случае модель предметной области.

Работать с PostgreSQL можно не только с помощью интерфейса командной строки, но и с помощью графического интерфейса инструмента, поставляемого в комплекте - pgAdmin. Это позволяет упростить и ускорить работу с базами данных в PostgreSQL.

PgAdmin работает через интерфейс браузера, а значит обладает независимостью от аппаратной составляющей. Многие из базовых и наиболее часто используемых SQL-операций в PgAdmin сведены к интуитивно понятному кнопочному интерфейсу.

#### 3.2 Java

В качестве языка программирования для программного продукта был выбран язык программирования Java[?], так как он отличается быстротой, высоким уровнем защиты и надежностью. Java - сильно типизированный объектно-ориентированный язык программирования, что позволяет проще производить отладку программного кода, а также легче формализовывать объекты предметной области в виде программного кода.

Программы на Java транслируются в байт-код Java, выполняемый виртуальной машиной Java (JVM) — программой, обрабатывающей байтовый код и передающей инструкции оборудованию как интерпретатор.

Достоинством подобного способа выполнения программ является полная независимость байт-кода от операционной системы и оборудования, что позволяет выполнять Java-приложения на любом устройстве, для которого существует соответствующая виртуальная машина. Другой важной особенностью технологии Java является гибкая система безопасности, в рамках которой исполнение программы полностью контролируется виртуальной машиной. Любые операции, которые превышают установленные полномочия программы (например, попытка несанкционированного доступа к данным или соединения с другим компьютером), вызывают немедленное прерывание.

### 3.3 Spring Framework

В качестве основного фреймворка для разработки был выбран Spring Framework[?], так как он универсален и предоставляет широкий функционал для разработки как масштабных корпоративных, так и небольших десктопных приложений. Spring Framework - универсальный фреймворк с открытым исходным кодом для Java-платформы. Несмотря на то, что Spring не обеспечивает какую-либо конкретную модель программирования, он широко распространён в Java-сообществе главным образом как альтернатива и замена стандартной модели построения корпоративных приложений, являющейся частью Java. Spring предоставляет боольшую свободу Java-разработчикам в проектировании; кроме того, он предоставляет хорошо документированные и лёгкие в использо-

вании средства решения проблем, возникающих при создании приложений корпоративного масштаба.

Особенности ядра Spring применимы в любом Java-приложении, и существует множество расширений и усовершенствований для построения веб-приложений на Java Enterprise платформе.

### 3.4 Deeplearning4j

В качестве вспомогательной библиотеки для интеграции нейронной сети в программное средство была выбрана библиотека Deeplearning4j[?]. Deeplearning4j - библиотека с открытым исходным кодом, написанная для языков Java и Scala, предоставляющая широкий функционал для обучения нейронных сетей и их последующей интеграции в Java приложение. Библиотека имеет полную документацию, множество примеров и обширное сообщество, включает реализацию ограниченной машины Больцмана, глубокой сети доверия, глубокого автокодировщика, стекового автокодировщика с фильтрацией шума, рекурсивной тензорной нейронной сети.

## 4 ОПИСАНИЕ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

В разделе описания виртуальной инфраструктуры представлена общая схема инфраструктуры, схемы мониторинга, репликации и балансировки DNS, используемые технологии виртуализации, алгоритмы взаимодействия пользователя и компонентов инфраструктуры.

### 4.1 Общая схема инфраструктуры

Общая схема инфраструктуры представлена на рис. ?? и чертеже СевГУ 09.03.01.15.A1.

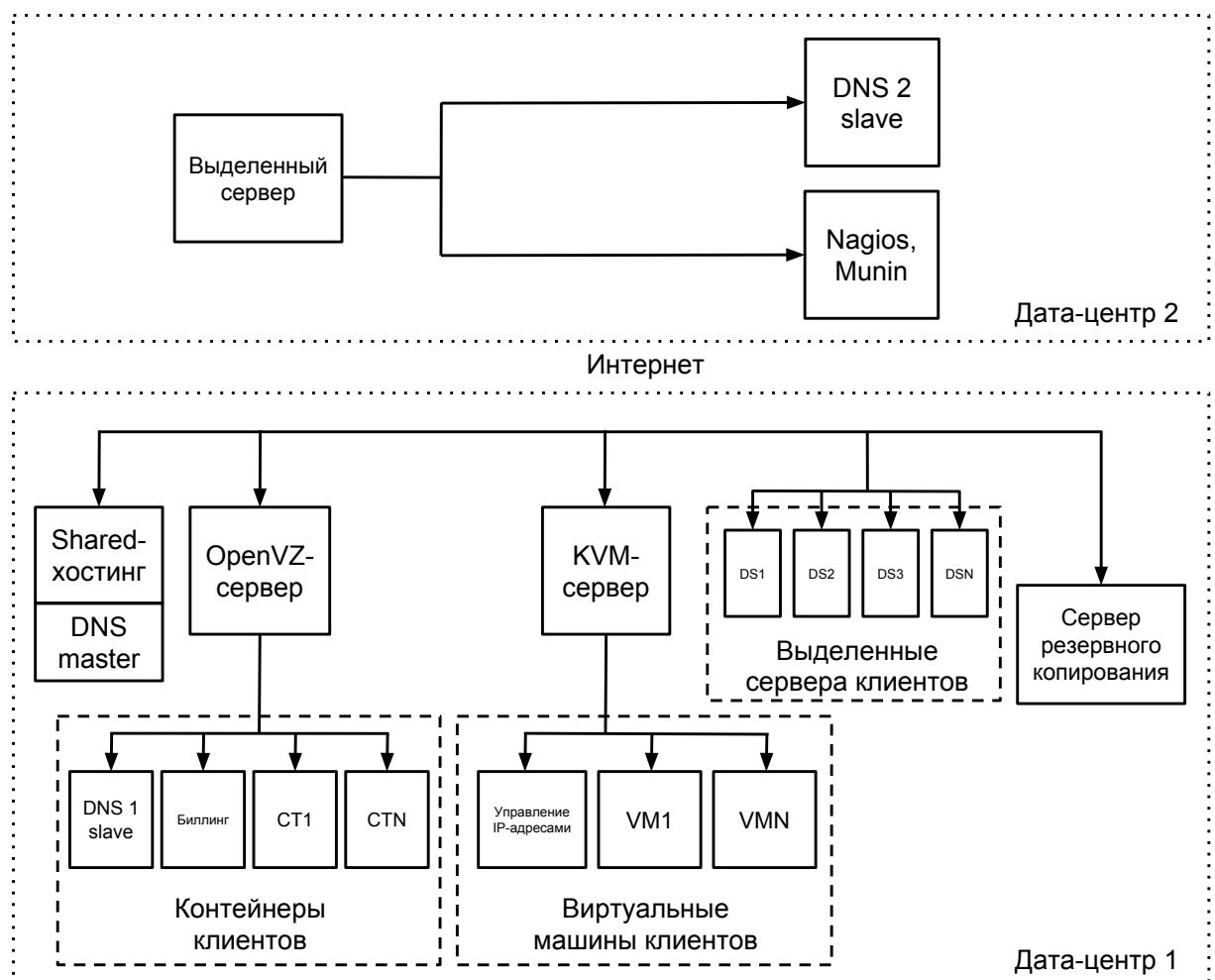


Рис. 4.1 – Общая схема инфраструктуры

В data-центре 1 располагается основная часть инфраструктуры: сервера shared-хостинга, виртуализации OpenVZ и KVM, сервер резервного копирования и выделенные сервера клиентов.

В data-центре 2 на двух арендованных виртуальных машинах находится один из подчиненных DNS-серверов, а также сервер мониторинга.

На физических серверах располагаются важные элементы инфраструктуры: главный и один подчиненный DNS-сервера, система биллинга и система управления IP-адресами.

## 4.2 Схема мониторинга

Схема мониторинга инфраструктуры представлена на рис. ??.

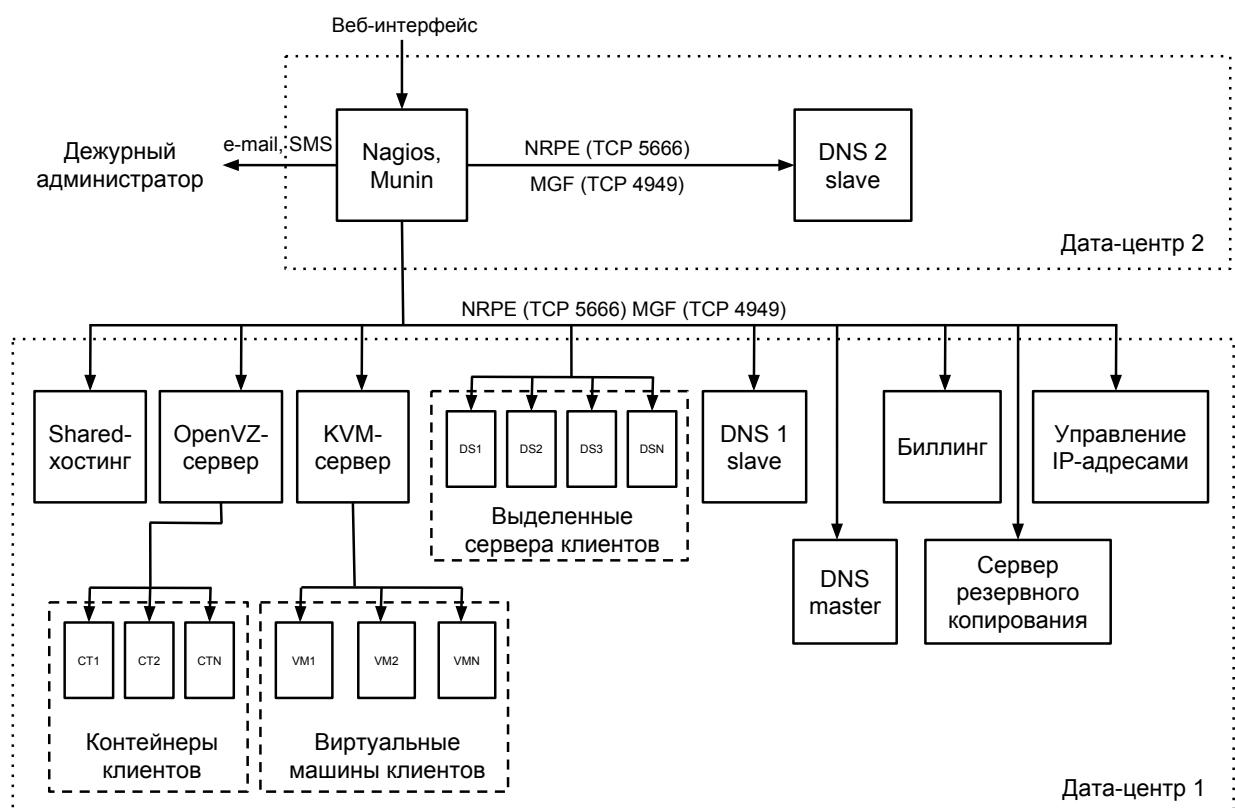


Рис. 4.2 – Схема мониторинга инфраструктуры

В случае возникновения проблемы на одном из серверов, Nagios фиксирует изменения и отправляет текстовые уведомления по SMS и электронной

почте дежурному администратору, который следит за системой мониторинга. Nagios работает по протоколу NRPE (Nagios Remote Plugin Executor) и слушает порт 5666.

Munin имеет возможность визуализировать состояние ресурсов с помощью графиков, наблюдая за графиками можно делать выводы о событиях, происходящих в инфраструктуре. Munin работает по протоколу MGF (Munin Graphing Framework) на порту 4949.

Помимо физических серверов, мониторятся также виртуальные машины, на которых располагаются сервисы инфраструктуры, а также некоторые виртуальные машины клиентов, по требованию.

#### 4.3 Схема репликации и балансировки нагрузки DNS-серверов

С целью обеспечения отказоустойчивости системы была разработана следующая схема репликации и балансировки нагрузки DNS-серверов. Схема представлена на рис. ??.

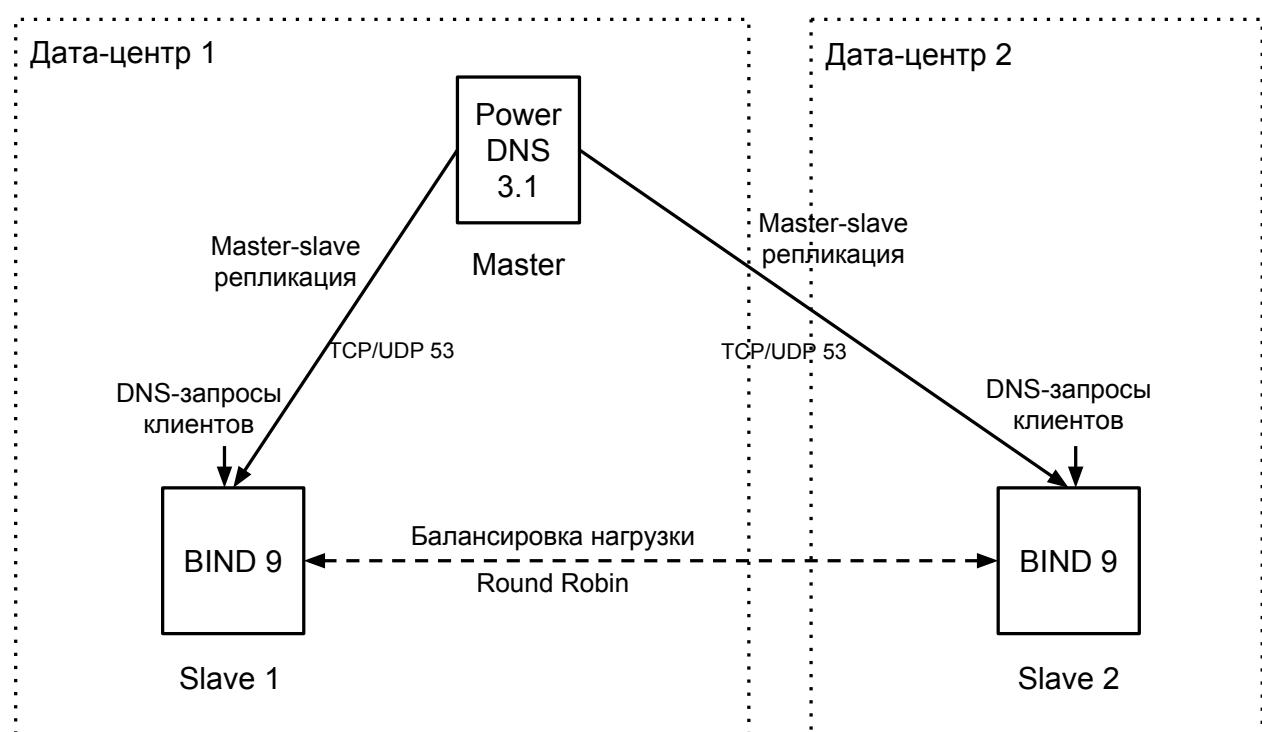


Рис. 4.3 – Схема репликации и балансировки нагрузки DNS-серверов

В каждой зоне есть один главный сервер имен на котором хранится официальная копия данных зоны. Администратор модифицирует информацию, касающуюся зоны, редактируя файлы главного сервера [?]. Подчиненный (slave) сервер копирует свои данные с главного сервера посредством операции, называемой передачей зоны (zone transfer). В зоне имеется два подчиненных сервера, один из которых располагается в другом дата-центре.

