**Архитектура информационно-коммуникационной платформы электронного правительства**

**СОДЕРЖАНИЕ**

[1 Сокращения 5](#_Toc113022484)

[2 Термины и определения 6](#_Toc113022485)

[3 Соглашения 9](#_Toc113022486)

[4 Назначение документа 9](#_Toc113022487)

[5 Цели и задачи проекта Архитектура ИКП ЭП 9](#_Toc113022488)

[6 Используемые стандарты и НПА 11](#_Toc113022489)

[7 Текущая ситуация 11](#_Toc113022490)

[8 Функциональная архитектура ИКП ЭП 12](#_Toc113022491)

[9 Представление пользователя 13](#_Toc113022492)

[9.1 Роли пользователей Архитектуру ИКП ЭП 13](#_Toc113022493)

[9.2 Потребитель служб облачных вычислений 14](#_Toc113022494)

[9.3 Поставщик служб облачных вычислений 14](#_Toc113022495)

[9.4 Партнер службы облачных вычислений 15](#_Toc113022496)

[9.5 Модели развертывания облачных вычислений 15](#_Toc113022497)

[10 Функциональное представление 17](#_Toc113022498)

[10.1 Функциональная архитектура 17](#_Toc113022499)

[10.1.1 Многоуровневая архитектура 18](#_Toc113022500)

[10.2 Функциональные компоненты 18](#_Toc113022501)

[10.2.1 Функциональные компоненты уровня пользователя 24](#_Toc113022502)

[10.2.2 Функциональные компоненты уровня доступа 33](#_Toc113022503)

[10.2.3 Функциональные компоненты уровня службы 38](#_Toc113022504)

[10.2.4 Функциональные компоненты уровня ресурса 44](#_Toc113022505)

[10.3 Многоуровневые функции 55](#_Toc113022506)

[10.3.1 Функциональные компоненты систем безопасности 55](#_Toc113022507)

[10.3.2 Функциональные компоненты Big Data (анализ больших данных) 70](#_Toc113022508)

[10.3.3 Мониторинг 71](#_Toc113022509)

[10.3.4 Обеспечение отказоустойчивости 74](#_Toc113022510)

[10.3.5 Оркестрация облака 77](#_Toc113022511)

# Сокращения

| **Сокращение** | **Определение** |
| --- | --- |
| IT | Информационные технологии |
| SLA | Соглашение об уровне обслуживания |
| SSO | Единый сервис авторизации и аутентификации |
| ГО | Государственный орган |
| ЕТС ГО | Единая Транспортная Среда ГО |
| Заказчик | Акционерное общество «Национальные информационные технологии» |
| ИК-инфраструктура | Информационно-коммуникационной инфраструктура |
| ИКП ЭП | Информационно-коммуникационной платформа электронного правительства |
| ИКТ | Информационная и коммуникационная технология |
| ИС | Информационная система |
| ОС | Операционная система |
| РК | Республика Казахстан |
| РЦОД | Региональный ЦОД |
| СПП | Сервисный программный продукт |
| СУБД | Система управления базами данных |
| СХД | Система хранения данных |
| СЦ ГО | Серверный Центр государственных органов |
| ЦОД | Центр обработки данных |
| ЭА ИКП ЭП | Эталонная Архитектура ИКП ЭП |
| IaaS | Инфраструктура как услуга |
| PaaS | Платформа как услуга |
| SaaS | Программное обеспечение как услуга |

# Термины и определения

| **Термин** | **Определение** |
| --- | --- |
| API (application programming interface) | Набор готовых [классов](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D1%81%D1%81_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)), [процедур](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D0%B4%D1%83%D1%80%D0%B0_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)), [функций](https://ru.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)), [структур](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B0_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)) и [констант](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%81%D1%82%D0%B0%D0%BD%D1%82%D0%B0_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)), предоставляемых приложением (библиотекой, сервисом) или операционной системой для использования во внешних программных продуктах. |
| BI (Business intelligence ) | Методы и инструменты для перевода необработанной информации в осмысленную, удобную форму. |
| DC (Data Center) | Специализированное здание для размещения (хостинга) серверного и сетевого оборудования и подключения абонентов к каналам сети Интернет. |
| DevOps (development operations) | Набор практик, нацеленных на активное взаимодействие специалистов по [разработке](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B7%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%BA%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D1%8F) со специалистами по [информационно-технологическому обслуживанию](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%B4%D0%B5%D1%80%D0%B6%D0%BA%D0%B0) и взаимную интеграцию их рабочих процессов друг в друга. Базируется на идее о тесной взаимозависимости разработки и эксплуатации программного обеспечения и нацелен на то, чтобы помогать организациям быстрее создавать и обновлять программные продукты и услуги. |
| IT инфраструктура | Комплекс взаимосвязанных информационных систем и сервисов, обеспечивающих функционирование и развитие средств информационного взаимодействия предприятия. |
| JAVA | Типизированный [объектно-ориентированный язык программирования](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%8A%D0%B5%D0%BA%D1%82%D0%BD%D0%BE-%D0%BE%D1%80%D0%B8%D0%B5%D0%BD%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F), разработанный компанией [Sun Microsystems](https://ru.wikipedia.org/wiki/Sun_Microsystems). |
| Linux | Cемейство [Unix-подобных операционных систем](https://ru.wikipedia.org/wiki/Unix-%D0%BF%D0%BE%D0%B4%D0%BE%D0%B1%D0%BD%D0%B0%D1%8F_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) на базе [ядра Linux](https://ru.wikipedia.org/wiki/%D0%AF%D0%B4%D1%80%D0%BE_Linux), включающих тот или иной набор утилит и программ. |
| Rest (Representational State Transfer - «передача состояния представления») | [Архитектурный стиль](https://ru.wikipedia.org/wiki/%D0%90%D1%80%D1%85%D0%B8%D1%82%D0%B5%D0%BA%D1%82%D1%83%D1%80%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D1%8F) взаимодействия компонентов распределённого приложения в [сети](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C). REST представляет собой согласованный набор ограничений, учитываемых при проектировании распределённой [гипермедиа](https://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%BF%D0%B5%D1%80%D0%BC%D0%B5%D0%B4%D0%B8%D0%B0)-системы. |
| SDN (software-defined networking) | Сеть передачи данных, в которой уровень управления сетью отделён от устройств передачи данных и реализуется программно. |
| SLA (Service Level Agreement) | Термин методологии ITIL, обозначающий формальный договор между заказчиком услуги и её поставщиком, содержащий описание услуги, права и обязанности сторон и, самое главное, согласованный уровень качества предоставления данной услуги. |
| SSO (Single Sign-On) | технология, при использовании которой пользователь переходит из одного раздела портала в другой без повторной [аутентификации](https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F). |
| Бизнес-требование | Требование в терминах прикладной области (в терминах бизнеса), определяющее назначение ПО |
| Биллинг | Бизнес-процесс выставления счетов к оплате клиентам |
| Виртуализация | Технология, которая позволяет запускать экземпляры операционных систем параллельно (каждый в контексте виртуальной машины) на единственной физической машине, со своей обработкой ресурсов, распределенных между всеми виртуальными машинами |
| Виртуальная машина | Программная реализация компьютера, которая может быть использована подобно физическому компьютеру |
| Гипервизор | Программное или микропрограммное обеспечение, позволяющее виртуализировать системные ресурсы.  Существует два типа гипервизоров:  гипервизоры типа 1 и гипервизоры типа 2.  Гипервизоры типа 1 работают непосредственно на оборудовании системы. Гипервизоры типа 2 работают поверх базовой операционной системы, которая обеспечивает службы виртуализации, такие как поддержка устройства ввода/вывода и управление памятью. |
| Дашборд | Форма с лаконично представленными статистическими данными, отчетами, чаще всего с элементами инфографики. |
| Контейнер | Виртуализация на уровне операционной системы – это метод виртуализации, при котором ядро операционной системы поддерживает несколько изолированных экземпляров пространств пользователя, вместо одного. Эти экземпляры называются контейнерами. В контексте проекта Архитектуры ИКП ЭП, контейнеры предназначаются для размещения элементов инфраструктур ИС или СПП. Под элементами инфраструктуры ИС или СПП подразумевается ЛПО, сервисы, код приложений, входящих в их состав |
| Облачная платформа | Технологическое решение, основанное на модели облачных вычислений |
| Оркестрация облака | Автоматическое размещение, координация и управление ресурсами облачной Платформы. |
| Патч | Изменение ПО, устанавливаемое вне релиза, содержит в себе исправление обнаруженных дефектов, изменение или добавление нового функционала системы. |
| Релиз | Версия программного продукта, представляющая собой совокупность работ, направленных на модификацию программного продукта в течение ограниченного периода времени на основе фиксированного набора бизнес-требований и исправлений ранее найденных дефектов, предназначена для установки в продуктивную (промышленную) среду. |
| Архитектура | Фундаментальные концепции или свойства системы в ее окружении, воплощенные в ее элементах, отношениях и принципах их проектирования и эволюции |
| Деятельность | Заданная последовательность или совокупность задач. |
| Продукт служб облачных вычислений | Служба облачных вычислений, объединенная с совокупностью бизнес-понятий, в терминах которых предлагается служба облачных вычислений |
| Функциональный компонент | Функциональный строительный блок, необходимый для участия в деятельности, поддержанный реализацией. |
| Каталог продуктов | Список всех продуктов служб облачных вычислений, которые поставщики службы облачных вычислений предоставляют потребителям служб облачных вычислений |
| Роль | Набор деятельностей, служащих общей цели |
| Каталог служб | Список всех служб облачных вычислений конкретного поставщика служб облачных вычислений |
| Сторона | Физическое или юридическое лицо, объединенное или нет, либо группа таких лиц в любых сочетаниях. Стороны в системе облачных вычислений являются ее заинтересованными сторонами. |
| Программные продукты автоматизации государственных органов | ИС, СПП или любой другой программный продукт, разработанный по заказу государственного органа и цель которого автоматизация бизнес-процессов заказчика. |
| Партнер | Индивидуальный предприниматель или юридическое лицо, осуществляющие деятельность в сфере информационно-коммуникационных технологий в рамках создания и оказания информационно-коммуникационных услуг |
| Аттестационное обследование | Комплекс организационно-технических мероприятий, направленных на изучение, анализ, оценку технической документации объекта аттестации, обследование состояния организации работ по выполнению требований информационной безопасности. |