На главном сервере установлен DNS-сервер PowerDNS. На подчиненных серверах — BIND 9.

Балансировка нагрузки осуществляется по алгоритму Round Robin (алгоритм кругового обслуживания). Алгоритм представляет собой перебор по круговому циклу: первый запрос передается одному серверу, затем следующий запрос передается другому и так до достижения последнего сервера [?].

#### 4.4 Используемые технологии виртуализации

На основе обзора литературы, проведенного в пункте ??, выбраны и внедрены технологии виртуализации OpenVZ (для организации контейнеров) и KVM (для организации виртуальных машин).

#### 4.5 Алгоритмы функционирования инфраструктуры

Взаимодействие пользователя с инфраструктурой происходит по сценариям, представленным в пункте ??.

В пункте ?? представлены сценарии взаимодействия компонентов инфраструктуры.

##### 4.5.1 Схема взаимодействия пользователя с инфраструктурой

Сценарий 1. Заказ облачного сервиса:

- a) пользователь обращается к инфраструктуре через веб-интерфейс с целью заказа услуги;

- б) биллинг регистрирует нового пользователя;
- в) заключается договор на предоставление услуги с указанием реквизитов пользователя;
- г) подсистема управления услугами производит выделение физического либо виртуального сервера (контейнера, виртуальной машины), либо иной услуги с требуемыми характеристиками;
- д) переход к сценарию 2.

Сценарий 2. Использование сервиса:

- а) клиент пользуется предоставленным сервисом некоторый период времени, используя веб-интерфейс (VNC, SSH);
- б) биллинг выставляет счет пользователю за оказанные услуги;
- в) пользователь оплачивает сервис;
- г) переход к пункту а, пока не наступит событие, соответствующее сценариям 3, 4, 5, 6 или 7.

Сценарий 3. Изменение условий предоставления сервиса:

- а) пользователь желает изменить условия предоставления сервиса, либо отказаться от него;
- б) биллинг регистрирует запрос;
- в) подсистема управления услугами производит изменение условий предоставления сервиса или удаляет его;
- г) переход к сценарию 2, в случае продолжения оказания сервиса, иначе к сценарию 5.

Сценарий 4. Окончание срока действия договора:

- а) у пользователя окончился срок действия договора;
- б) биллинг блокирует услуги;
- в) если пользователь желает продлить срок действия договора, переход к сценарию 6, иначе к сценарию 5.

Сценарий 5. Окончание использования облачной услуги:

- а) пользователь желает завершить использование сервиса;
- б) биллинг регистрирует отмену использования сервиса;

- в) подсистема управления услугами удаляет пользовательскую услугу (выделенный сервер, контейнер, виртуальная машина) из списка используемых.

Сценарий 6. Продление договора:

- а) пользователь обращается к инфраструктуре через веб-интерфейс с целью продления срока действия договора;
- б) биллинг регистрирует факт заключения нового договора;
- в) переход к сценарию 2.

Сценарий 7. Возникновение проблем в работе услуги:

- а) пользователь обращается к биллингу через веб-интерфейс с целью представления заявки на устранение проблемы и информации о возникшей проблеме;
- б) биллинг регистрирует запрос и направляет его технической поддержке;
- в) техническая поддержка первого уровня устраняет проблему, если нет, то заявка передается в отдел системного администрирования;
- г) переход к сценарию 2.

Алгоритмы взаимодействия пользователем с инфраструктурой представлены на чертеже СевГУ 09.03.01.15.А2.

#### 4.5.2 Алгоритм взаимодействия компонентов инфраструктуры

Сценарий 1. Мониторинг:

- а) Nagios мониторит состояние сервисов;
- б) Nagios обнаружил недоступность или сбой сервиса;
- в) отправка электронного и SMS-сообщения дежурному администратору;
- г) дежурный администратор исправляет проблему;
- д) переход к пункту а.

Сценарий 2. Резервное копирование:

- а) запуск задания инкрементального резервного копирования;
- б) расчет свободного дискового пространства на удаленном хранилище для инкрементальной или полной копии;

- в) в случае нехватки дискового пространства на удаленном хранилище — отправка электронного сообщения системному администратору, переход к пункту е;
- г) архивация и сжатие данных;
- д) передача данных по сети;
- е) конец резервного копирования.

Сценарий 3. Распределение IP-адресов:

- а) добавлен новый физический сервер, контейнер, виртуальная машина или клиент хостинга заказал дополнительный адрес;
- б) проверка свободного IP-адреса;
- в) если свободного адреса нет, то уведомление о необходимости заказа новой подсети IP-адресов у провайдера, переход к пункту е;
- г) привязка нового IP-адреса к серверу;
- д) удаление привязанного адреса из списка свободных;
- е) конец.

Сценарий 4. Добавление нового сервера:

- а) заказ услуги физического сервера, контейнера или виртуальной машины;
- б) выделение IP-адресов;
- в) подключение к системе мониторинга;
- г) трансфер или создание зоны на главном DNS-сервере;
- д) подключение к системе резервного копирования;
- е) конец.

Сценарий 5. Добавление нового домена:

- а) трансфер или создание зоны на главном DNS-сервере;
- б) проверка доступности подчиненных DNS-серверов;
- в) репликация зоны на подчиненные сервера;
- г) ожидание обновления зон провайдера;
- д) проверка работоспособности DNS;
- е) конец.

Алгоритм взаимодействия компонентов инфраструктуры представлен на чертеже СевГУ 09.03.01.15.А3.

## 5 РУКОВОДСТВО АДМИНИСТРАТОРА

Руководство администратора содержит информацию о сетевой инфраструктуре, используемых технологиях виртуализации и программном обеспечении.

### 5.1 Расположение серверов в сетевой инфраструктуре

Во всей инфраструктуре на физических серверах первого дата-центра располагаются:

- shared-хостинг (10.0.0.100);
- виртуализация OpenVZ (10.0.1.100);
- виртуализация KVM (10.0.2.100);
- сервер резервного копирования (10.0.3.100);
- физические сервера клиентов (10.0.4.100 — 10.0.4.200).

В свою очередь, некоторые важные сервисы инфраструктуры располагаются на виртуальных машинах:

- сервер биллинга (10.0.1.101), OpenVZ;
- сервер управления IP-адресами (10.0.2.101), KVM;
- сервер DNS 1 (10.0.2.102), KVM.

Сервер мониторинга и сервер DNS 2 располагаются на виртуальных машинах KVM в другом дата-центре. Сервер shared-хостинга выполняет роль главного (master) DNS-сервера и управляет с помощью PowerDNS.

### 5.2 Сервер shared-хостинга

Сервер shared-хостинга является самым уязвимым местом всей инфраструктуры из-за большого количества и плотности клиентов на сервере. Распределение ресурсов между пользователями происходит за счет встроенных в ядро Linux механизмов.

Стоит отметить, что после переезда на новый сервер для хранения данных доступен RAID-массив из SSD дисков объемом 1 Тб.

На сервере установлен и настроен веб-сервер в составе следующего ПО:

- http-сервер Apache HTTP Server, кэширующий и проксирующий http-сервер nginx и обработчик динамических PHP-запросов php-fpm;
- memcached кэширует динамические запросы в оперативной памяти;
- MySQL и PostgreSQL выполняют роли серверов баз данных.

nginx принимает запросы к серверу с порта 80 и решает каким образом обрабатывать запрос. Если это запрос на получение статического файла (изображение, js-код, CSS, видео, аудио, архивы), то nginx сам его обрабатывает и в случае необходимости кэширует. Если же запрашивается динамическое содержимое, то nginx передает запрос на бэкенд, где его, в зависимости от настройки виртуального хоста сайта, обрабатывает либо php-fpm, либо встроенный в Apache модуль mod\_php. nginx не может кэшировать динамические запросы, поэтому для этого используется memcached, который работает в связке с Apache и позволяет кэшировать динамические запросы. Для работы Apache с memcached необходима установка модуля PHP php5-memcached:

Почтовой связкой на сервере shared-хостинга выступает SMTP-сервер Exim Internet Mailer, а запросы по протоколам POP3 и IMAP принимает Dovecot. В качестве антиспам-связки выступает Postgrey, Spamassassin, ClamAV и OpenDKIM. Конфигурации данных сервисов являются стандартными.

ProFTPD необходим для работы пользователей по протоколу FTP. Доступна возможность подключения пользователей по протоколу FTPS (порт 22).

Сервер управления временем NTP обращается к следующим серверам за уточнением времени на сервере:

Конфигурация SSH требует отдельного пояснения. Доступ к SSH по стандартному порту закрыт, это позволяет избавиться от большинства злоумышленников, которые пытаются скомпрометировать пароль доступа к серверу. Также запрещен вход от пользователя root, для этого создан отдельный пользователь. Можно ограничить доступ к серверу по SSH, оставив только доверенные адреса или подсети адресов.

Подключение к серверу по SSH и получение root-прав:

Разрешен вход на сервер по ключам:

Резервное копирование данных пользователей осуществляется средствами панели ISPmanager 5 в ночное время, применяется инкрементальный метод резервного копирования. В инкрементальном методе копирования при первом резервном копировании будет создана полная копия, в которой будут сохранены все файлы. При последующих будут сохраняться файлы, измененные с момента предыдущей полной или инкрементальной копии. Для восстановления необходимо несколько копий — полная и все инкрементальные, сохраненные

до выбранной точки восстановления. Раз в неделю (в воскресенье) запускается очередная полная резервная копия данных. На сервере функционирует скрипт блокировки адресов, которые слишком часто подбирают пароли доступа к панели администратора наиболее популярных CMS (система управления содержимым), таких как WordPress и Joomla. Скрипт написан на языке Shell, находится в открытом доступе и имеет простое использование:

Основные конфигурации настроек веб-сервера хранятся в файлах:

- /etc/nginx/nginx.conf;
- /etc/apache2/apache2.conf;

- /etc/php5/{apache2,cgi,cli,fpm}/php.ini;
- /etc/mysql/my.cnf;
- /etc/postgresql/9.1/main/postgresql.conf.

Для сканирования уязвимостей на сайтах пользователей используется утилита maldet, которая находит подозрительные файлы в системе и составляет отчет по найденным файлам.

Установка и пример использования maldet:

На сервере shared-хостинга на сайтах пользователей находится большое количество уязвимостей, которые часто используются для рассылки спама с сервера. Для обнаружения большого числа рассылок с сервера был написан плагин для системы мониторинга Nagios, который контролирует число писем в почтовой очереди, а также проверяет наиболее популярные организации (например Spamhaus), которые собирают данные о спам-серверах.

Для просмотра списка очереди используется команда exim -bp или mailq. Таким образом можно просмотреть количество писем для разных доменов и их количество:

В данном случае очевидна рассылка писем с сайта spamsite.ru. Посмотреть идентификатор письма (ID), а также содержимое заголовков и тела письма можно теми же командами, но с другими параметрами:

Если сайт действительно заражен, то следует отключить его, оповестить пользователя о закрытии сайта и необходимости избавления от вредоносного кода. Также необходимо удалить спам-письма из очереди сообщений:

В случае неработоспособности панели ISPmanager 5 возможна ее перезагрузка:

### 5.3 Сервер виртуализации OpenVZ

Список всех существующих в системе контейнеров можно узнать командой `vzlist -a`:

В заголовках показывается ID контейнера, число процессов в контейнере, текущий статус, IP-адрес и имя контейнера. Список всех доступных шаблонов операционной системы и список шаблонов установленных локально:

Каждый контейнер имеет свой конфигурационный файл, которые хранятся в каталоге `/etc/sysconfig/vz-scripts/`, именуются эти файлы по CTID контейнера. Например, для контейнера с `CTID=101`, файл будет называться `101.conf`. При создании контейнера можно использовать типовую конфигурацию для VPS. Типовые файлы конфигураций находятся в том же каталоге:

В этих конфигурационных файлах описаны контрольные параметры ресурсов, выделенное дисковое пространство, оперативная память и прочие ресурсы. На базе уже существующего файла конфигурации создан типовой файл, подходящий для большинства контейнеров именуемый `ve-custom.conf-sample`. Таким образом, при использовании этого конфигурационного файла, будет создаваться контейнер, которому будет доступен 1 Гб выделенного дискового пространства, 128 Мб оперативной памяти и 128 Мб SWAP. В дальнейшем, при

создании контейнеров, следует использовать данный конфигурационный файл. Создание контейнера осуществляется командой:

где 101 — CTID контейнера, --ostemplate — шаблон ОС, --config — используемый шаблон конфигурационного файла. Перед первым запуском контейнера необходимо установить его IP адрес, hostname, указать DNS сервера и задать пароль суперпользователя. Для настройки VPS используется команда vzctl set. Для того, чтобы контейнер запускался при старте хост-компьютера (например после перезагрузки), необходимо использовать команду:

При использовании ключа --save, сохраняются параметры контейнера в соответствующий ему конфигурационный файл. Аналогично задается hostname и IP-адрес:

Адреса DNS серверов (в большинстве случаев адрес DNS совпадает с адресом хост-компьютера, поэтому можно вместо адреса указать параметр inherit):

Установка пароля суперпользователя:

Пароль будет установлен в VPS, в файл /etc/shadow и не будет сохранен в конфигурационный файл контейнера. Если же пароль будет утерян или забыт, то можно будет просто задать новый. После настроек нового контейнера, его можно запустить:

Проверка сетевых интерфейсов внутри гостевой ОС:

Должны присутствовать сетевые интерфейсы:

- lo (127.0.0.1);
- venet0 (127.0.0.2);
- venet0:0 (10.0.0.210).