# Соглашения

1. В данном документе используется термин «ИКТ» и «Системы ИКТ», где аббревиатура ИКТ обозначает «информационно-коммуникационная технология», как определено в 3.1332 ISO/IEC/IEEE 24765. Данный термин используется для того, чтобы, прояснить, что архитектура покрывает не только технологии вычисления и хранения, связанные с компьютерными системами, но также и коммуникационные сети, которые связывают системы вместе.
2. Ссылки на термины, определенные в разделе 2 и ITU-T Y.3500 | ISO/IEC 17788, выделены жирным шрифтом.

# Назначение документа

Настоящий документ формализует описание ролей облачных вычислений в контексте проекта Архитектуры ИКП ЭП, функциональную архитектуру и функциональные компоненты облачных вычислений, необходимые для реализации проекта Архитектуры ИКП ЭП и служб облачных вычислений. Технические требования определены с учетом анализа и модели использования существующих ИК-инфраструктур Серверного Центра ГО и региональных ЦОД, а также планируемых проектов по расширению парка аппаратного обеспечения Заказчика.

Архитектура служит для следующих целей:

1. описания сообщества заинтересованных сторон облачных вычисленийв контексте проекта Архитектуры ИКП ЭП;
2. описания функциональной архитектуры ИКП ЭП
3. иллюстрации с целью облегчения понимания различных служб облачных вычислений, их предоставления и использования в контексте проекта Архитектуры ИКП ЭП.

# Цели и задачи проекта Архитектура ИКП ЭП

Национальный проект «Технологический рывок» ставит перед Оператором и Сервисным Интегратором новые, перспективные задачи:

* Направление 5.5: Создание инновационной экосистемы:
  + Задача 1. Поддержка площадок инновационного развития.
  + Задача 2. Развитие технологического предпринимательства, стартап культуры и НИОКР
  + Задача 3: Цифровизация внутренней деятельности государственных органов
  + Задача 4. Формирование спроса на инновации

Целью проектирования Архитектуры ИКП ЭП является разработка решения, ориентированного на предоставление полного комплекса услуг облачных вычислений для государственных органов.

В соответствии со стандартом ISO/IEC 17788-2016 облачные вычисления — это парадигма для предоставления возможности сетевого доступа к масштабируемому и эластичному пулу разделяемых физических или виртуальных ресурсов, обеспечивающая самообслуживание и администрирование по требованию.

Архитектуры ИКП ЭП предусматривает разделение общей ИТ-инфраструктуры на две изолированные облачные зоны, исходя из концепции разграничения по требованиям информационной безопасности и/или в зависимости от типов доступа пользователей. Одна из облачных зон предусматривает доступность сервисов для пользователей через ЕТС ГО, вторая – для пользователей с доступом через сеть Интернет. Взаимодействие между зонами осуществляется через ВШЭП.

Проектирование Архитектуры ИКП ЭП запланировано с целью реализации в автоматизированном виде бизнес-процессов, необходимых для эффективного оказания массовых облачных услуг, рассчитанных на весь рынок государственных заказчиков РК и на полный спектр необходимых им облачных услуг (используя которые, ГО могли бы осуществить максимальную автоматизацию своих бизнес-процессов, а также перенести существующие программные продукты в Архитектуру ИКП ЭП).

Реализация и внедрение Архитектуру ИКП ЭП позволит решить следующие задачи:

1. расширить список ИК-услуг, предоставляемых оператором и сервисным интегратором;
2. внедрить облачные инструменты управления инфраструктурами программных продуктов автоматизации государственных органов.
3. предоставить поставщикам программных продуктов автоматизации государственных органов среду управления проектами и их сопровождением по всему жизненному циклу, а также среду разработки и тестирования программных продуктов.
4. предоставить Оператору и Сервисному Интегратору среду коллективного взаимодействия для автоматизации задач, связанных с развитием, сопровождением и техническим обслуживанием ИКП ЭП.

Внедрение Архитектуру ИКП ЭП станет еще одной ступенью для развития информационно-коммуникационной платформы «электронного правительства».

Согласно национального проекта «Технологический рывок» должен быть осуществлен переход на платформенную модель (Мероприятие 3).

# Используемые НПА и стандарты

При разработке архитектуры Платформы использовались положения документов Системы государственного планирования, требования НПА и рекомендации следующих стандартов:

Основаниями разработки Концепции являются:

1. Национальный план развития Республики Казахстан до 2025 года утвержденный указом Президента Республики Казахстан от 15 февраля 2018 года № 636, (задача 3. Открытое правительство, будет внедрен платформенный подход, общенационального приоритета Республики Казахстан до 2025 года “Новая модель государственного управления”);
2. Общенациональные приоритеты Республики Казахстан до 2025 года, утвержденные указом Президента Республики Казахстан от 26 февраля 2021 года № 520 (общенациональный приоритет Республики Казахстан до 2025 года “Новая модель государственного управления”);
3. Концепция развития государственного управления в Республике Казахстан до 2030 года утвержденная указом Президента Республики Казахстан от 26 февраля 2021 года № 522 (тотальная цифровизация системы государственного управления);
4. Концепция развития отрасли информационно-коммуникационных технологий и цифровой сферы, утвержденная постановлением Правительства Республики Казахстан от 30 декабря 2021 года № 961 (перенос сервисов ГО на единую платформу GovTech, Цифровое управление (Government-to-Government, G2G) Применение платформенного подхода для совершенствования процессов взаимодействия с гражданами).

Концепция определяет цели и задачи, основные принципы перехода на платформенную модель цифровизации и архитектуру платформы, порядок перехода и создания платформы GovTech, основные составляющие ее элементы, а также общую оценку ожидаемых результатов и ожидаемого социально-экономического эффекта от ее создания.

Создание платформы GovTech должно обеспечивать:

Перенос сервисов ГО на единую платформу GovTech по результатам обследования информационно-коммуникационной инфраструктуры и объектов информатизации "электронного правительства";

Реализацию базовых платформенных сервисов, специализированных прикладных цифровых сервисов для осуществления автоматизации деятельности государственного органа, в том числе государственных функций и оказания вытекающих из них государственных услуг, с учетом обеспечения приоритетности создания и развития объектов информатизации "электронного правительства" и оказания информационно-коммуникационных услуг, а также прав на технологии, преимущественно принадлежащие казахстанским правообладателям;

Подключение государственных органов к цифровой платформе (информационным системам и ресурсам), между которыми обеспечено информационное взаимодействие

1. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года;
2. Требования по развитию архитектуры "электронного правительства", утвержденные приказом Министра информации и коммуникаций Республики Казахстан от 31 мая 2018 года № 239;
3. Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832;
4. Правила классификации объектов информатизации и классификатор объектов информатизации, утвержденные приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135;
5. Правила проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры, утверждённые Приказом Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ;
6. ГОСТ ISO/IEC 17788- 2016. Информационные технологии. Облачные вычисления. Общие положения и терминология.
7. ГОСТ Р ИСО/МЭК 17789. Информационные технологии. Облачные вычисления. Эталонная архитектура.
8. СТ РК ISO/IEC TS 27017. Информационная технология. Руководство по мерам информационной безопасности для использования сервисами облачных вычислений, основанное на стандарте ISO/IEC 27002.
9. ISO/IEC TS 27017. Свод практик по мерам защиты персональных данных при оказании публичных облачных услуг.
10. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

# Текущая ситуация

В настоящее время Оператором и Сервисным Интегратором предпринимаются усилия по развитию информационно-коммуникационной платформы «электронного правительства».

В рамках данных работ выполняются следующие работы:

1. Осуществляется проект по созданию консолидированной вычислительной площадки с применением технологии виртуализации для централизованного предоставления вычислительных ресурсов государственным органам на базе СЦ ГО и инфраструктуры РЦОД. Основной задачей проекта является предоставление услуг хостинга вычислительных мощностей на виртуальных серверах собственного оборудования Оператора, размещенного в СЦ ГО и РЦОД. Использование технологии виртуализации в СЦ ГО и РЦОД доказало возможность гибко и в кратчайшие сроки наращивать или уменьшать выделенные мощности, что необходимо при эксплуатации любой ИС.
2. Проводятся работы по переходу на сервисную модель информатизации, что влечет за собой увеличение объёмов общего потребления государственными органами ИТ-ресурсов, предоставляемых Оператором информационно-коммуникационной инфраструктуры.
3. Проводятся работы по изменению сетевой инфраструктуры, закуплено новое оборудование, которое позволило вывести сетевое взаимодействие на новый уровень (SDN сеть) – работы проводятся в СЦ ГО.

Перечисленные выше основные шаги по развитию текущей инфраструктуры и увеличению спроса на программные продукты автоматизации государственных органов, требуют новых механизмов как для управления предоставляемыми в аренду ГО виртуальными ресурсами (особенно в части автоматизации процессов сопровождения и администрирования) , так и для управления процессами разработки, тестирования и публикации программных продуктов автоматизации государственных органов. В частности, очень остро стоит вопрос по упрощению/ унификации процессов сопровождения программных продуктов автоматизации государственных органов, размещаемых в среде ИКП ЭП.

Проект Архитектуры ИКП ЭП должен консолидировать в себе уже начавшиеся процессы и новые задачи, стать логичным завершением процесса реформ облачной инфраструктуры Оператора.

# Функциональная архитектура ИКП ЭП

Создание Архитектуру ИКП ЭП регламентируется стандартом ГОСТ Р ИСО/МЭК 17789. «Информационные технологии. Облачные вычисления. Эталонная архитектура», который определяет эталонную архитектуру облачных вычислений (ЭАОВ). Эталонная архитектура включает роли облачных вычислений, деятельности облачных вычислений, а также функциональные компоненты облачных вычислений и отношения между ними.

Системы облачных вычислений могут быть описаны с различных точек зрения. Для использования в ЭАОВ были предложены четыре различных представления:

1. **представление пользователя;**
2. **функциональное представление;**
3. **представление реализации;**
4. **представление развертывания.**



Рисунок - Преобразования между архитектурными представлениями

Таблица 1 – Представления архитектуры в контексте проекта ИКП ЭП

|  |  |  |
| --- | --- | --- |
| **Представление** | **Описание представления** | **Документ, в котором детализировано представление** |
| Представление пользователя | Контекст системы, стороны, роли и деятельности облачных вычислений | Раздел 9 данного документа |
| Функциональное представление | Функции, необходимые для поддержания деятельностей облачных вычислений | Раздел 10 данного документа |
| Представление реализации | Функции, необходимые для внедрения служб облачных вычислений в пределах служебных частей и/или инфраструктурных частей | Раздел 10 данного документа. |
| Представление развертывания | Как функции служб облачных вычислений технически осуществлены в пределах уже существующих элементов инфраструктуры или в пределах новых элементов, которые будут введены в данной инфраструктуре. | В реализации требований пункта М1 технической спецификации, документе  «Аналитический отчет и рекомендации» |

# Представление пользователя

## Роли пользователей Архитектуру ИКП ЭП

Учитывая, что распределенные услуги и их предоставление являются сутью облачных вычислений, все деятельности, связанные с облачными вычислениями, разделяются на три основные группы: деятельности, использующие услуги, деятельности, предоставляющие услуги, и деятельности по поддержке таких услуг.

Данный подраздел содержит описания общих ролей, связанных с облачными вычислениями.

Важно отметить, что сторона может играть более одной роли в любой данный момент времени.

Как показано на рисунке 9.1 роли облачных вычислений представляют собой:

* потребителя служб облачных вычислений (см. 9.2);
* поставщика служб облачных вычислений (см. 9.3);
* партнера службы облачных вычислений (см. 9.4).



Рисунок - Роли облачных вычислений

## Потребитель служб облачных вычислений

Потребителем служб облачных вычислений Архитектуру ИКП ЭП являются государственные органы, сотрудники Сервисного Интегратора, сотрудники Оператора.

## Поставщик служб облачных вычислений

Поставщик служб облачных вычислений предоставляет доступ к службам облачных вычислений потребителям служб облачных вычислений.

Поставщик служб облачных вычислений ответственен за выполнение отношений с потребителями служб облачных вычислений, развитие и обслуживание облачной Платформы

Поставщиками служб облачных вычислений являются Сервисный Интегратор и Оператор

## Партнер службы облачных вычислений

Партнер службы облачных вычислений— сторона, которая поддерживает или помогает деятельности поставщика служб облачных вычислений или потребителя служб облачных вычислений, либо обеих служб.

В качестве партнера службы облачных вычислений будут выступать поставщики / разработчики программных продуктов автоматизации государственных органов.