Если сеть в порядке, то можно соединиться к контейнеру по SSH с хост-компьютера:

Вход в контейнер напрямую с хост-компьютера осуществляется командой vzctl enter:

Для остановки контейнера используется команда vzctl stop. Для полной остановки контейнера, системе требуется немного времени. Иногда нужно выключить VPS как можно быстрее, например, если контейнер был подвержен взлому. Для того чтобы срочно выключить VPS, используется ключ --fast:

Для перезапуска контейнера можно использовать команду vzctl restart. Для того чтобы удалить контейнер, его нужно сначала остановить:

Команда выполняет удаление частной области сервера и переименовывает файл конфигурации, дописывая к нему .destroyed. Иногда бывает нужно выполнить команду на нескольких VPS. Для этого можно использовать команду:

Например можно узнать сколько времени работают все запущенные контейнеры:

Если на хост-ноде наблюдается высокое значение Load Average, то в первую очередь следует посмотреть данные значения непосредственно у контейнеров:

В случае обнаружения нагружающего контейнера, стоит подключиться к нему и устранить причину нагрузки. Непосредственно с хост-ноды можно узнать, какому контейнеру принадлежит процесс:

Свободное место в контейнере можно узнать командой df:

Подключение модуля TUN для контейнера (необходимо для работы OpenVPN).  
Прежде чем запускать контейнер нужно убедиться, что модуль TUN загружен на хост-ноде:

В случае, если модуль не загружен:

Разрешаем использовать устройство TUN контейнеру:

Запуск контейнера:

Создание в контейнере собственного устройства TUN:

Для пользователей в контейнерах доступен брандмауэр Netfilter, для его работы в файле /etc/vz/vz.conf должна присутствовать строка:

Для того, чтобы для контейнеров был доступен FUSE, его необходимо включить на хост-ноде и проверить, что он успешно включен:

Также необходимо добавить автозагрузку модуля при перезапуске хост-ноды:

Проброс FUSE для контейнера 101:

В контейнере проверяем, пробросилось ли устройство:

Резервное копирование контейнеров осуществляется утилитами `vzdump` и `vzrestore`:

Для работы OpenVZ с файлами используется `ploop`, так как `simfs` является устаревшим методом. Диски с файловыми системами контейнеров хранятся в `/vz/private` и имеют имя `root.hdd`. Смена размера диска для контейнера:

## 5.4 Сервер виртуализации KVM

В целом, администрирование KVM-ноды не отличается от администрирования OpenVZ. Однако в случае OpenVZ возможно получить доступ к пользовательскому контейнеру непосредственно с хост-ноды, в случае с KVM это

невозможно, это следует учесть при работе с виртуальной машиной. Изменение размера диска также является нетривиальной задачей, высок риск краха всей файловой системы без возможности восстановления данных. Команды, которые чаще всего используются при администрировании виртуальных машин на базе KVM:

Для защиты сервера от брутфорса пароля SSH на серверах OpenVZ и KVM используется fail2ban. Установка (в CentOS 6, для установки fail2ban нужно подключить репозиторий EPEL):

fail2ban блокирует с помощью IPTables на некоторое время активные адреса, которые пытаются соединиться по SSH после пяти неудачных попыток, также отправляет администратору письмо с уведомлением о блокировке:

Разблокировать IP адрес из бана:

Пример разблокировки:

В виртуальных машинах пользователи зачастую склонны забывать пароль от MySQL. В данном случае существует простое решение проблемы.

Остановка службы MySQL:

Запуск службы с опцией --skip-grant-tables:

Подключение к серверу MySQL при помощи клиента:

Ввод нового пароля для root:

Остановка сервера MySQL:

Запуск MySQL-сервера и вход с новым паролем:

## 5.5 Дополнительные виртуальные сервера

В качестве сервера мониторинга используется Nagios, для построения графиков — Munin. Дополнительной настройки этих сервисов не требуется.

Добавление новых хостов происходит вручную, требуется лишь править адреса и сервисы, которые требуется мониторить.

Важно мониторить свободное место на жестком диске сервера резервного копирования и вовремя очищать старые резервные копии.

На DNS серверах используется master-slave репликация, причем один из DNS-серверов, равно как и сервер мониторинга расположены в другом data-центре для обеспечения отказоустойчивости системы. Также между подчиненными серверами настроена балансировка нагрузки.

## 5.6 Защита от DDoS-атак

Стоит незамедлительно реагировать на DDoS-атаки. При обнаружении подозрительного трафика следует убедиться, что это действительно DDoS, а также поинтересоваться у data-центра реакцию сетевого оборудования на нее. Определить DDoS это или нет можно с помощью утилит netstat и iftop.

Намеренную DDoS-атаку сложно остановить лишь с помощью программных средств, однако некоторые несложные скрипты позволяют отражать небольшие «любительские» атаки на отказ. Подобный скрипт блокировки DDoS-атак представлен в приложении А. Скрипт анализирует текущие подключения к серверу на основе утилиты netstat, в случае превышения определенного лимита подключений, адрес попадает в блок IPTables на некоторое время.

Для блокировки намеренных атак требуется аппаратная защита на уровне сетевого оборудования. Защита от распределенных DDoS-атак основывается на многофакторном анализе трафика, который поступает на каждый защищаемый сервер. Во время нормальной работы система защиты может самообучаться или настраиваться, а после обнаружения атаки либо автоматически, либо по требованию, активно противодействует нелегитимному трафику.

В данном случае защитником выступает data-центр, который имеет в распоряжении оборудование, способное осуществлять фильтрацию трафика и предотвращение атак на отказ.

## 5.7 Общие рекомендации по администрированию инфраструктуры

Следует следить за новостными рассылками о критических уязвимостях в операционной системе и используемом программном обеспечении.

Если работа сервера замедлилась, в диагностике проблемы помогут утилиты ps, top, atop, htop. В случае обнаружения сетевых проблем на помощь придут утилиты ping, traceroute, nmap, mtr, tcpdump, iftop.

Важно следить за состоянием RAID на сервере, в случае сбоя одного из дисков, следует обратиться к поддержке data-центра с просьбой о замене диска.

Необходимо подбирать сложные для перебора пароли, периодически их менять и уведомлять пользователей о смене пароля. Для генерации паролей подходит утилита pwgen:

Стоит аккуратно работать на сервере под учетной записью root, не стоит запускать неизвестные скрипты или двоичные файлы. Необходимо проверять контрольные суммы загруженных пакетов и следить за цифровой подписью.

Не следует просто так перезагружать сервер, рекомендуется это делать только в случаях чрезвычайной необходимости (например обновление ядра).

Всегда стоит проверять наличие актуальных резервных копий, а также свободное место на системах хранения данных. Стоит также настроить ротацию логов, это позволит сэкономить место на диске.

На физических нодах стоит устанавливать только самый необходимый, минимальный набор программного обеспечения, для уменьшения вероятности компрометации сервера.

Всегда стоит вести документацию в том или ином виде и логировать свои действия на сервере. Логи, которые могут помочь в диагностике неисправностей:

- /var/log/{apache2,httpd}/error.log;
- /var/log/auth.log;
- /var/log/dmesg;

- `/var/log/kern.log`;
- `/var/log/libvirt/libvirtd.log`;
- `/var/log/mail.log`;
- `/var/log/messages`;
- `/var/log/mysql/mysql-slow.log`;
- `/var/log/nginx/error.log`;
- `/var/log/syslog`;
- `/var/log/vzctl.log`.

В случае обнаружения неполадок с аппаратной частью, стоит незамедлительно обратиться к провайдеру для проверки работоспособности аппаратуры. В случае недочетов в программном обеспечении стоит обратиться к технической поддержке ПО.

## 6 РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

В руководстве администратора рассмотрен процесс заказа услуги пользователем, внешний интерфейс панелей управления. Панели биллинга, панели управления хостингом, контейнерами и виртуальными машинами имеют простой интуитивный интерфейс с возможностью тонкой настройки.

Рассмотрен процесс подачи запроса в техническую поддержку. Для пользователя доступны ответы на самые часто задаваемые вопросы в разделе *wiki*.

Руководство пользователя представлено в приложении Б.

## 7 РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

В режиме нормального функционирования мониторинг показывает полную работоспособность всех сервисов системы (рис. ??).

<a href="#">dams-oo-ups1</a>	<a href="#">Battery expired</a>	OK	13-12-2011 09:43:58	32d 18h 0m 3s	1/2	OK: noBatteryNeedsReplacing	
	<a href="#">Battery status</a>	OK	13-12-2011 09:45:32	32d 18h 0m 3s	1/2	OK: batteryNormal	
	<a href="#">Battery temperature</a>	OK	13-12-2011 09:44:41	32d 18h 0m 3s	1/2	SNMP OK - 28	
	<a href="#">Input voltage</a>	OK	13-12-2011 09:44:08	0d 14h 5m 54s	1/2	SNMP OK - 244	
	<a href="#">Output load</a>	OK	13-12-2011 09:45:32	32d 18h 0m 3s	1/2	SNMP OK - 35	
	<a href="#">Output status</a>	OK	13-12-2011 09:45:00	0d 10h 49m 2s	1/2	OK: onLine	
	<a href="#">Temperature sensor</a>	OK	13-12-2011 09:44:00	32d 17h 58m 40s	1/2	SNMP OK - 23	
<a href="#">dams-oo-ups2</a>	<a href="#">Battery expired</a>	OK	13-12-2011 09:44:00	70d 2h 7m 53s	1/2	OK: noBatteryNeedsReplacing	
	<a href="#">Battery status</a>	OK	13-12-2011 09:44:00	70d 0h 44m 29s	1/2	OK: batteryNormal	
	<a href="#">Battery temperature</a>	OK	13-12-2011 09:44:00	70d 2h 6m 15s	1/2	SNMP OK - 30	
	<a href="#">Input voltage</a>	OK	13-12-2011 09:45:24	0d 14h 6m 38s	1/2	SNMP OK - 244	
	<a href="#">Output load</a>	OK	13-12-2011 09:44:00	70d 2h 6m 17s	1/2	SNMP OK - 57	
	<a href="#">Output status</a>	OK	13-12-2011 09:44:41	0d 10h 49m 21s	1/2	OK: onLine	
<a href="#">dams-oo-ups3</a>	<a href="#">Battery expired</a>	OK	13-12-2011 09:44:49	70d 2h 7m 29s	1/2	OK: noBatteryNeedsReplacing	
	<a href="#">Battery status</a>	OK	13-12-2011 09:45:32	70d 2h 6m 32s	1/2	OK: batteryNormal	
	<a href="#">Battery temperature</a>	OK	13-12-2011 09:44:00	70d 2h 7m 33s	1/2	SNMP OK - 35	
	<a href="#">Input voltage</a>	OK	13-12-2011 09:44:00	0d 8h 2m 2s	1/2	SNMP OK - 246	
	<a href="#">Output load</a>	OK	13-12-2011 09:44:42	70d 2h 7m 53s	1/2	SNMP OK - 23	
	<a href="#">Output status</a>	OK	13-12-2011 09:45:30	0d 4h 40m 32s	1/2	OK: onLine	
<a href="#">dams-oo-ups4</a>	<a href="#">Battery expired</a>	OK	13-12-2011 09:44:01	70d 2h 6m 8s	1/2	OK: noBatteryNeedsReplacing	
	<a href="#">Battery status</a>	OK	13-12-2011 09:44:00	38d 19h 7m 14s	1/2	OK: batteryNormal	
	<a href="#">Battery temperature</a>	OK	13-12-2011 09:44:49	70d 2h 7m 16s	1/2	SNMP OK - 26	
	<a href="#">Input voltage</a>	OK	13-12-2011 09:45:42	0d 8h 8m 20s	1/2	SNMP OK - 244	
	<a href="#">Output load</a>	OK	13-12-2011 09:45:08	70d 2h 7m 28s	1/2	SNMP OK - 45	
	<a href="#">Output status</a>	OK	13-12-2011 09:45:31	0d 5h 8m 31s	1/2	OK: onLine	
<a href="#">dams-oo-ups5</a>	<a href="#">Battery expired</a>	OK	13-12-2011 09:44:00	34d 18h 39m 8s	1/2	OK: noBatteryNeedsReplacing	
	<a href="#">Battery status</a>	OK	13-12-2011 09:44:42	34d 18h 39m 7s	1/2	OK: batteryNormal	
	<a href="#">Battery temperature</a>	OK	13-12-2011 09:44:42	34d 18h 39m 7s	1/2	SNMP OK - 29	
	<a href="#">Input voltage</a>	OK	13-12-2011 09:44:32	0d 14h 7m 30s	1/2	SNMP OK - 243	
	<a href="#">Output load</a>	OK	13-12-2011 09:45:32	34d 18h 39m 8s	1/2	SNMP OK - 55	
	<a href="#">Output status</a>	OK	13-12-2011 09:45:49	0d 10h 52m 13s	1/2	OK: onLine	
<a href="#">dams-oo-ups6</a>	<a href="#">Battery expired</a>	OK	13-12-2011 09:45:31	70d 2h 6n 16s	1/2	OK: noBatteryNeedsReplacing	
	<a href="#">Battery status</a>	OK	13-12-2011 09:44:49	70d 2h 5m 52s	1/2	OK: batteryNormal	
	<a href="#">Battery temperature</a>	OK	13-12-2011 09:45:44	38d 18h 22m 2s	1/2	SNMP OK - 35	
	<a href="#">Input voltage</a>	OK	13-12-2011 09:45:28	0d 8h 8m 34s	1/2	SNMP OK - 244	
	<a href="#">Output load</a>	OK	13-12-2011 09:44:12	70d 2h 7m 33s	1/2	SNMP OK - 16	
	<a href="#">Output status</a>	OK	13-12-2011 09:45:07	0d 5h 10m 55s	1/2	OK: onLine	
<a href="#">dams-rsl-sw1</a>		<a href="#">ports</a>	OK	13-12-2011 09:44:38	19d 19h 1m 19s	1/2	OK: host '10.2.0.251', interfaces up: 41, down: 0, dormant: 0, excluded: 0, unused: 0
<a href="#">dams-rsl-sw2</a>		<a href="#">ports</a>	OK	13-12-2011 09:45:29	19d 19h 0m 33s	1/2	OK: host '10.2.0.250', interfaces up: 5, down: 0, dormant: 0, excluded: 0, unused: 0

Рис. 7.1 – Работоспособность сервисов в штатном режиме

В случае появления внештатных ситуаций, система мониторинга фиксирует аномальные явления, такие как недоступность хостов или отдельных сервисов. Мониторинг способен запоминать код ошибки, поэтому диагностика неисправностей является несложной задачей. Пример реакции системного мониторинга на недоступность сервера представлен на рис. ??.