## Модели развертывания облачных вычислений

Модели развертывания облачных вычислений — это способы организации облачных вычислений на основе управления и разделения физических или виртуальных ресурсов

Модели развертывания облачных вычислений согласно ГОСТ ISO/IEC 17788- 2016 включают в себя:

1. **Публичное облако**: Модель развертывания облачных вычислений, в которой службы облачных вычислений потенциально доступны любому потребителю службы облачных вычислений, и ресурсы управляются поставщиком службы облачных вычислений. Публичное облако может принадлежать, находиться под руководством и управляться академической, правительственной или бизнес-организацией, или любой их комбинацией. Данное облако функционирует на мощностях поставщика службы облачных вычислений. Фактическая доступность для определенных потребителей службы облачных вычислений может подлежать юридическому регламентированию. Публичные облака имеют очень широкие границы, где потребителю службы облачных вычислений предоставлен доступ к услугам публичного облака с немногими ограничениями, если таковые имеются:
2. **Частное облако**: модель развертывания облачных вычислений, в которой службы облачных вычислений используются исключительно единственным потребителем службы облачных вычислений, и ресурсами управляет тот же потребитель службы облачных вычислений. Частное облако может принадлежать, находиться под руководством и управляться самой организацией или третьим лицом, и ресурсы для функционирования облака могут находиться как у владельца, так и вовне. Потребитель службы облачных вычислений может также разрешить доступ другим сторонам для собственной выгоды. Частные облака стремятся установить строго управляемую границу вокруг частного облака, основанного на ограничении потребителей сотрудниками единственной организации;
3. **Общественное облако**: модель развертывания облачных вычислений, в которой службы облачных вычислений исключительным образом поддерживают определенное сообщество потребителей службы облачных вычислений и обслуживаются этим сообществом, и где ресурсами управляет, по крайней мере один член этого сообщества. Потребители службы облачных вычислений, входящие в сообщество, имеют общие требования и отношения друг с другом. Общественное облако может принадлежать, находиться под руководством и управляться одной или более организациями в сообществе, третьим лицом или некоторой их комбинацией, ресурсы для функционирования облака могут принадлежать сообществу или внешнему владельцу. Общественные облака ограничивают участие до группы потребителей службы облачных вычислений, у которых есть общий набор потребностей и задач, в отличие от открытых публичных облаков, при этом в общественных облаках участвуют более широкое количество потребителей, чем в частных облаках. Общие потребности и задачи включают, в частности, миссию, требования информационной безопасности, политику и этику.
4. **Гибридное облако**: Модель развертывания облачных вычислений, использующая, по крайней мере, две различные модели развертывания облачных вычислений. Включенные развертывания остаются при этом уникальными единицами, но связаны соответствующей технологией, которая обеспечивает функциональную совместимость (интероперабельность), переносимость данных и переносимость приложений. Гибридное облако может принадлежать, находиться под руководством и управляться самой организацией или третьей стороной, и может функционировать на ресурсах организации или вне нее. Гибридные облака представляют ситуации, в которых взаимодействия между двумя различным развертываниями могут быть необходимы, но остаются связанными через соответствующие технологии. Границы как таковые, установленные гибридным облаком, отражают два его основных развертывания.

Для реализации проекта Архитектуры ИКП ЭП сложно провести жёсткие границы и выбрать единственную возможную модель развертывания. В предлагаемой архитектуре сочетаются характеристики как публичного облака, так как к нему потенциально может получить доступ любой поставщик/ разработчик программных продуктов для использования среды облачной разработки и тестирования. В тоже время предоставление услуг облачных вычислений на коммерческой основе возможно только для государственных органов, что в большей степени соответствует модели развертывания «частное облако», но с поправкой, что потребителем услуг облачных вычислений является не одна организация, а группа организаций – государственные органы. В процессе развития Архитектуры ИКП ЭП не исключается ее интеграция с облачными решениями сторонних поставщиков, что является частью модели «гибридное облако».

Модель развертывания «гибридное облако» является одним из наиболее удобных вариантов для реализации проектов СПП, для которых поставщики будут предоставлять не только программное обеспечение, но и полностью программно-аппаратный комплекс, размещенный на мощностях поставщиков. В архитектурной диаграмме данная возможность обозначена на уровне пользователя как «Службы облачных вычислений партнеров» (Рисунки 5 и 6)

Облачные ресурсы партнеров облачных вычислений, интегрируемые в Архитектуру ИКП ЭП должны соответствовать нормам Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности (утв. ПП РК от 20 декабря 2016 года № 832) и СТ РК ISO/IEC TS 27017. «Информационная технология. Руководство по мерам информационной безопасности для использования сервисами облачных вычислений, основанное на стандарте ISO/IEC 27002».

# Функциональное представление

Функциональное представление — это представление о функциях, необходимых для оказания услуг облачных вычислений в соответствии с целями и задачами облачной Платформы. В контексте проекта Архитектуры ИКП ЭП это описание функциональности, предоставляемой модулями и компонентами ИКП ЭП потребителям услуг облачных вычислений.

Функциональная архитектура также определяет зависимости между функциями.

Функциональное представление обращается к таким понятиям облачных вычислений как:

* функциональные компоненты;
* функциональные уровни;
* многоуровневые функции.

На рисунке ниже представлены понятия функций, слоев и компонентов.

* 

Рисунок - Функциональное иерархическое представление

## Функциональная архитектура

Функциональная архитектура для ИКП ЭП описывает реализацию служб облачных вычислений как совокупность функциональных компонентов высокого уровня.

Функциональная архитектура описывает функциональные компоненты в терминах многоуровневого представления, где определенные типы функций сгруппированы в каждый уровень и между компонентами в последовательных слоях есть интерфейсы.

### Многоуровневая архитектура

У многоуровневого представления, используемого в архитектуре ИКП ЭП, предусмотрены четыре уровня, а также ряд функций, которые проходят через эти уровни:

* уровень пользователя;
* уровень доступа;
* уровень службы;
* уровень ресурсов.

Функции, которые охватывают все уровни, называются многоуровневыми функциями. Структура многоуровневого представления показана схематически на рисунке ниже.



Рисунок - Структура многоуровневого представления облачных вычислений

## Функциональные компоненты

Данный раздел описывает архитектуру ИКП ЭП с точки зрения общего набора **функциональных компонентов облачных вычислений**. **Функциональный компонент** — функциональный элемент архитектуры, который используется для осуществления определенной **деятельности** или части **деятельности,** и у которого есть реализационный артефакт в конкретной реализации архитектуры, например, компонент программного обеспечения, подсистема или приложение.

На рисунках ниже представлен высокоуровневый обзор **функциональных компонентов** архитектуры, организованных в многоуровневую инфраструктуру с учетом доступа из двух зон:

1. Интернет – доступ к ИКП ЭП посредством публичных сетей
2. ЕТС ГО – доступ к ИКП ЭП из закрытой сети государственных органов

Набор доступных функциональных компонентов отличается в зависимости от зоны из которой осуществляется доступ. Для размещения компонентов программных продуктов автоматизации государственных органов предусмотрено также использование РЦОД.

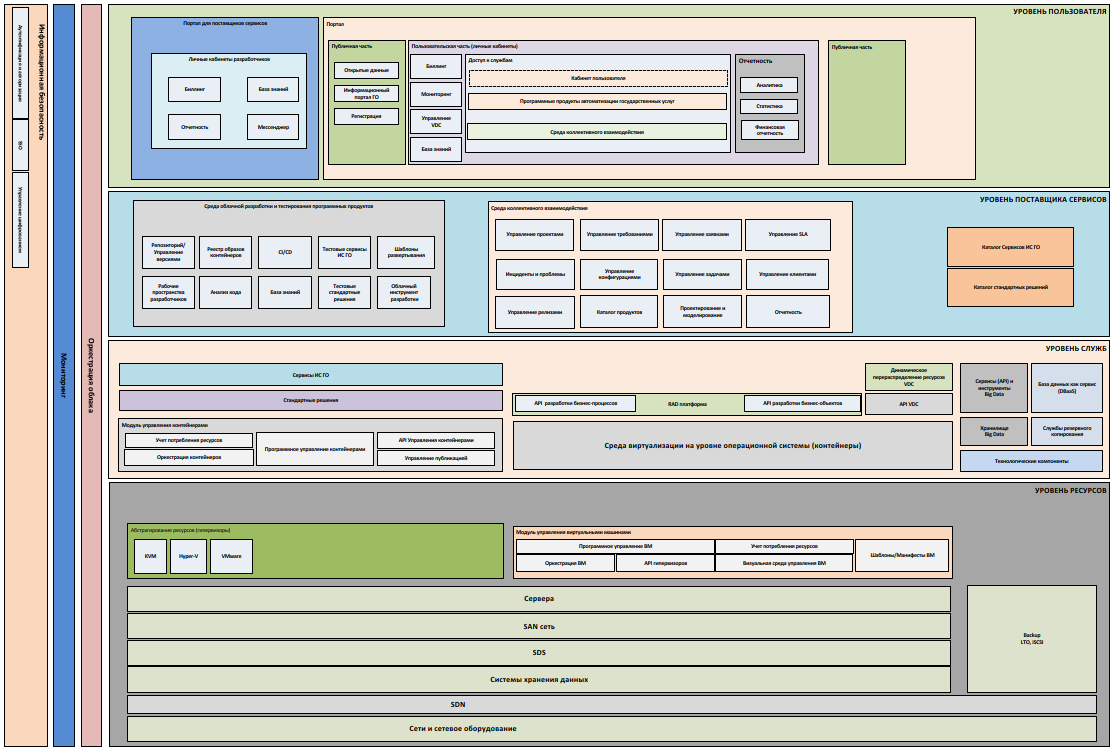


Рисунок – Детализация многоуровневого представления функций ИКП ЭП (доступ через Интернет)