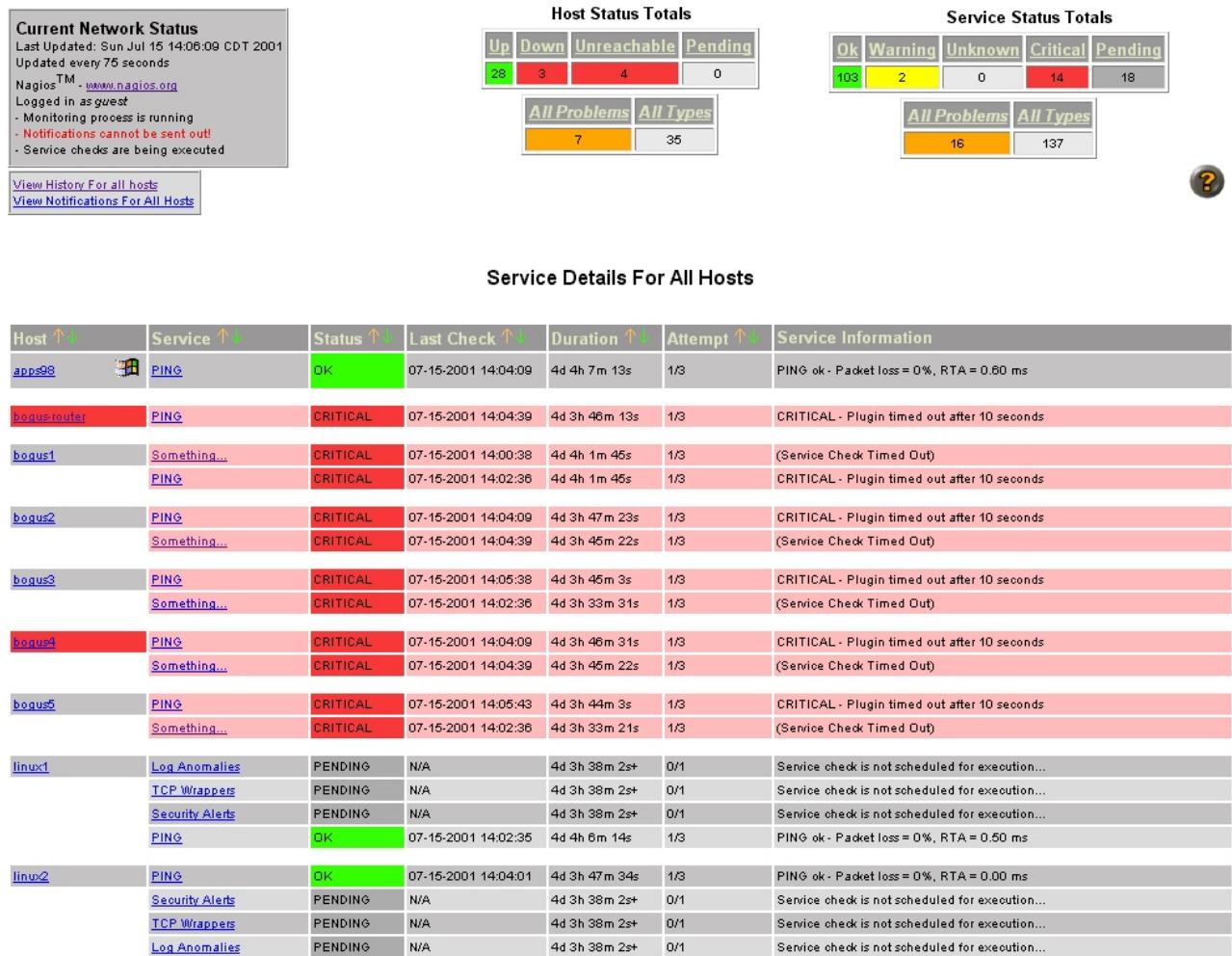


Рис. 7.2 – Недоступность некоторых серверов инфраструктуры

Пример реакции системы мониторинга Nagios на неисправность одного из дисков в RAID-массиве представлен на рис. ??.

Hardware	CRITICAL	01-26-2011 08:29:38	1d 15h 21m 10s	3/3	CRITICAL : Disk Drive Bay 1 Drive 5: In Critical Array CRITICAL : Disk Drive Bay 1 Drive 4: In Critical Array CRITICAL : Disk Drive Bay 1 Drive 3: In Critical Array CRITICAL : Disk Drive Bay 1 Drive 2: Drive Fault CRITICAL : Disk Drive Bay 1 Drive 2: In Critical Array CRITICAL : Disk Drive Bay 1 Drive 1: In Critical Array CRITICAL : Disk Drive Bay 1 Drive 0: In Critical Array CRITICAL : Drive 2 in enclosure 32 on controller 0 Fw: D305 - FAILED WARNING : RAID 5 Logical Volume 0 on controller 0, Drives:(0e32,1e32,2e32,3e32,4e32,5e32) - DEGRADED - Server: Dell Inc. PowerEdge 2950 s/n: System BIOS: 2.4.3 2008-08-15
----------	----------	---------------------	----------------	-----	--

Рис. 7.3 – Сбой работы диска в RAID-массиве

## 7.1 Нагрузка сети во время резервного копирования

Каждую ночь на серверах запускается задача резервного копирования, в это время наблюдается повышенная нагрузка на сервере, связанная со снятием

дампов баз данных, архивацией и сжатием архивов для передачи по сети на сервер резервного копирования.

Как правило повышение нагрузки незначительное, что можно наблюдать на рис. ??.

```
top - 13:10:28 up 5 days, 6:26, 1 user, load average: 3,04, 3,47, 4,40
Tasks: 185 total, 1 running, 184 sleeping, 0 stopped, 0 zombie
%Cpu(s): 26,1 us, 8,1 sy, 0,0 ni, 65,2 id, 0,5 wa, 0,0 hi, 0,0 si, 0,0 st
KiB Mem: 24745308 total, 14228264 used, 10517044 free, 1392500 buffers
KiB Swap: 16383996 total, 59036 used, 16324960 free, 9615508 cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
21171	mysql	20	0	849m	527m	5532	S	27,6	2,2	497:16.96	mysqld
4437	root	20	0	816m	307m	12m	S	3,0	1,3	60:51.18	core
6127	www-data	20	0	331m	257m	2236	S	1,0	1,1	0:03.62	nginx
21194	root	20	0	548m	64m	11m	S	1,0	0,3	26:35.18	core
31987	root	20	0	99,2m	5360	1876	S	1,0	0,0	6:29.09	ihttpd
7221	root	20	0	322m	42m	568	S	0,7	0,2	0:02.78	apache2
18065	root	20	0	322m	42m	568	S	0,7	0,2	0:00.06	apache2
18181	root	20	0	322m	42m	568	S	0,7	0,2	0:00.02	apache2
34	root	20	0	0	0	0	S	0,3	0,0	3:44.26	kworker/7:0
46	root	20	0	0	0	0	S	0,3	0,0	4:12.10	kworker/2:1
50	root	20	0	0	0	0	S	0,3	0,0	3:33.21	kworker/6:1
223	root	20	0	0	0	0	S	0,3	0,0	38:07.82	jbd2/sda3-8
6126	www-data	20	0	331m	257m	2204	S	0,3	1,1	0:01.41	nginx
9860	root	20	0	322m	42m	568	S	0,3	0,2	0:02.06	apache2
14453	root	20	0	322m	42m	568	S	0,3	0,2	0:01.05	apache2
15297	root	20	0	322m	42m	568	S	0,3	0,2	0:00.77	apache2
16826	root	20	0	322m	42m	568	S	0,3	0,2	0:00.35	apache2
16827	root	20	0	322m	42m	568	S	0,3	0,2	0:00.39	apache2
17319	root	20	0	322m	42m	568	S	0,3	0,2	0:00.25	apache2
17846	root	20	0	322m	42m	568	S	0,3	0,2	0:00.09	apache2
<b>18158</b>	<b>root</b>	<b>20</b>	<b>0</b>	<b>24476</b>	<b>1744</b>	<b>1196</b>	<b>R</b>	<b>0,3</b>	<b>0,0</b>	<b>0:00.02</b>	<b>top</b>
28120	root	20	0	322m	51m	9524	S	0,3	0,2	2:23.84	apache2
1	root	20	0	10648	680	648	S	0,0	0,0	0:34.27	init

Рис. 7.4 – Состояние системы во время процесса резервного копирования

На графике Munin можно наблюдать значительное повышение утилизации сетевого канала во время резервного копирования. График представлен на рис. ?? . Значения представленные на графике являются условными, сетевого канала в 10 Мб/с явно недостаточно для такой инфраструктуры. На деле используется сеть с пропускной способностью 100 Мб/с.

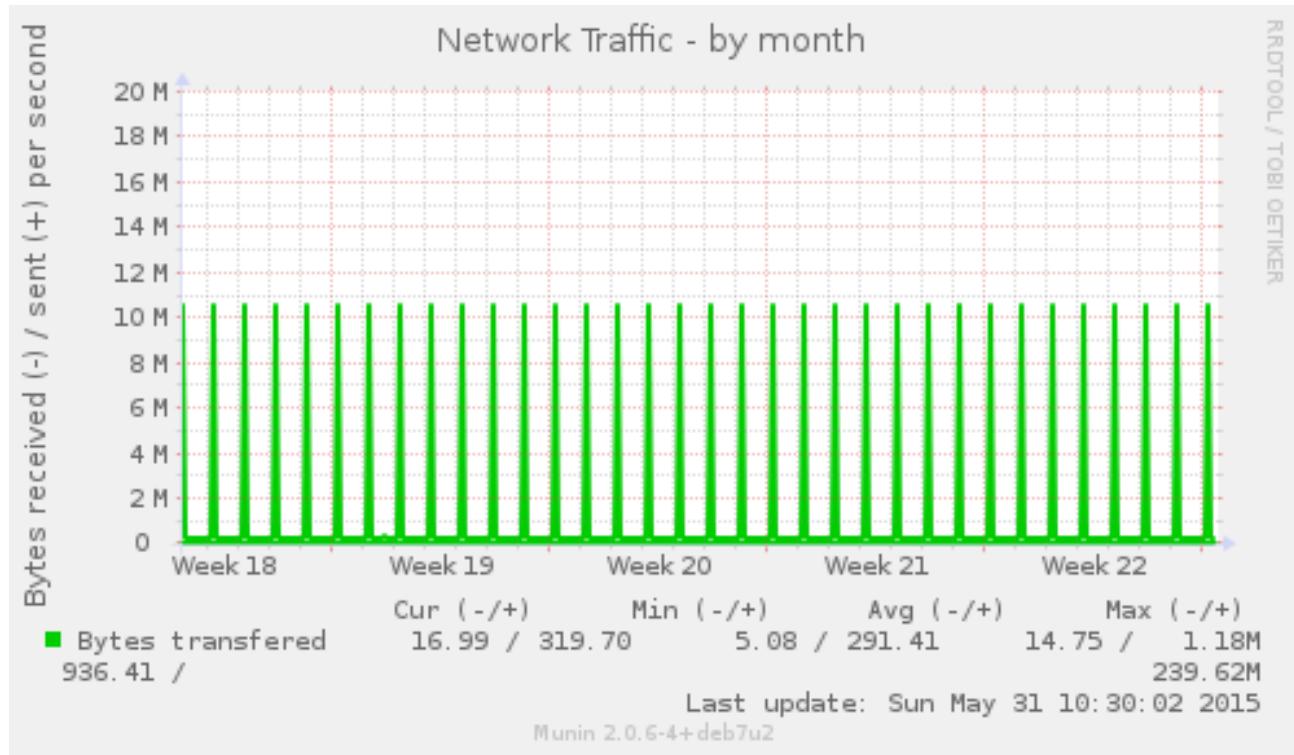


Рис. 7.5 – Состояние системы во время процесса резервного копирования

На графике представлено состояние канала сети за последний месяц, пиками на графике являются значения максимальной пропускной способности сети.

## 7.2 Состояние сервера в период атаки на отказ

Можно выделить три основных типа DDoS атак:

- переполнение сетевого канала;
- большое количество одновременных подключений (syn-flood);
- исчерпание процессорных мощностей сервера (HTTP-flood).

От последних двух типов атак можно защищаться средствами операционной системы. В случае переполнения сетевого канала, решением проблемы является расширение сетевого канала.

Состояние нагрузки системы во время DDoS-атаки можно проанализировать на рис. ??.

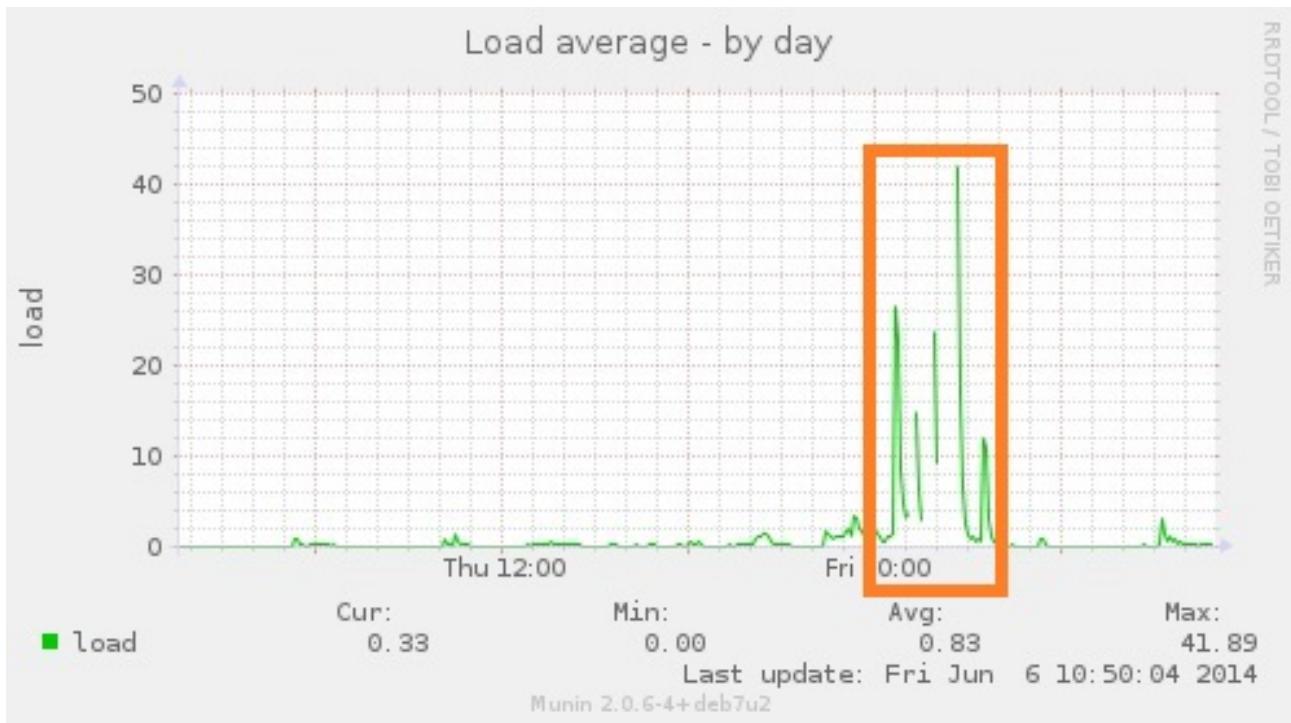


Рис. 7.6 – Значительное повышение нагрузки в период 0:00

В данный промежуток времени нагрузка составила 40 LA, что превышает среднюю нагрузку на используемом сервере в 20 раз. При этом, в процессах системы наблюдается явная нагрузка на сервер баз данных (рис. ??).

```

1 [|||||] 93.5%      5 [|||||] 91.8%
2 [|||||] 93.5%      6 [|||||] 94.1%
3 [|||||] 91.8%      7 [|||||] 96.4%
4 [|||||] 94.1%      8 [|||||] 92.3%
Mem [|||||] 112743/24165MB] Tasks: 690, 298 thr; 21 running
Swp [|||||] 4029/16380MB] Load average: 40.68 53.21 40.80
Uptime: 4 days, 18:17:41

```

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
2434	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.00	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2457	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.19	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2458	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.00	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2459	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.00	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2460	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.02	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2461	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.53	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2462	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.34	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2463	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.00	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2464	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.00	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2228	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.02	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2229	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.01	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2230	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.41	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2231	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.00	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2232	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.01	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2233	mysql	20	0	6179M	1270M	4716	S	30.0	5.3	0:00.52	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2234	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.30	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2235	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.02	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di
2270	mysql	20	0	6179M	1270M	4716	S	0.0	5.3	0:00.15	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-di

Рис. 7.7 – Все процессорные ядра заняты обработкой запросов

На графиках соединений с брандмауэром также наблюдается аномальное явление (рис. ??).

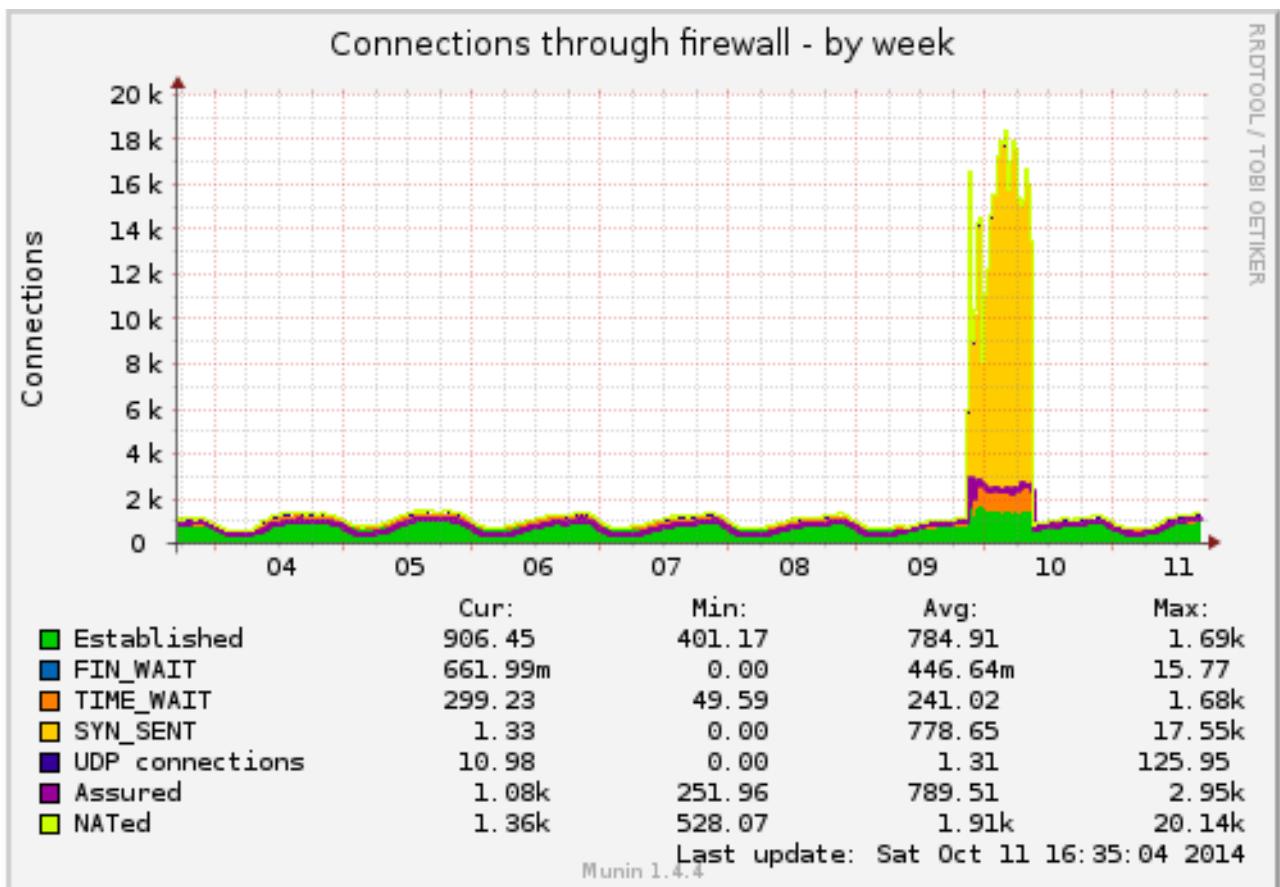


Рис. 7.8 – Превышено число соединений к брандмауэру в 40 раз

Если взглянуть на вывод команды netstat, то можно заметить наиболее активные адреса:

### 7.3 Отказ одного из DNS-серверов

Nagios зафиксировал недоступность одного из DNS-серверов, неспособного осуществлять обработку запросов (рис. ??).

DNS IP Match	OK	05-31-2015 10:24:24	1010d 17h 4m 5s	1/5	DNS OK: 0.006 seconds response time. www.nagios.com returns 50.116.21.73
DNS Resolution	OK	05-31-2015 10:24:34	1804d 2h 9m 6s	1/5	DNS OK: 0.005 seconds response time. www.nagios.com returns 50.116.21.73
HTTP	OK	05-31-2015 10:21:09	962d 17h 25m 30s	1/5	HTTP OK: HTTP/1.1 301 Moved Permanently - 557 bytes in 0.001 second response time
Ping	OK	05-31-2015 10:22:33	1771d 9h 57m 6s	1/5	OK - www.nagios.com: rta 0.261ms, lost 0%
DNS IP Match	CRITICAL	05-31-2015 10:21:37	943d 17h 27m 37s	5/5	DNS CRITICAL - expected '199.59.148.10,199.59.150.39,199.59.150.7' but got '199.59.148.10,199.59.148.82,199.59.149.198,199.59.149.230,199.59.150.39'
DNS Resolution	CRITICAL	05-31-2015 10:24:39	1758d 15h 42m 10s	1/5	DNS CRITICAL
HTTP	UNKNOWN	05-31-2015 10:21:14	382d 20h 27m 48s	5/5	check_http: Invalid onredirect option - -u
Ping	OK	05-31-2015 10:24:19	1758d 15h 44m 33s	1/5	OK - www.twitter.com: rta 42.352ms, lost 0%

Рис. 7.9 – Недоступность DNS-сервера

При этом все сайты доступны и работают в штатном режиме, так как отсутствие одного из трех серверов не влияет на работоспособность всей инфраструктуры. Один из подчиненных серверов все еще доступен и способен обрабатывать пользовательские DNS-запросы. После возобновления работоспособности сервера, оба подчиненных сервера функционируют в штатном режиме:

Таким образом, в ходе проектирования и тестирования инфраструктуры удалось реализовать отказоустойчивую систему, способную оперативно обнаруживать неисправности в инфраструктуре. Также немаловажным фактором является реакция команды системных администраторов и технической поддержки data-центра, в условиях критических ситуаций важно проявить особую внимательность в решении проблем.

## 8 ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ

В разделе экспериментальных исследований описано исследование наиболее опасных критических уязвимостей в программном обеспечении, используемом в облачных средах, а также эксплуатация уязвимости CVE-2016-5195 в производственной среде. В подразделе эксплуатации уязвимости также описана защита от уязвимости и меры по предотвращению, мониторингу и оперативному реагированию на подобные инциденты.

### 8.1 Критические уязвимости в 2016 г.

Критические уязвимости 2016 г. в программном обеспечении [?], используемом в облачной среде представлено в табл. ??.

Таблица 8.1 – Наиболее опасные критические уязвимости 2016 г.

CVE ID	CVSS	Тип уязвимости	ПО
CVE-2016-5195	7.2	Получение привилегий	Linux Kernel
CVE-2016-6258	7.2	Получение привилегий	Xen
CVE-2016-5696	5.8	Получение данных	Linux Kernel
CVE-2016-3710	7.2	Запуск кода	QEMU
CVE-2016-8655	7.2	DoS, получение привилегий	Linux Kernel
CVE-2016-4997	7.2	DoS, получение привилегий, доступ к памяти	Linux Kernel
CVE-2016-4484	7.2	Получение привилегий	CryptSetup
CVE-2016-6309	10.0	DoS, запуск кода	OpenSSL
CVE-2016-1583	7.2	Переполнение стека, получение привилегий, DoS	Linux Kernel

Рассмотрим подробнее уязвимости из этой таблицы.

Опасная уязвимость CVE-2016-5195 «Dirty COW» обнаружена Филом Остером в ходе исследования зараженного сервера. Данная уязвимость присут-

ствовала в составе ядра Linux 10 лет, начиная с версии 2.6.22. Исправлена в октябре 2016 г [?].

Суть уязвимости состоит в том, что при чтении области данных памяти при использовании механизма copy-on-write (COW), используется одна общая копия, а при изменении данных — создается новая копия, а так называемый «Dirty Bit» указывает был ли изменен соответствующий блок памяти. Проблема возникает при одновременном вызове функции `madvise()` и записи в страницу памяти, к которой пользователь не имеет доступа на изменение. При многочисленном повторении запросов происходит «гонка» (race condition) и экспloit получает право на изменение страницы памяти, которая может относится к привилегированному `suid`-файлу.

Таким образом, с использованием эксплоитов можно повысить привилегии локального пользователя например до пользователя `root`. В выпущенном патче добавлен соответствующий флаг `FOLL_COW`, который является индикатором окончания операции COW:

Уязвимость в гипервизоре Xen — CVE-2016-6258 (XSA-182) позволяет привилегированному пользователю гостевой системы выполнить свой код на уровне хост-системы. Уязвимость применима только к режиму паравиртуализа-

ции и не работает в режиме аппаратной виртуализации, а также на архитектуре ARM.

В паравиртуализированных окружениях, для быстрого обновления элементов в таблице страниц памяти пропускались ресурсоемкие повторные проверки доступа. Данные проверки реализовывались с помощью очистки Access/Dirty битов, однако этого оказалось недостаточно [?]. В патче к уязвимости представлен код, в котором исправлены проверки доступов, а именно добавлены дополнительные повторные проверки:

Уязвимость CVE-2016-5696 в ядре Linux, позволяющая вклиниться в стороннее TCP-соединение была обнародована на конференции Usenix Security Symposium. Из-за недоработки механизмов ограничения интенсивности обработки ACK-пакетов, существует возможность вычислить информацию о номере последовательности, которая идентифицирует поток в TCP-соединении, и

со стороны отправить подставные пакеты, которые будут обработаны как часть атакуемого соединения [?].

Суть атаки заключается в наводнении хоста запросами для срабатывания ограничения в обработчике ACK-пакетов, параметры которого можно получить меняя характер нагрузки. Для атаки необходимо создать шум, чтобы определить значение общего счетчика ограничения интенсивности ACK-ответов, после чего на основании оценки изменения числа отправленных пакетов определить номер порта клиента и осуществить подбор номера последовательности для конкретного TCP-соединения.

В патче к этой уязвимости увеличен лимит TCP ACK и добавлена дополнительная рандомизация для снижения предсказуемости параметров работы системы ограничения ACK-пакетов:

Уязвимость CVE-2016-3710 «Dark portal» обнаружена в QEMU, который используется для эмуляции оборудования в Xen и KVM. При использовании метода эмуляции stdvga, из-за записи в регистр памяти VBE\_DISPI\_INDEX\_BANK, хранящий смещение адреса текущего банка видеопамяти, возможно обращение к областям памяти, выходящим за границы буфера, так как предлагаемые банки видеопамяти адресуются с использованием типа byte (uint8\_t \*), а обрабатываются как тип word (uint32\_t \*) [?]. Уязвимость

позволяет выполнить код на хост-система с правами обработчика QEMU (обычно root или qemu-dm).

В патче к уязвимости добавлены дополнительные проверки диапазона памяти:

Уязвимость в ядре Linux CVE-2016-8655 позволяет злоумышленнику запустить код на уровне ядра с использованием функции `packet_set_ring()` через

манипуляции с кольцевым буфером TRACERET\_V3 [?]. Использовать уязвимость можно для выхода за пределы контейнера, для этого необходимо чтобы локальный пользователь имел полномочия по созданию сокетов AF\_PACKET.

Устранена уязвимость в декабре 2016 г. с помощью кода, перехватывающий возможные гонки:

Уязвимость CVE-2016-4997 присутствует в подсистеме netfilter ядра Linux и связана с недоработкой в обработчике setsockopt IPT\_SO\_SET\_REPLACE и может быть использована в системах, использующих изолированные контейнеры [?]. Проблема проявляется при использовании пространств имен для изоляции сети и идентификаторов.

В патче к уязвимости была добавлена дополнительная проверка адреса функции xt\_entry\_foreach():

Уязвимость CVE-2016-4484 выявлена в пакете CryptSetup, применяемом для шифрования дисковых разделов в Linux. Ошибка в коде скрипта разблокировки позволяет получить доступ в командную оболочку начального загрузочного окружения с правами суперпользователя.

Несмотря на шифрование разделов возможны ситуации при которых некоторые разделы не шифруются (например /boot), таким образом возможно

оставить в системе исполняемый файл с правами setuid root для повышения привилегий или скопировать шифрованный раздел по сети для подбора пароля [?].

Для эксплуатации уязвимости необходимо удерживать клавишу Enter в ответ на запрос доступа к зашифрованным разделам. Спустя 70 секунд удерживания клавиши осуществляется автоматический вход в командную оболочку.

Проблема вызвана некорректной обработкой лимита на максимальное число попыток монтирования. Исправление доступно в виде загрузки GRUB с параметром «panic» или в виде патча, устанавливающего лимит:

Сотрудники компании Google выявили уязвимость CVE-2016-6309 в OpenSSL, позволяющая злоумышленникам выполнить произвольный код при обработке отправленных ими пакетов. При получении сообщения размером больше 16 Кб, при перераспределении памяти остается висячий указатель на старое положение буфера и запись поступившего сообщения производится в уже ранее освобожденную область памяти.

В патче опубликованном в сентябре 2016 г. исправлена проблема с висячим указателем:

Ядро Linux подвержено уязвимости CVE-2016-1583, благодаря которой существует возможность поднятия привилегий локальному пользователю при помощи eCryptfs.

С помощью формирования рекурсивных вызовов в пространстве пользователя возможно добиться переполнения стека ядра. Злоумышленник может организовать цепочку рекурсивных отражений в память файла, при которой процесс отражает в свое окружение другие файлы [?]. При чтении содержимого файлов будет вызван обработчик pagefault для процессов, что приведет к переполнению стека.

Соответствующие исправления были приняты в июне 2016 г. в ядре Linux:

## 8.2 Эксплуатация уязвимости ядра Linux CVE-2016-5195

Наиболее опасной уязвимостью 2016 г. является CVE-2016-5195 с кодовым именем «Dirty COW». Такая степень опасности обусловлена тем, что ей подвержены практически все ядра Linux начиная с версии 2.6.22, а также легкостью применения эксплоитов.

В данном разделе применяется экспloit [?], позволяющий получить права суперпользователя из-под локального пользователя.

Для эксплуатации используется дистрибутив CentOS:

Необходимо повысить привилегии локального пользователя dcow до суперпользователя root, для этого необходимо скачать экспloit и установить инструменты для компиляции (gcc/g++). После установки всех необходимых настроек компилируем код эксплоита:

После компиляции исходного кода эксплоита, в текущем каталоге появляется бинарный файл, запуск которого в автоматическом режиме позво-

ляет получить права доступа суперпользователя и сменить его пароль на «dirtyCowFun»:

Для исправления уязвимости в кратчайшие сроки для ядра Linux был внесен патч, а мейнтайнеры дистрибутивов опубликовали пакеты с исправлениями. Для обновления дистрибутива и устранения уязвимости необходимо скачать исправленную версию ядра и произвести перезагрузку.

В случае когда целый парк серверов не имеет возможности совершать перезагрузку необходимо использовать такие технологии как kpatch, livepatch, KernelCare. Подобные технологии позволяют применять патчи для ядра Linux без перезагрузки.

Технология KernelCare является коммерческим решением и позволяет без особых проблем в оперативном порядке использовать патчи для ядра, в том числе патч для CVE-2016-5195.

Пример эксплуатации уязвимости при использовании KernelCare:

Как видно из вывода команд, экспloit не работает при включенном KernelCare.

Пример отключения KernelCare и попытка эксплуатации уязвимости:

В облачной среде, где при каждой минуте простоя поставщик облачных услуг теряет деньги, использование подобных технологий позволяет существенно уменьшить время простоя серверов.