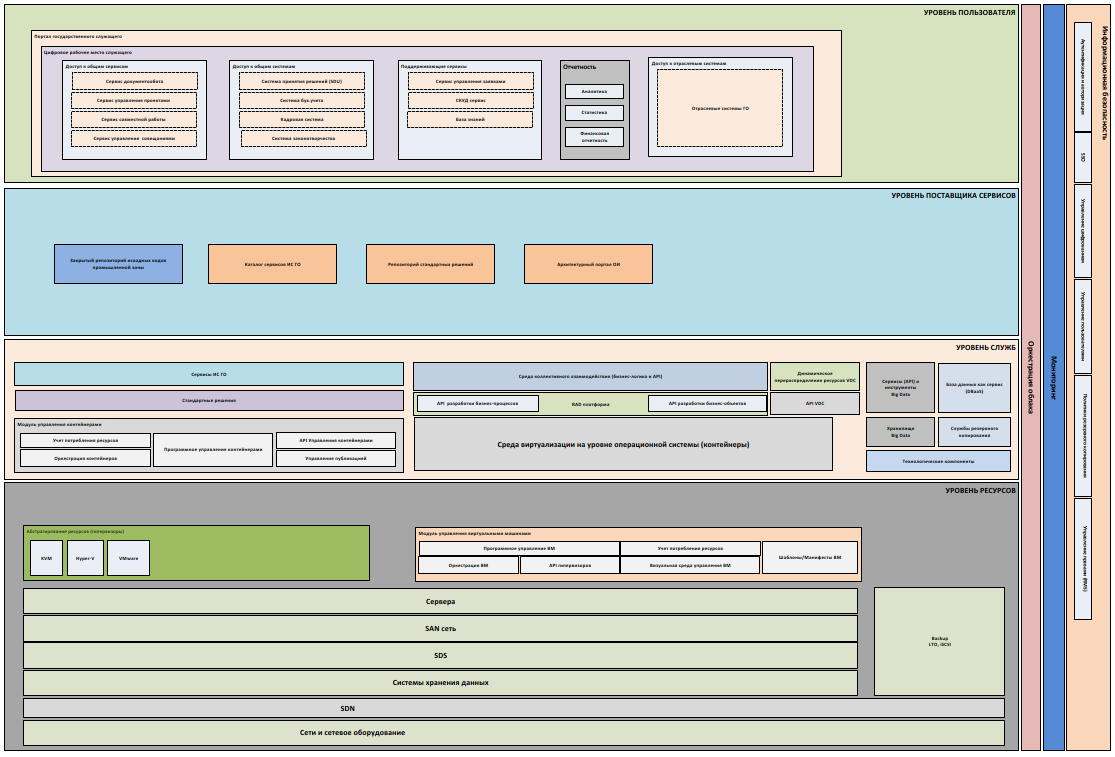


Рисунок 6 – Детализация многоуровневого представления функций ИКП ЭП (доступ через ЕТС ГО)



Рисунок 7 – Взаимодействие между зонами ИКП ЭП



Рисунок 8 – Компоненты ИКП ЭП на уровне РЦОД

Уровень РЦОД предназначен для размещения функциональных компонентов программных продуктов автоматизации государственных органов, для обеспечения доступа к ним из регионов. Данная возможность предоставляется с целью децентрализации доступа , оптимизации нагрузки на функциональные компоненты программных продуктов автоматизации государственных органов

### Функциональные компоненты уровня пользователя

Уровень пользователя — это пользовательский интерфейс, через который потребитель служб облачных вычислений взаимодействует с поставщиком служб облачных вычислений и службами облачных вычислений (функциями ИКП ЭП и программными продуктами автоматизации государственных органов). На уровне пользователя расположены компоненты:

1. Для неавторизованных пользователей
2. Для авторизованных пользователей

На уровне пользователя расположены компоненты, обеспечивающие переход пользователя на уровень доступа, такие как например, личный кабинет, в котором для каждого пользователя определяется набор доступных ему компонентов. Уровень пользователя предназначен для перехода на уровень доступа и состоит из легковесных веб интерфейсов, обеспечивающих данный переход

На рисунке ниже представлены функциональные компоненты уровня пользователя.



Рисунок 8 - Функциональные компоненты уровня пользователя

**Функциональные компоненты** уровня пользователя включают:

1. Портал
2. Доступ к программным продуктам автоматизации государственных органов
3. Доступ к среде коллективного взаимодействия
4. Доступ к службам облачных вычислений партнеров
5. Доступ к управлению виртуальными машинами
6. Доступ к отчетности
7. Доступ к информационным панелям (дашбордам) Единой Системы Мониторинга
8. Среда разработки и тестирования программных продуктов
9. Регистрация в качестве пользователя Архитектуры ИКП ЭП

Пользователи служб облачных вычислений будут работать с публичной или закрытой частью портала, посредством SSO проходить авторизацию и аутентификацию и в соответствии с правами получать доступ к программным продуктам, размещенным в ИКП ЭП и ее управляющим компонентам.

Дополнительным требованием к развитию ИКП ЭП будет являться реализация платформы с максимальным использованием open-source решений№

Использование платных решений должно быть разрешено только по согласию ГО (Владельца), Системного интегратора и Оператора.

#### Портал

Основная цель – обеспечение единой точки входа для внешних и внутренних пользователей. Портал будет состоять из закрытой и публичной части.

Портал должен предоставлять следующую функциональность:

1. Портал самообслуживания;
2. Рабочая среда обмена знаниями;
3. Динамические (Web 2.0) сайты;
4. Закрытая часть;
5. Публичная часть.

##### Управление контентом и web-публикациями

Встроенная система управления контентом должна представлять собой структурированное решение с поддержкой рабочих процессов на базе ролей, разделения формы и содержания, а также процессов утверждения и управления версиями. Библиотеки документов должны поддерживать управление версиями, блокировку документов и автоматизированную конвертацию типов файлов для совместной работы над документами. Должны быть совместимы с протоколом WebDAV и могут интегрироваться с приложениями Microsoft Office для динамического обмена документами. При этом для хранения контента могут применяться и системы сторонних разработчиков.

##### Совместная работа

В комплект инструментов для совместной работы Портала должны войти доски сообщений, блоги. Все они должны поддерживать экспорт в RSS, присвоение тегов, общие метаданные и социальные закладки — и совместимы с гибкой системой групп пользователей, организаций и сайтов. Эти инструменты позволят вести плодотворные дискуссии, осуществлять обмен знаниями. Пользователи смогут не просто управлять процессом своей работы благодаря встроенному почтовому клиенту и персональным календарям, но и сообщать своим коллегам о своих находках и таким образом быть членом команды.

##### База знаний

Встроенная функциональность базы знаний позволяет реализовать любые проекты, любой сложности, также поддерживаются информационные ресурсы построенные на базе технологии WIKI.

##### Зоны портала

Портал состоит из двух зон: публичной, доступной всем пользователям и закрытой, доступной только зарегистрированным пользователям в соответствии с их правами.