### 8.3 Мониторинг уязвимостей в программном обеспечении

Для своевременного реагирования на уязвимости в ПО, используемом в облачной среде необходим их мониторинг. В ходе исследования различных открытых баз уязвимостей и систем мониторинга не было обнаружено автоматизированных инструментов, позволяющих интегрировать поиск уязвимостей в систему мониторинга.

Для написания такой системы использовалась открытая база уязвимостей сайта [www.cvedetails.com](http://www.cvedetails.com) [?]. Сайт cvedetails позволяет в ограниченном режиме получить доступ к базе посредством JSON API.

Возможна интеграция программы с любой системой мониторинга или запуском по расписанию. Существует поддержка указания даты поиска уязвимостей, по умолчанию скрипт ищет уязвимости на сегодняшний день:

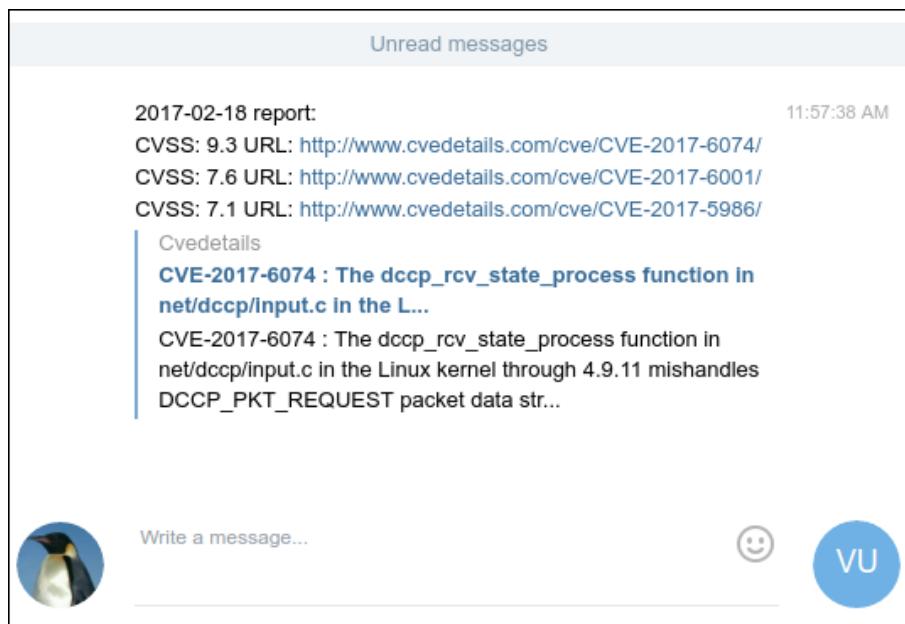


Рис. 8.1 – Уведомление программы в Telegram

Программа получает данные от сайта в JSON-формате вида:

Поддерживается интеграция приложения с мессенджером Telegram (рис. ??).

Описание кодов выхода программы представлено в табл. ??:

Таблица 8.2 – Коды выхода программы

Код	Сообщение	Отправлено в Telegram?
0	Уязвимости не найдены	Нет
1	Уязвимости найдены	Нет
2	Уязвимости найдены	Да
3	Уязвимости найдены	Нет, неверные токен и идентификатор

Исходный код программы представлен в прил. А.

## 9 АНАЛИЗ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

В ходе проведенной работы спроектировано программное средство с учетом поставленных требований.

Разработаны спецификация и архитектура программного средства, в рамках которых были описаны структура базы данных, классы и модули.

Разработан продукт минимальной жизнедеятельности согласно документации. Продукт может быть запущен в эксплуатацию при условии дополнительной разработки.

Данное программное решение является удобным инструментом для хранения и организации в автоматическом режиме загруженных фотографий. Целевой аудиторией являются люди, занимающихся производством фотоконтента.

## 10 БЕЗОПАСНОСТЬ ЖИЗНЕНДЕЯТЕЛЬНОСТИ

В разделе выполнен анализ условий труда администратора и их требованиям освещенности, электробезопасности, микроклимата, шума, требованиям к оборудованию, к организации рабочего места пользователя ПК.

### 10.1 Краткая характеристика помещения

Согласно санитарным нормам, ширина стола должна быть не менее 0.6 м, глубина не менее 0.8 м, также необходимо обеспечить расстояние между боковыми поверхностями мониторов не менее 1.2 м.

На рис. ?? изображена планировка и размещение оборудования на рабочем месте.

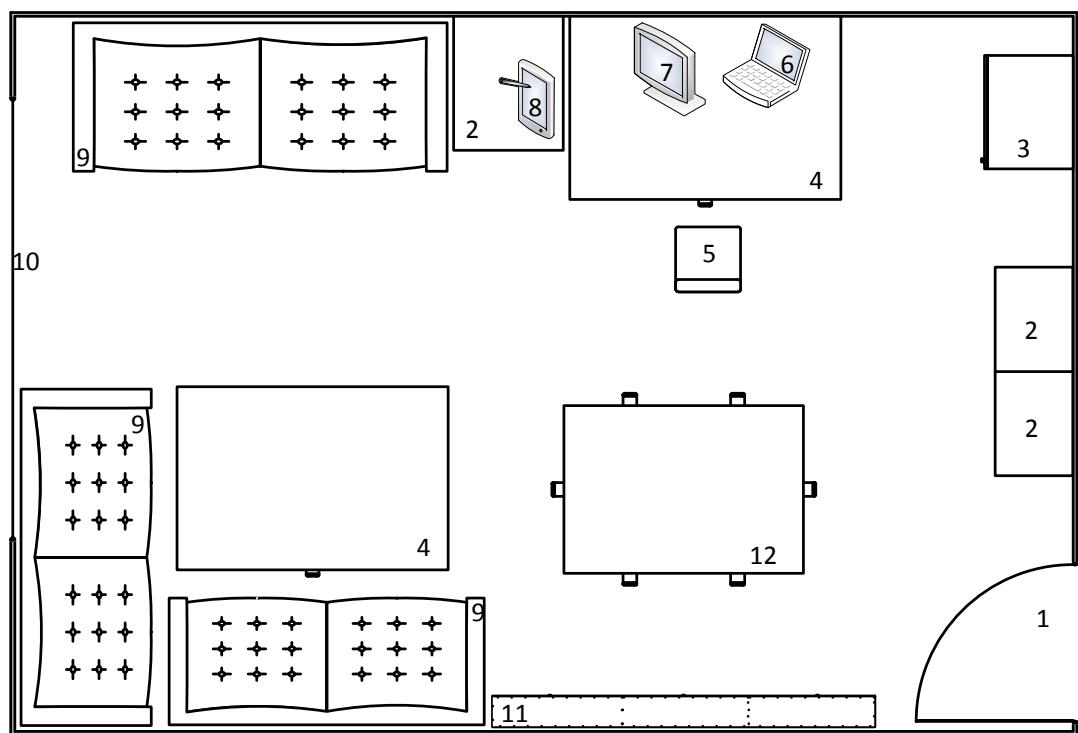


Рис. 10.1 – Планировка и размещение оборудования на рабочем месте  
1 — дверь; 2 — тумбочка; 3 — холодильник; 4 — стол; 5 — кресло; 6 — ноутбук; 7 — монитор; 8 — планшет; 9 — кровать; 10 — окно; 11 — шкаф; 12 — обеденный стол

## 10.2 Микроклимат

Метеорологические условия (микроклимат) характеризуются следующими параметрами:

- температурой воздуха;
- относительной влажностью;
- скоростью движения воздуха на рабочем месте;
- барометрическим давлением.

В комнате, где находится персональный компьютер, должен поддерживаться определенный температурный режим для нормальной эксплуатации ЭВМ и условий труда администратора.

Параметры воздушной среды в кабинете должны соответствовать требованиям ГОСТ 12.1.005-88 «Общие санитарно-гигиенические требования к воздуху санитарной зоны». При этом необходимо учитывать, что работа администратора относится к разряду легких работ (разряд 1а — затраты энергии до 150 ккал/час), а кабинет — к производственным помещениям.

В помещении имеются источники избыточного тепла:

- тепловыделение от ноутбука;
- тепло, выделяемое персоналом.

Тепловыделение от светильников отсутствует, так как используется люминесцентное освещение. Для поддержания оптимального уровня температуры используется как естественная вентиляция (через двери и окна путем проветривания), так и искусственная (при помощи вентилятора), так как в текущих условиях проживания невозможно установить кондиционер. Для обогрева помещения в зимнее время используется водяное отопление.

## 10.3 Освещение

В зависимости от необходимости, производственное освещение в кабинете может быть как естественным, создаваемым непосредственно солнцем и диффузным (рассеянным) светом, так и искусственным, осуществляемым

электрическими лампами. Естественное освещение характеризуется тем, что создаваемое освещение изменяется в очень широких пределах, в зависимости от времени года, дня и метеорологических факторов. При выборе норм естественного освещения учитывается разряд выполняемых работ, система освещения, коэффициент солнечности, коэффициент светового климата [?].

Мероприятия, за счет которых выполняются требования норм СП 52.13330.2011 «Естественное и искусственное освещение»:

- проверка, не реже одного раза в год, соответствия освещенности на рабочей поверхности нормам искусственного освещения;
- очистка светильников не реже одного раза в три месяца;
- протирка окон (стекол) не реже двух раз в год.

#### 10.4 Шум и вибрация

Источниками шума в помещении являются:

- непосредственно персональный компьютер (вентиляторы охлаждения процессора и видеокарты);
- разговорная речь;
- шум вне рабочей зоны.

Постоянный шум оказывает отрицательное воздействие на человека, как биологически, так и психологически, что отражается на качестве работы и общей производительности труда сотрудников. Снижается производительность труда и повышается количество допущенных ошибок, некоторые из которых могут быть критическими. Допустимый уровень звука — 50 дБА, при работающем оборудовании в кабинете ожидаемый уровень звука — 40-48 дБА.

#### 10.5 Пожаробезопасность

Пожар в помещении может возникнуть при взаимодействии горючих веществ, окислителя (условия пожара) и источников воспламенения (причина пожара). Горючие вещества в кабинете: деревянные столы, двери, полы

(паркет), покрытия стен, изоляция соединительных кабелей, жидкости для протирки узлов компьютера и другие.

Возможные источники и причины возникновения пожара:

- эксплуатация неиспользованного оборудования;
- неправильное применение электронагревательных приборов;
- неисправность проводки;
- короткое замыкание;
- нарушение правил пожарной безопасности.

Для отвода тепла от персонального компьютера необходимы работающие вентиляторы, помещение проветривается, поэтому кислород, как окислитель процессов горения, имеется в достаточном количестве. Исходя из этого, помещение кабинета, согласно нормам СП 2.13130.2012 «Системы противопожарной защиты». Обеспечение огнестойкости объектов защиты», по степени пожаробезопасности следует отнести к категории Д (помещения, в которых в обращении находятся негорючие вещества и материалы в холодном состоянии).

В качестве средств тушения пожара применяются углекислотные огнетушители, используемые для тушения электроустановок, находящихся под напряжением.

## 10.6 Электробезопасность

В кабинет электроэнергия поступает для питания персональных компьютеров и электрического освещения. Питание осуществляется от трехфазной сети переменного тока напряжением 380/220 В (+10..-15%) частотой 50 Гц (+1 Гц).

Поскольку помещение сухое (относительная влажность не более 75%), температура не превышает 30 °С, то, согласно ПУЭ 7 («Правилам устройства электроустановок»), оно не относится к категории помещений повышенной опасности. Однако возможна потенциальная опасность поражения людей электрическим током. Источниками и причинами опасности являются:

- открытые токопроводящие части оборудования, кабельной проводки;

- неисправность электрооборудования, электрических розеток;
- короткое замыкание в результате повреждения изоляции.

Для предотвращения поражения электрическим током потребителей электроэнергии в кабинете необходимо предусмотреть следующие технические мероприятия:

- все токопроводящие части оборудования и кабельной проводки должны быть защищены ограждающими кожухами;
- все металлические конструкции, которые могут оказаться под напряжением в результате короткого замыкания, должны быть заземлены, защищены и выполнено защитное отключение.

В качестве заземляющих проводников должны быть использованы элементы металлических конструкций, металлическое обрамление кабельных каналов. Здание должно быть оборудовано комплексом мер, предотвращающих попадание энергии молний в электрическую сеть, а также поражение людей, для чего на здание устанавливаются громоотводы.

Кроме технических, необходимо проведение организационных мероприятий:

- к работе с электроустановками допускаются только лица, прошедшие инструктаж и проверку знаний правил техники безопасности в соответствии с ГОСТ 12.1.009-76, ПТЭ и ПТБ;
- периодически осуществляется контроль сопротивления электрической изоляции токоведущих частей (в соответствии с требованиями ПУЭ 7, оно не должно быть ниже 0.5 м<sup>2</sup> по отношению к корпусу ЭВМ).

## 10.7 Эргономика и техническая эстетика

Эффективность работы администратора (программиста) во многом зависит от организации рабочих мест. Рабочее положение администратора — сидячее. Стул по возможности должен быть регулируемым по высоте, поскольку клавиатура и дисплей компьютеров должны находиться в зоне наилучшего

обзора. Для сохранения работоспособности имеет большое значение выбор основной рабочей позы.

Техническая эстетика позволяет снижать нервное утомление и вредные воздействия на функции организма в процессе труда. Огромное значение в эстетическом оформлении производства имеет цвет. Окраска, форма, внешний вид производственного помещения и оборудования улучшают условия освещения, а также психологическое состояние человека. Стены имеют светло-зеленый цвет, не вызывающий раздражения, потолок — белый цвет, что обеспечивает максимальное отражение света.

Рассматриваемое помещение соответствует требованиям ГОСТ 12.2.032-78 «Рабочее место при выполнении работ сидя. Общие эргономические требования».

## 10.8 Режим труда и отдыха

Работа администратора относится к категории работ связанных с опасными и вредными условиями труда. В процессе труда на администратора оказывают действие следующие опасные и вредные производственные факторы, физические:

- повышенный уровень статического электричества;
- повышенный уровень шума;
- повышенные уровни запыленности воздуха рабочей зоны;
- повышенная яркость светового изображения;
- повышенный или пониженный уровень освещенности;
- неравномерность распределения яркости в поле зрения;
- повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека.

Рациональный режим труда и отдыха — это правильное чередование работы и перерывов в ней в течение смены, суток, недели, года, устанавливаемое с целью обеспечения высокой производительности труда и сохранения здоровья работающих. Основным перерывом является перерыв на обед. Обеденный

перерыв при 8-часовой рабочей смене устанавливается продолжительностью не менее 30 мин через 4 часа после начала работы.

Режим отдыха складывается из нескольких компонентов:

- времени на гигиенические процедуры и личные надобности (2-3) от сменного времени независимо от вида труда;
- времени регламентированных перерывов на отдых (входят в состав рабочего времени), определяемого по показателю условий труда или по интегральному показателю снижения работоспособности;
- времени микропауз, а также времени обеденного перерыва (нерабочего времени), остающегося от приема пищи.

Режим труда и отдыха должен быть построен в соответствии с особенностями трудовой деятельности пользователей персонального компьютера и характером функциональных изменений со стороны различных систем организма работников.

## 10.9 Выводы

В ходе выполнения работы, была дана краткая характеристика помещения и выполняемых работ. Составлен план помещения и размещения оборудования. Были определены оптимальные параметры микроклимата, шума, освещения. Даны рекомендации по эргономике и режиму труда.

Наиболее неблагоприятными факторами являются микроклимат и искусственное освещение, обеспечиваемое люминесцентными лампами.

## ЗАКЛЮЧЕНИЕ

В ходе проведенной работы спроектировано программное средство с учетом поставленных требований.

Разработаны спецификация и архитектура программного средства, в рамках которых были описаны структура базы данных, классы и модули.

Разработан продукт минимальной жизнедеятельности согласно документации. Продукт может быть запущен в эксплуатацию при условии дополнительной разработки.

Данное программное решение является удобным инструментом для хранения и организации в автоматическом режиме загруженных фотографий. Целевой аудиторией являются люди, занимающихся производством фотоконтента.

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

ЦОД — центр обработки данных  
ПО — программное обеспечение  
GNU — проект по разработке свободного программного обеспечения  
GPL — General Public License, универсальная общественная лицензия  
ОЗУ — оперативное запоминающее устройство  
SSD — Solid State Drive, твердотельный накопитель  
NIST — National Institute of Standards and Technology, Национальный институт стандартов и технологий  
СХД — система хранения данных  
SaaS — Software as a Service, программное обеспечение как услуга  
PaaS — Platform as a Service, платформа как услуга  
IaaS — Infrastructure as a Service, инфраструктура как услуга  
ОС — операционная система  
SOA — service-oriented architecture, сервис-ориентированная архитектура  
AWS — Amazon Web Services  
GCE — Google Compute Engine  
OMG — Object Management Group  
ИТ — информационные технологии  
CSA — Cloud Security Alliance  
DMTF — Distributed Management Task Force  
SNIA — Storage Networking Industry Association  
OGF — Open Grid Forum  
OCC — Open Cloud Consortium  
OASIS — Organization for the Advancement of Structured Information Standards  
IETF — Internet Engineering Task Force, инженерный совет Интернета  
ITU — International Telecommunications Union, Международный институт электросвязи

ETSI — European Telecommunications Standards Institute, Европейский институт телекоммуникационных стандартов

ANSI — American national standards institute, Американский национальный институт стандартов

IDPS — Intrusion Detection and Prevention Systems, руководство по системам обнаружения и предотвращения вторжений

EC2 — Elastic Compute Cloud, веб-сервис компании Amazon, предоставляющий вычислительные мощности в облаке

API — Application Programming Interface, интерфейс создания приложений