Функционал публичной зоны:

1. Новости – новостной раздел портала
2. Каталог продуктов – каталог продуктов и услуг, оказываемых поставщиком облачных вычислений
3. Регистрация – регистрационные формы для потребителей облачных услуг и для партнеров службы облачных вычислений

Функционал закрытой зоны:

1. Личный кабинет пользователя
   1. Отчетность – статистика потребления услуг, аналитические и финансовые отчеты, связанные с потреблением услуг
   2. Интерфейс SSO – интерфейс, позволяющий переключаться между программными продуктами, размещенными в ИКП ЭП и сервисами компонентов платформы, в соответствии с правами пользователя
   3. Доступ к среде коллективного взаимодействия
   4. Доступ к программным продуктам партнеров – получение доступа к продуктам, размещенным в других облачных средах (в соответствии с моделью «гибридное облако»
2. Доступ к управлению виртуальными дата-центрами (10.2.1.1.5)
3. Биллинг – работа со счетами (раздел 10.2.1.1.6)
4. Мониторинг - просмотр результатов мониторинга и аудита (раздел 10.2.1.1.7)
5. База знаний (раздел 10.2.1.1.8)

##### Управление виртуальным дата-центром (VDC)

Виртуальный дата-центр в контексте проекта Архитектуры ИКП ЭП – это набор арендованных у поставщика служб облачных вычислений виртуальных ресурсов. Виртуальные ресурсы это:

1. Сервера
2. Сети
3. СХД

Которые объединены в логический пул. Потребитель может организовать арендованные ресурсы в один пул, в тоже время он может разделить арендованные ресурсы на несколько логических пулов (дата-центров), например, для разделения ресурсов между размещаемыми на них информационными системами или другими продуктами автоматизации государственных органов.

Компонент «Управление виртуальными дата-центрами» предоставляет потребителю услуг облачных вычислений набор интерфейсов для управления арендованными виртуальными ресурсами, а также для взаимодействия с поставщиком служб облачных вычислений в части сопровождения и технической поддержки арендованных ресурсов.

Компонент предоставляет доступ к интерфейсам управления дата-центрами пользователя, данный функционал предусматривает:

* 1. Просмотр карт дата-центров
  2. Управление пулами ресурсов (дата-центрами)
  3. Оформление заявки на предоставление виртуальных аппаратных ресурсов
  4. Оформление заявки на предоставление сетевых соединений
  5. Оформление заявки на изменение конфигураций существующих виртуальных машин
  6. Оформление заявки на изменение существующих сетевых соединений

Карта дата-центра – это визуальный инструмент, на котором пользователь видит сервера входящие в состав дата-центра, СХД и сети, может просматривать их спецификации и оформлять заявки на изменение существующих ресурсов и добавление новых.

##### Биллинг

Биллинг - это одна из ключевой функциональности облачных решений, реализующая такую особенность ИКП ЭП как - измеримое обслуживание.

Биллинг обеспечивает автоматизацию бизнес-процессов по заказу и потреблению услуг, выписке счетов, проведению оплат и контролю сопутствующего документооборота.

Функционал состоит из следующих возможностей:

1. Хранение договора клиента и ведение его баланса
2. Хранение услуг и ведение их стоимости
3. Проведение начислений за предоставленные услуги
4. Изменения стоимости услуг
5. Проведение платежей
6. Перевод денежных средств с договора на договор
7. Ввод остатков по клиентам при переносе их из другой системы
8. Хранение выставленных счетов клиенту
9. Погашение выставленных счетов

Это необходимый минимум для корректного проведения начислений за услуги и учета денежных средств.

Каждый пользователь настраивает для себя определенный набор услуг в личном кабинете, а также конфигурирует виртуальный ЦОД или ЦОДы.

Система биллинга будет ежемесячно формировать счет на аренду виртуализированных аппаратных ресурсов и услуг ИКП ЭП согласно тарификатора. Счета будут доступны пользователям в соответствующем разделе личного кабинета.

Согласно законам, бюджеты ГО формируются на будущий год целиком поэтому классическая структура биллинга будет противоречить законодательству. Но при этом государственный орган может уменьшать или увеличивать необходимое ресурсы. В случае уменьшения ГО будет формировать экономию. Увеличивать же ресурсы ГО сможет только в рамках утвержденного бюджета.

Функциональность биллинга предполагает наличие каталога услуг и наличие функций, которые учитывают использование услуг пользователями.

На первом этапе реализации Платформы биллинг будет сервисом, требования к которому будет вырабатываться эмпирическим путем в период разработки и функционирования Платформы.

В данное время предполагается что биллинг будет выступать больше как учетная система, которая подтверждает, что заказчику были предоставлены услуги в полном объеме и контроля невыхода за рамки бюджета в части потребляемых мощностей и количества услуг. Такой подход связан из-за наличия двух проблем наличия со стороны заказчика контроля, что ему оказали услуги в полном объеме и контроля со стороны поставщика, что не предоставлено больше, согласно заявленного лимита.

В личном кабинете раздела биллинга которые обеспечит возможности для пользователя:

1. контроля бюджета;
2. состав инфраструктуры;
3. количества потребления услуг.

Предполагается наличие административной части биллинга в личном кабинете, которая позволяет выбрать пользователю вид услуги, период использования и формирование отчетности в различных срезах, например, по видам услуг или использование услуги за определенный период времени.

##### Мониторинг (доступ к информационным панелям Единой Системы Мониторига)

Посредством SSO пользователь получает доступ к информационным панелям (дашбордам) Единой Системы Мониторинга. ИКП ЭП не имеет собственной системы мониторинга, ее компоненты поставляют логи и метрики в Единую Систему Мониторинга Оператора, в данном разделе портала пользователь получает доступ к информации по мониторингу его виртуальных дата-центров (VDC) и программных продуктов автоматизации государственных органов принадлежащих ему и размещенных на ресурсах Архитектуры ИКП ЭП

##### База знаний

Центральная wiki подобная база знаний, содержащая информацию по работе с ИКП ЭП, ее сервисам и компонентам.

#### Доступ к программным продуктам автоматизации государственных органов

Доступ к информационным системам и СПП в соответствии с правами доступа пользователя. В ИКП ЭП используется единая точка входа SSO, как следствие пользователь, прошедший процедуры аутентификации и авторизации, получает список доступных ему информационных систем и СПП в соответствующем разделе закрытой зоны портала и может переключаться между ними без прохождения дополнительной аутентификации и авторизации в соответствии с правами доступа, представленными ему для работы в информационной системе и СПП.

#### Доступ к среде коллективного взаимодействия

Переход к функциям среды коллективного взаимодействия расположенным на уровне доступа в соответствии с правами пользователя. Доступен при работе в зоне ЕТС ГО

#### Доступ к службам облачных вычислений партнеров

В ИКП ЭП предусмотрена техническая возможность интеграции служб облачных вычислений партнеров. В соответствии с моделью развертывания «Гибридное облако». Данная возможность может быть использована в процессе развития ИКП ЭП, для расширения списка предоставляемых облачных услуг за счет функциональности облачных решений сторонних вендров. Доступ к службам облачных вычислений партнеров предоставляется в ИКП ЭП только при доступе к ней через Интернет.

В качестве служб облачных вычислений партнеров могут выступать СПП, размещенные на облачных ресурсах поставщиков. Данная модель развертывания СПП крайне удобна, в случае, когда поставщик СПП отвечает не только за программную часть, приложение, но поставляет комплексное решение, программно-аппаратный комплекс.

#### Доступ к управлению виртуальными машинами

Доступ администратора Оператора к визуальным средам управления виртуальными машинами. В данном случае речь идет о служебных визуальных инструментах, не управлением виртуальным дата центром (VDC). Для работы с VDC предусмотрен отдельный компонент, описанный в разделе 10.2.1.1.6. Доступ к управлению виртуальными машинами предоставляется только в зоне ЕТС ГО.

#### Доступ к отчетности

Специализированный раздел закрытой зоны портала, в котором пользователь получает доступ к набору статистических и аналитических отчетов, содержащих информацию о его активности или активности его подразделений или государственного органа (в соответствии с правами доступа пользователя) в части использования сервисов ИКП ЭП. А также в данном разделе находится специализированная секция для финансовой отчетности генерируемой на основе информации модуля «Биллинг»

#### Регистрация

Функциональный компонент предоставляющий возможность регистрации в качестве пользователя Архитектуру ИКП ЭП. Пользователь может зарегистрироваться как:

1. Сотрудник государственного органа
2. Поставщик/разработчик программного обеспечения
3. Сотрудник Сервисного Интегратора
4. Сотрудник Оператора

Для каждого типа пользователей должна быть разработана своя форма регистрации и свой процесс проверки регистрационных данных и предоставления прав доступа. Формы и процессы согласуются с Заказчиком на этапе реализации проекта Архитектуры ИКП ЭП и реализуются средствами «Среды коллективного взаимодействия» модуля «Управления заявками».