vCPU — Virtual Central Processing Unit, виртуальное процессорное ядро

AMI — Amazon Machine Images

EBS — Elastic Block Store, сервис постоянного хранилища блочного уровня для использования с инстансами Amazon

SPI — Security Parameter Index, индекс параметра обеспечения безопасности

BGP — Border Gateway Protocol, протокол граничного шлюза

AS — автономная сетевая система

DNS — Domain Name System, система доменных имен

NTP — Network Time Protocol, протокол сетевого времени

SNMP — Simple Network Management Protocol, простой протокол сетевого управления

NDA — Non-disclosure agreement, соглашение о неразглашении

SSH — Secure Shell, безопасная оболочка

SQL — Structured Query Language, язык структурированных запросов

XSS — Cross-Site Scripting, межсайтовый скриптинг

VPN — Virtual Private Network, виртуальная частная сеть

МАИ — метод анализа иерархии

KVM — Kernel-based Virtual Machine, свободный гипервизор

ИС — индекс согласованности

СС — случайная согласованность

ОС — отношение согласованности

ЛПР — лицо принимающее решение

IoT — Internet of Things, интернет вещей

DDoS — Distributed Denial of Service, распределенная атака на отказ

SDN — Software-defined Networking, программно-определенная сеть

CVE — Common Vulnerabilities and Exposures, словарь известных уязвимостей

ID — IDentifier, идентификатор

CVSS — Common Vulnerability Scoring System, система оценки уязвимостей

COW — Copy-on-write, копирование при записи

ARM — Advanced RISC Machine, усовершенствованная RISC-машина

GRUB — GRand Unified Bootloader, загрузчик операционной системы

JSON — JavaScript Object Notation, текстовый формат обмена данными

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. O'Reilly T. What Is Web 2.0 // O'Reilly Media. 2005. URL: <https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html> (дата обращения: 20.05.2019).
2. Convolutional Neural Networks (LeNet) [Электронный ресурс] // DeepLearning 0.1 documentation: [сайт]. URL: <http://deeplearning.net/tutorial/lenet.html> (дата обращения: 19.05.2019).
3. Simonyan K., Zisserman A. Very Deep Convolutional Networks for Large-Scale Image Recognition // Computer Vision and Pattern Recognition, Apr 2015.
4. Russakovsky O., Deng J., Su H., Krause J., Satheesh S., Ma S., Huang Z., Karpathy A., Khosla A., Bernstein M., Berg A.C., Fei-Fei L. ImageNet Large Scale Visual Recognition Challenge // IJCV, 2015.
- Lin Y.P., Jung T.P. Improving EEG-Based Emotion Classification Using Conditional Transfer Learning // Frontiers in Human Neuroscience, Jun 2017.
5. Martin Ester, Hans-Peter Kriegel, Jörg Sander, Xiaowei Xu. A density-based algorithm for discovering clusters in large spatial databases with noise // Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD-96), AAAI Press, 1996.
6. Michael Cohen, Yin Tat Lee, Gary Miller, Jakub Pachocki, Aaron Sidford. Geometric median in nearly linear time // Proc. 48th Symposium on Theory of Computing (STOC 2016). — Association for Computing Machinery, 2016.
7. D. Eppstein, M. S. Paterson, Frances Yao. On nearest-neighbor graphs // Discrete and Computational Geometry. 1997. — Т. 17, вып. 3. — С. 263–282.
8. PostgreSQL 11.3 Documentation [Электронный ресурс] // PostgreSQL 11.3 Documentation: [сайт]. <http://www.postgresql.org/docs/current/interactive/> (дата обращения: 10.05.2019).

9. JDK 11. [Электронный ресурс] // openjdk.java.net: [сайт].  
<http://openjdk.java.net/projects/jdk/11/> (дата обращения: 10.05.2019).
10. Ю. Козмина, Р. Харроп, К. Шефер, К. Хо. Spring 5 для профессионалов // «Вильямс», 2019.
11. Паттерсон Дж., Гибсон А. Глубокое обучение с точки зрения практика // ДМК-Пресс, 2018.

## ПРИЛОЖЕНИЕ

ПРИЛОЖЕНИЕ А

ИСХОДНЫЙ КОД СКРИПТА DDOS DEFLATE













# ПРИЛОЖЕНИЕ Б

## РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

The screenshot shows a website with a navigation bar at the top. Below the navigation, there are four main service icons: 'Тарифы!' (Tariff) with a rocket icon, 'VPS-SSD!' with a server icon, 'DEDICATED!' with a server icon, and 'Партнёрка!' with a piggy bank icon. Each section contains descriptive text and a small note about discounts.

ШАРЕД ХОСТИНГ НА SSD ДИСКАХ!			
<b>Бинго 10</b> рублей <b>137</b> /месяц <i>При оплате за год скидка 15%!</i>	<b>Бинго 20</b> рублей <b>218</b> /месяц <i>При оплате за год скидка 15%!</i>	<b>Бинго 50</b> рублей <b>384</b> /месяц <i>При оплате за год скидка 15%!</i>	<b>Бинго 50</b> рублей <b>563</b> /месяц <i>При оплате за год скидка 20%!</i>

Рис. Б.1 — Список тарифов на сайте

The screenshot shows a step in the tariff selection process. It features a red banner with the text 'У НАС ЗАПРЕЩЕНО! - порно, вирусы, спам, варез и всё остальное, что запрещено законодательством РФ!' and a green banner with the text 'ТЕСТОВЫЙ ДОСТУП! - мы предоставляем тестовый доступ по Вашему запросу в биллинге!'. Below these banners, there are four large buttons labeled 'ЗАБРАТЬ' (Take). At the bottom, there is a 'Проверьте нас!' (Check us out!) button and a 'UP time 99.7%' status indicator.

Рис. Б.2 — Для выбора нужного тарифа необходимо нажать кнопку «ЗАБРАТЬ» под ним

**Регистрация**

У меня уже есть учетная запись [У меня уже есть учетная запись](#)

Язык интерфейса	Русский
Имя пользователя	Иван Иванов
Пароль доступа	*****
Подтверждение пароля	*****
E-mail адрес	test@example.com
Страна	Российская Федерация
Статус заказчика	Частное лицо
Контактное лицо (Ф.И.О.)	Иванов И.И.,
Откуда вы узнали о нас	Поисковые системы

**Ok**

Рис. Б.3 — Регистрация в биллинге для возможности заказа услуги

The screenshot shows the main interface of the BILL billing system. At the top, there is a navigation bar with icons for user profile, cart, and search, along with a message 'Ctrl + Shift + M'. Below the navigation bar, there are two main menu sections: 'Клиент' (Client) and 'Товары/Услуги' (Products/Services). The 'Клиент' section includes links for Profile, Cart, Orders, Coupons, and User Settings. The 'Товары/Услуги' section includes links for Virtual Hosting, Virtual Servers, Dedicated Servers, and Domains. The central content area is titled 'Нет заказов' (No orders) and contains a message stating that there are no unpaid or open orders. It also includes a button labeled 'Заказать услугу' (Order service). The top right corner of the interface shows a status message 'Нет заказов'.

Рис. Б.4 — Пример заказа услуги в биллинге

Выбор типа услуги

- Dedicated server
- Domain name
- Shared hosting
- VPS

Рис. Б.5 — Выбор типа услуги

Корзина

Xeon E3-1270 3.8Ghz (312.00 EUR в год)	312.00 EUR	Изменить	Удалить
--	------------	----------	---------

Итого: 312.00 EUR

Оплатить

Заказать услугу

Рис. Б.6 — Список услуг в корзине

Виртуальный хостинг

Id	Доменное имя	Тариф	Действует до	Состояние	Цена за месяц
87	gome.coffee	Host C	2015-06-20	Активен	3.00 EUR / Месяц

Рис. Б.7 — Список заказанных услуг в разделе хостинга

The screenshot shows a web application interface for managing expenses. At the top, there are tabs for 'Главная' (Home) and 'Расходы' (Expenses). Below the tabs, there is a title 'Расходы' with a small icon of a cash register. On the right side of the header, there are icons for refresh, star, and file. A search bar at the top right contains the text 'Ctrl + Shift + F'. The main content area is a table listing expenses:

Id	Наименование	Дата списания	Сумма	Не оплачено	Оплачено платежами
10	Телематические услуги - VPS Two #70 (pretty.one) , Месяц	2015-03-20	11.00 EUR	0.00 EUR	pfx/7
11	Телематические услуги - Host A #80, Полгода	2015-03-20	6.00 EUR	0.00 EUR	pfx/7

Рис. Б.8 — Список расходов на услуги

The screenshot shows a configuration window titled 'Настройки пользователя - devtest' (User Settings - devtest). The window is part of a larger interface with a sidebar containing various management links. The main form has fields for user information and settings:

Имя пользователя	devtest
Язык	Русский
Пароль	(empty field)
Подтверждение	(empty field)
Доступ к панели управления	С любого IP
Стартовая страница	Главная
Строк на странице	1000
Количество записей	5000
Вид кнопок	Значки и текст
Подсказки	Активные
Предупреждать о несохраненных полях на форме	(checkbox checked)
Уровень опыта пользователя	Новичок

At the bottom of the window are 'Ok' and 'Отмена' (Cancel) buttons.

Рис. Б.9 — Настройки пользователя хостинга

Главная Менеджер файлов

**Менеджер файлов /**

Создать Просмотр Изменить Атрибуты Антивирус Удалить Копировать Извлечь Архив Скачать Закачать Перейти Настройки Ctrl + Shift + F

Имя	Размер	Права	Владелец	Группа	Дата изменения
.ssh	4 KiB	755 [drwxr-xr-x]	devtest	devtest	2015-05-25 20:00:23
apsTmp	4 KiB	770 [drwxrwx--]	devtest	devtest	2015-05-27 15:26:00
binTmp	4 KiB	777 [drwxrwxrwx]	devtest	devtest	2015-05-17 09:06:13
email	4 KiB	751 [drwxr-x-X]	devtest	devtest	2015-02-20 14:06:36
etc	4 KiB	755 [drwxr-xr-x]	devtest	devtest	2015-04-21 18:57:37
logs	4 KiB	751 [drwxr-X-X]	devtest	devtest	2015-05-30 06:47:43
modTmp	4 KiB	770 [drwxrwx--]	www-data	devtest	2015-05-29 16:33:56
php-bin	4 KiB	751 [drwxr-x-X]	devtest	devtest	2015-05-28 18:01:02
www	4 KiB	751 [drwxr-X-X]	devtest	devtest	2015-05-27 15:26:00
tmp > modTmp	7	777 [lwxrwxrwx]	root	root	2015-05-26 19:05:05
.codepage	11	644 [-rw-r--r--]	devtest	devtest	2015-03-24 10:30:03

Рис. Б.10 — Файловый менеджер в панели управления хостингом

Главная FTP-пользователи

**FTP-пользователи**

Создать Изменить Удалить Вкл. Выкл.

Имя	Домашняя директория
devtest	/

Рис. Б.11 — Список FTP-пользователей

Каталог Web-скриптов

Web-скрипты, готовые к установке

Система	Версия	Описание	Установить
Drupal	7.37-55	Open source content management system and blogging engine	<a href="#">Установить</a>
Prestashop	1.6.0.9-84*	PrestaShop is the fastest, the lightest, and the most progressive Open Source e-commerce software.	<a href="#">Установить</a>
WordPress	4.2.2-106	WordPress — идеальная платформа для публикации, ориентированная на красоту, поддержку стандартов и удобство использования.	<a href="#">Установить</a>
joomla	3.2.3-6	Content management system and Web application framework	<a href="#">Установить</a>
phpBB	3.1.4-38	phpBB is the most widely used open source bulletin board solution in the world.	<a href="#">Установить</a>

(\*) - Web-скрипты имеют несколько версий пакетов, готовых к установке. Чтобы установить версию Web-скрипта, отличную от предлагаемой по умолчанию, воспользуйтесь кнопкой "Установить"

[Отмена](#)

Рис. Б.12 — Возможность установки популярных CMS из каталоге Web-скриптов

WWW-домены

Создать Изменить Удалить Скрипты Ошибки Редиректы Доступ Статистика Включить Выключить Каталог

Имя	Корневая директория	IP-адреса	Параметры
devtest1.ru	/www/devtest1.ru	188.127.255.177	
devtest2.ru	/www/devtest2.ru	188.127.255.177	
devtest3.ru	/www/devtest3.ru	188.127.255.177	
devtest4.ru	www/devtest4.ru	188.127.255.177	

Рис. Б.13 — Управление www-доменами

Резервные копии

Создать Восстановить Данные Скачать Закачать

План	Тип плана	Дата	Размер, MiB	Хранилище	Тип копии
Инкрементальный бэкап	Инкрементальный	2015-05-28 00:45:02 (2 дня, 18 часов назад)	357.83	ftpbackup	Инкрементальный
Инкрементальный бэкап	Инкрементальный	2015-05-27 00:52:09 (3 дня, 18 часов назад)	341.47	ftpbackup	Полный

Рис. Б.14 — Управление резервными копиями

Почтовые ящики

Имя	IP-адрес	Размер, Mb	Свойства
test@devtest2.ru	188.177.255.177	0 / 0	

Рис. Б.15 — Управление почтовыми ящиками

Контейнеры

Id	Наименование	Основной IP-адрес	Доменное имя	Шаблон ОС	Файловая система	Память, Mb	Размер диска, Mb	Состояние	Примечание
250	vm787	105.127.246.105	multi24play.ru	centos-6-x86_64	ploop	512	2000		

Рис. Б.16 — Список контейнеров в панели управления OpenVZ

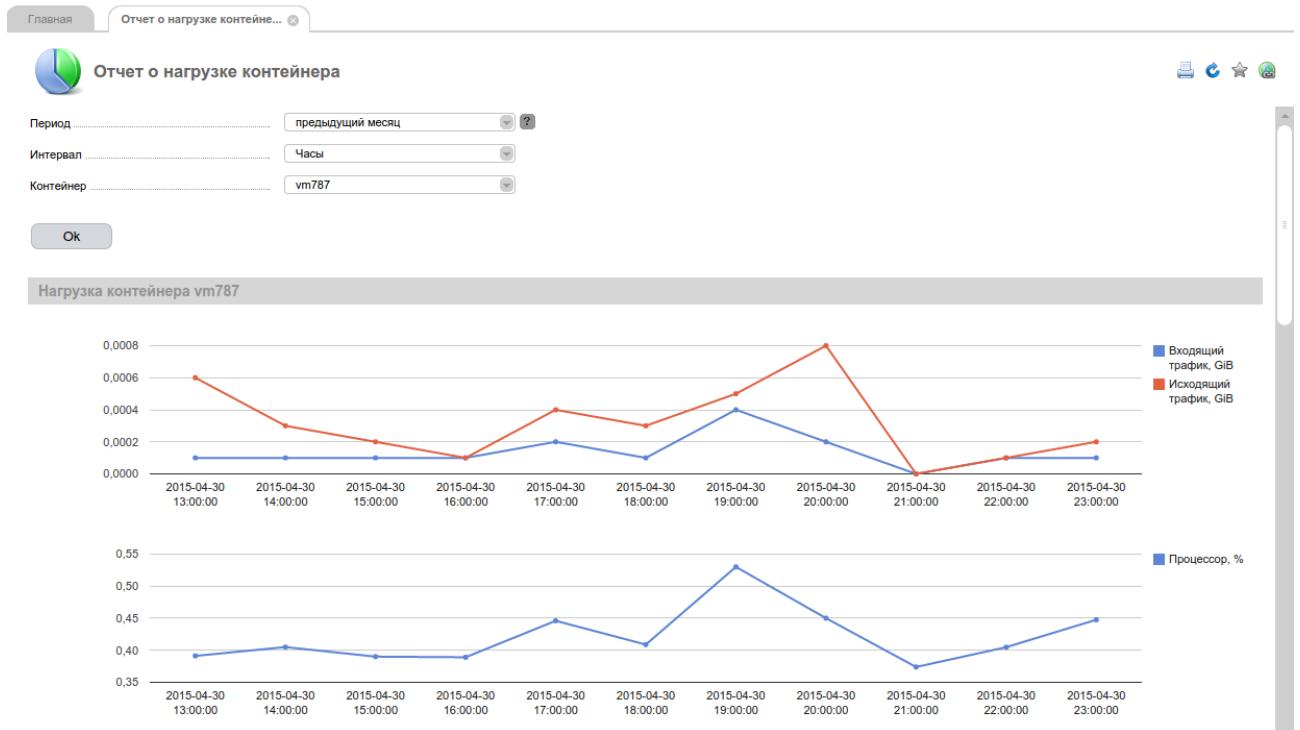


Рис. Б.17 — Отчет о нагрузке контейнера

Журнал посещений

Нажмите на заголовок, чтобы обновить данные

Время	Пользователь	Удалённый IP-адрес
2015-05-18 16:17:59	tpro	95.156.156.54
2015-05-13 16:10:12	tpro	95.215.158.220
2015-05-12 17:34:31	tpro	95.215.158.220
2015-05-12 17:34:31	tpro	95.215.158.220
2015-05-12 15:57:48	tpro	95.215.158.220
2015-05-05 16:24:14	tpro	95.215.157.152
2015-04-16 16:20:57	tpro	178.212.102.38
2015-04-10 00:47:27	tpro	171.212.97.171
2015-04-07 22:43:53	tpro	95.215.156.54
2015-04-07 19:10:23	tpro	95.215.156.54
2015-04-07 19:10:23	tpro	95.215.156.54
2015-04-07 18:21:28	tpro	54.215.156.54
2015-04-07 18:21:28	tpro	95.156.156.54
2015-04-07 18:09:59	tpro	54.215.156.54
2015-04-07 18:09:59	tpro	95.156.156.54
2015-04-07 18:04:52	tpro	54.215.156.54

Рис. Б.18 — Журнал посещений панели OpenVZ

Виртуальные машины

Создать	Изменить	Удалить	Старт	Стоп	Перезапуск	Переустановить	Пароль	Диски	Интерфейсы	IP-адреса	Информация	VNC	Ctrl + Shift + F
Id	Наименование	Доменное имя	Основной IP-адрес	Шаблон ОС	Память, МБ	Количество ядер	Размер дисков, МБ	Состояние					
137	testISP5	testisp5.ru	250.127.238.250	CentOS-6-amd64	1024	1	10000	Остановлено					

Рис. Б.19 — Список виртуальных машин в панели управления KVM

Список ISO-образов

Удалить	Id	Имя образа	Время удаления	Размер	Состояние
	1	debian-8.0.0-amd64-netinst.iso		246.00 MB	Готово
	2	CentOS-7-x86_64-Minimal-1503-01.iso		636.00 MB	Готово

Рис. Б.20 — Список ISO-образов

Голова с зеленым значком

Главная Список зап... > Запрос

 Запрос

Тема запроса ..... \* Недоступность сайта test.ru ?

Услуга ..... Host A #80 ?

Отдел .....  Technical ?  Sales

Текст сообщения \*

Здравствуйте.  
Сайт [test.ru](#) недоступен, пожалуйста найдите причину его неработоспособности.  
Спасибо.

Прикрепить файл ..... Screenshot.png Выберите файл ?

Прикрепить файл ..... Выберите файл ?

Отправить Отмена

Рис. Б.21 — Запрос к технической поддержке

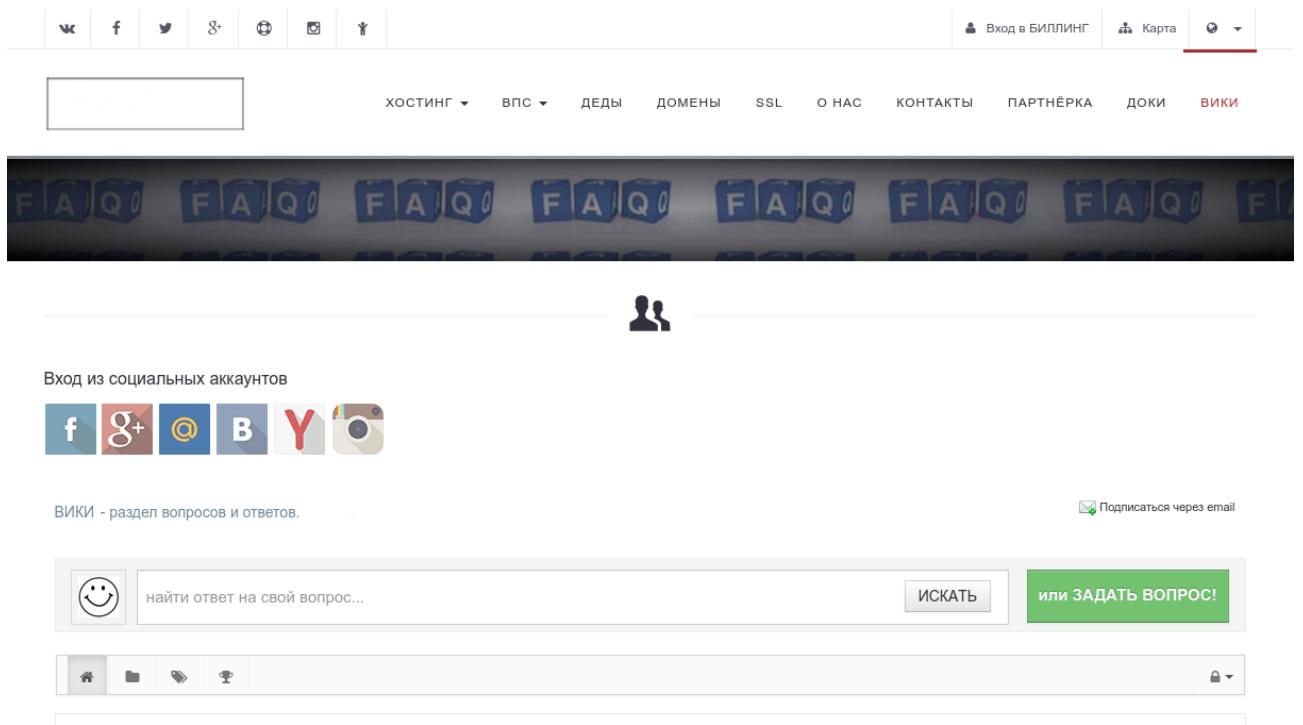


Рис. Б.22 — Регистрация в wiki

1C Bitrix - php.ini Вопрос

Шаред хостинг - общий хостинг

© Воскресенье, 12 Апр 2015

Приветствую. Подскажите какие параметры нужно прописать в php.ini чтобы заработал Битрикс ?

**Артем Трет'яков**  
Оффлайн

Битрикс bitrix 1c php.ini

Нравится Это сообщение понравилось пользователям Николай и Администратор

Ответы (1)

Старые первыми Самое последние Наибольшее число голосов Нравится

0

Administrator спросил(a):

Приветствую. Подскажите какие параметры нужно прописать в php.ini чтобы заработал Битрикс ?

Здравствуйте Артём.

Для корректной работы СУС Битрикс на шаред хостинге Бингхост, Вам нужно прописать в php.ini:

```
mbstring.func_overload=2
mbstring.internal_encoding=utf-8
```

И попросить дежурного админа перезагрузить apache.

Нравится Николай нравится это сообщение.

Рис. Б.23 — Пример вопроса в wiki

«УТВЕРЖДАЮ»

Генеральный директор Ильин А.А.

---

«09» апреля 2015г.

## АКТ

внедрения дипломной работы бакалавра, студента кафедры Информационных технологий и компьютерных систем Севастопольского государственного университета Умерова Амета Ремзиевича, на тему «Разработка виртуальной инфраструктуры для реализации облачных услуг», выполненной по специальности 09.03.01 — информатика и вычислительная техника.

Я, ниже подписавшийся, генеральный директор ООО «Информационные технологии» Ильин Антон Александрович, составил настоящий акт о том, что результаты дипломной работы бакалавра Умерова А.Р. использованы в прикладных разработках по созданию виртуальной инфраструктуры, для реализации облачных услуг в ООО «Информационные Технологии». В частности:

- использована свободная технология виртуализации OpenVZ;
- организован мониторинг и система резервного копирования контейнеров клиентов на базе свободного ПО;
- внедрена схема использования свободной панели VestaCP в клиентских контейнерах.

Данный акт не является основанием для взаимных финансовых расчетов.

(генеральный директор)

Ильин Антон Александрович