После прохождения процедуры подачи заявки на регистрацию, пользователь получает временный доступ на Портал где ему доступна возможность просмотра статуса заявки на регистрацию.

Процесс регистрации доступен в обеих зонах ИКП ЭП: Интернет и ЕТС ГО. Аутентификация и авторизация пользователей проводится через сервисы ИКП ЭП опубликованные на ВШЭП.

#### Среда облачной разработки и тестирования

Среда облачной разработки и тестирования подробно описана в документе «Архитектура среды разработки и тестирования». В контексте данного документа кратко указаны ее функции.

Среда разработки и тестирования предназначена для автоматизации полного цикла разработки программных продуктов автоматизации государственных органов. От появления требования до публикации в промышленной зоне и переходу на техническую поддержку.

На уровне пользователя размещены следующие компоненты облачной среды разработки и тестирования:

1. Личные кабинеты разработчиков – личные рабочие пространства разработчиков
2. Облачный инструментарий разработки – среда разработки, поддерживающая все основные языки программирования, работающая в браузере пользователя
3. Шаблоны развертывания – веб интерфейс каталога шаблонов развертывания ПО, позволяющий запускать установку ПО, изменять конфигурацию шаблонов развертывания.
4. Интерфейс реестра образов контейнеров – веб портал реестра образов контейнеров, который позволяет ознакомиться с содержимым каталога образов, их описанием, функциональностью и историей версий.
5. Интерфейс репозитория – пользовательский интерфейс репозитория исходных кодов и сборок системы управления версиями.
6. Интерфейс CI/CD – веб интерфейс настройки системы CI/CD

##### **Среда для разработки бизнес-объектов и среда для разработки бизнес-процессов**

Среда для разработки бизнес объектов и разработки бизнес-процессов - среды визуальной разработки, которые включают в себя возможность визуального редактирования бизнес-процессов и моделей данных. Комплексные среды, которые позволяют конструировать, тестировать и внедрять бизнес-процессы и модели данных (бизнес-объекты, такие, например, как документы) при помощи визуальных инструментов, а также непосредственно все необходимые инструменты для работы с объектами: включая формуляры и средства разработки форматно-логического контроля при заполнении формуляров.

Использование визуальных сред разработки позволяет значительно сократить сроки разработки и внедрения процессов и моделей данных в любой информационной системе. Также, значительным преимуществом является возможность настройки и изменения процессов и моделей без необходимости вносить изменения в код, таким образом, позволяя бизнес-пользователям работать с процессами напрямую, без необходимости привлекать инженеров для изменения исходных кодов информационных систем.

Реализация визуальной среды разработки должна соответствовать мировым стандартам в области платформ для разработки бизнес-приложений в общем, и RAD платформ в частности. Ключевая задача внедрения визуальных сред разработки - уменьшение трудозатрат и сокращение сроков разработки программных продуктов особенно в фазе прототипирования и пилотных проектов, что в свою очередь влечет за собой существенное уменьшение бюджета для таких задач. Визуальная среда разработки является расширением облачной среды разработки программных продуктов.

На базе визуальных сред предоставляется возможность создавать полноценные приложения, интегрируя их в программные продукты или публикуя как отдельные самостоятельные программные продукты или сервисы ИКП ЭП

Функционал разработчика более подробно описан в документе «Архитектура среды облачной разработки и тестирования».

### Функциональные компоненты уровня доступа

На рисунке ниже представлены функциональные компоненты уровня доступа, которые включают:

* Среда облачной разработки и тестирования программных продуктов;
* Среда коллективного взаимодействия;
* Закрытый репозиторий исходных кодов и сборок промышленной зоны;
* Каталог стандартных решений;
* Каталог сервисов ИС ГО



**Рисунок 9** - **Функциональные компоненты уровня доступа**

#### Среда облачной разработки и тестирования программных продуктов

Доступ разработки реализован в среде облачной разработки и тестирования и описан в документе «Архитектура среды для разработки и тестирования». В данном разделе кратко описан функционал ее компонентов на уровне доступа.

* 1. Репозиторий исходных кодов и сборок/Система управления версиями – репозиторий «Среды облачной разработки и тестирования» для публикации исходных кодов и сборок программных продуктов, разрабатываемых поставщиками для публикации в инфраструктуре ИКП ЭП. Включает систему управления версиями кода.
  2. Рабочие пространства разработчиков – инфраструктура необходимая для обеспечения облачной разработки, включает в себя
     1. Хранилище проектов разработчика
     2. Исполняемую среду для разрабатываемого проекта
     3. Интеграционные интерфейсы (API) для синхронизации с десктоп-приложением (не облачным интегрированным окружением разработки)
  3. Реестр образов контейнеров – в контексте уровня доступа речь идет о API репозитория, который позволяет:
     1. Скачивать образы
     2. Публиковать образы
     3. Удалять образы
  4. Система анализа кода - Система, а также среда для непрерывного анализа и измерения качества кода
  5. CI/CD – Continuous Integration/Continuous Delivery – это среда для выполнении частых автоматизированных сборок проекта и выполнения тестов, для скорейшего выявления и решения проблем
  6. База знаний – wiki подобная база-знаний, содержащая информацию по работе в «Среде облачной разработки и тестирования»
  7. Тестовые сервисы ИС ГО- тестовая среда с сервисами государственных органов
  8. Тестовые стандартные решения – тестовая среда с тестовыми версиями сервисов публикуемых программными продуктами автоматизации государственных органов

Роль и назначение стандартных решений, а также сервисов ИС ГО описана в разделах 10.2.2.4 и 10.2.2.5

#### Среда коллективного взаимодействия

Среда коллективного взаимодействия – это решение по автоматизации бизнес-процессов Сервисного Интегратора и Оператора, связанных с развитием, сопровождением и техническим обслуживанием ИКП ЭП и для управления разработкой и сопровождением программных продуктов автоматизации государственных органов, разрабатываемых и публикуемых на ресурсах ИКП ЭП.

«Среда коллективного взаимодействия», подробно описана в документе «Архитектура среды облачной разработки и тестирования», в контексте данного документа дается краткое описание ее функционала.

На данном уровне архитектуры функциональность «Среды коллективного взаимодействия» включает в себя:

1. Управление проектами – компонент, который используется для управления проектами по разработке программного обеспечения, а также для автоматизации управления внутренними проектами Сервисного Интегратора и Оператора
2. Управление релизами – компонент для управления публикацией релизов программного обеспечения, размещенного в ИКП ЭП
3. Управление инцидентами и проблемами – компонент для автоматизации сервисного сопровождения программных продуктов во время их разработки и после публикации в промышленной среде. Так же используется Оператором для осуществления поддержки пользователей ИКП ЭП
4. Управление конфигурациями (CMDB)- компонент предоставляет базу данных управления конфигурациями (CMDB) - репозиторий всего, что касается компонентов информационных систем (аппаратных и программно-аппаратных компонентов). CMDB помогает организации понять взаимосвязи между этими компонентами и отслеживать их конфигурации.
5. Управление задачами - предоставляет функциональность по управлению задачами и поручениями, с учетом ролей и обязанностей всех участников.
6. Управление требованиями - предоставляет функциональность по управлению требованиями, для коллективной работы над ними
7. Управление заявками - управление заявками на обслуживание позволяет своевременно и оперативно производить необходимое обслуживание аппаратной и программной инфраструктуры, а также любых других ИТ-систем и отдельных узлов.
8. Управление SLA - управление соглашениями об уровне обслуживания (SLA) - является важным аспектом внедрения информационно-технических услуг и решений, данный компонент формализует и систематизирует учет SLA по отношению к внедренным и предоставляемым ИТ-услугам, в рамках принятых контрактных обязательств
9. Управление клиентами (CRM) – компонент управления взаимоотношениями с клиентами
10. Каталог продуктов – каталог продуктов ИКП ЭП
11. Проектирование и моделирование – облачный векторный графический редактор для диаграмм и блок схем.

Функциональные компоненты Среды коллективного взаимодействия расположены только в зоне ЕТС ГО, так как БД должна быть общая для всех зон. Пользователи, находящиеся в зоне Интернет, получают доступ к функциональным компонентам Среды коллективного взаимодействия посредством SSO через ВШЭП.

#### Закрытый репозиторий исходных кодов и сборок промышленной зоны

Программные продукты, разработанные в «Среде облачной разработки и тестирования» ИКП ЭП, согласно методике, описанной в документе «Методики реализации проектов по автоматизации» и прошедшие тестирование, посредством компонента «Управление релизами» среды коллективной работы, перемещаются в закрытый репозиторий промышленной зоны, подробно процесс описан в документе «Методики миграции СПП со среды разработки и тестирования в ИКП ЭП».

#### Каталог стандартных решений

Каталог сервисов, публикуемых программными продуктами автоматизации государственных органов.

Программные продукты автоматизации государственных органов, разрабатываемые в «Среде разработки и тестирования» должны проектироваться с учетом требований сервис-ориентированной архитектуры (SOA). В контексте проекта Архитектуры ИКП ЭП это означает, что функционал программных продуктов автоматизации государственных органов, который потенциальном может быть использован другими программными продуктами, должен проектироваться с учетом его реализации в виде сервиса. Сервисы физически размещаются на ресурсах программных продуктов автоматизации государственных органов, в каталоге публикуется информация о них. На уровне служб ИКП ЭП размещается функционал обеспечивающий доступ к данным сервисам.

Каталог сервисов предоставляет разработчикам программных продуктов автоматизации государственных органов следующую функциональность:

1. Название сервиса
2. Описание функциональности сервиса
3. Методы сервиса и их сигнатуры
4. URL сервиса в промышленной зоне
5. URL сервиса в тестовой зоне
6. Примеры кода, иллюстрирующие работу с методами сервиса

В процессе разработки программных продуктов поставщики используют тестовые версии сервисов, опубликованные в специализированной тестовой зоне среды разработки и тестирования.

В каталоге сервисов должен быть включен сервис определения местоположения для мобильных приложений (геолокация)

#### Каталог сервисов ИС ГО

Каталог сервисов государственных органов, опубликованных на ШЭП/ВШЭП. Данные сервисы не являются частью ИКП ЭП. ИКП ЭП содержит каталог сервисов ИС ГО и предоставляет доступ к ним, через уровень служб в соответствии с зоной доступа: Интернет (ВШЭП), ЕТС ГО (ШЭП).

Многим программным продуктам автоматизации государственных органов требуется взаимодействие с сервисами предоставляемыми информационными системами и базами данных государственных органов. Для упрощения и стандартизации разработки интеграционных механизмов с данными сервисами и базами данных в среде ИКП ЭП должен быть реализован каталог сервисов ИС ГО на основе SmartBridge, который предоставит разработчикам программных продуктов автоматизации государственных органов следующий функционал:

1. Название сервиса
2. Описание функциональности сервиса
3. Методы сервиса и их сигнатуры
4. URL сервиса в промышленной зоне
5. URL сервиса в тестовой зоне
6. Примеры кода, иллюстрирующие работу с методами сервиса

В процессе разработки программных продуктов поставщики используют тестовые версии сервисов ИС ГО, опубликованные в специализированной тестовой зоне среды разработки и тестирования.

Обязательным сервисом является сервис ведения и предоставления Единой нормативно-справочной информации.

### Функциональные компоненты уровня службы

**Функциональные компоненты** уровня службы включают:

* Модуль управления контейнерами;
* Модуль управления виртуальными машинами;
* RAD платформу;
* Среду коллективного взаимодействия;
* Хранилище Big Data на основе имеющейся системы SmartDataUkimet;
* Сервисы Big Data;
* Службы резервного копирования;
* API VDC;
* Динамическое распределение ресурсов VDC;
* Сервисы ИС ГО;
* Стандартные решения.
* Технологические компоненты



Рисунок 10 - Функциональные компоненты уровня службы

#### 10.2.3.1 Модуль управления контейнерами

Функциональный компонент «Модуль управления контейнерами» отвечает за:

1. Оркестрацию контейнеров
2. Программное управление контейнерами
   1. Запуск
   2. Остановка
   3. Разворачивание
   4. Удаление
   5. Очистка не используемых ресурсов (Garbage Collection)
3. Управление публикацией – служба, отвечающая за выполнение шаблонов развертывания ПО.
4. API управления контейнерами – сервисы для программного взаимодействия с модулем управления контейнерами
5. Учет потребляемых ресурсов – компонент собирающий статистику по потребляемым пользователями ресурсам для модуля биллинга

#### 10.2.3.2 Модуль управление виртуальными машинами

Функциональный компонент «Модуль управления виртуальными машинами» отвечает за:

1. Оркестрацию виртуальных машин;
2. Работу с API гипервизоров;
3. Программное управление виртуальными машинами – набор программных компонентов, предоставляющих функционал для:
   1. Запуска виртуальной машины;
   2. Остановки виртуальной машины;
   3. Изменения конфигурации виртуальной машины;
   4. Удаление виртуальной машины;
   5. Создание виртуальной машины на основе образа;
   6. Создание виртуальной машины на основе параметров.

Программное управление виртуальными машинами будет использоваться в среде коллективного взаимодействия при работе с заявками пользователей для автоматизации работы администратора Оператора. Программное управление виртуальными машинами абстрагирует другие компоненты ИКП ЭП от реализации API гипервизоров сред аппаратной реализации и предоставляет универсальный программный интерфейс (API) для работы с любыми, поддерживаемыми ИКП ЭП гипервизорами.

1. Визуальная среда для работы с виртуальными машинами – набор инструментов для администратора Оператора, для управления виртуальными машинами в визуальной среде, предоставляет набор функций аналогичный программному управлению виртуальными машинами.
2. Шаблоны ВМ – каталог шаблонов виртуальных машин
3. Учет потребляемых ресурсов – компонент собирающий статистику по потребляемым пользователями ресурсам для модуля биллинга

#### 10.2.3.4 RAD платформа

Функциональный компонент «RAD платформа» (Rapid Application Development - быстрая разработка приложений) является визуальным конструктором, состоящим из двух ключевых элементов:

1. Сервисы для разработки бизнес-процессов.
2. Сервисы для разработки бизнес-объектов (моделей данных программных продуктов).

Решения RAD предназначены для быстрой разработки программных продуктов с использованием визуальных сред, практических без написания кода. Функциональный компонент «RAD платформа» является так же основой для компонента «Среда коллективного взаимодействия» и части «Среды облачной разработки и тестирования» ее компонентов:

1. Среда визуальной разработки бизнес-процессов
2. Среда визуальной разработки бизнес-объектов

Предоставляя вышеперечисленным компонентам необходимые сервисы для реализации функциональности данных модулей.

#### 10.2.3.5 Среда коллективного взаимодействия

На данном слое ИКП ЭП, функциональный компонент «Среда коллективного взаимодействия» размещает сервисы (API) и компоненты бизнес-логики.

В своем ядре «Среда коллективного взаимодействия» базируется на функционале компонента «RAD платформа», что позволяет оперативно, без вмешательства разработчиков вносить изменения в жизненные циклы обработки данных (бизнес-процессы) и изменять модели данных. Это необходимо для обеспечения требуемой гибкости компонента «Среда коллективного взаимодействия». Гибкость необходима для оперативного реагирования на изменяющиеся потребности в части функционала модулей.

#### 10.2.3.6 Хранилище Big Data

Хранилище Big Data – центральное хранилище модуля работы с большими данными и их обработки. Функциональный компонент Big Data относится к многоуровневым функциям. Более подробно функционал данного модуля описан в разделе 10.3.2.

#### 10.2.3.7 Сервисы Big Data

Сервисы для работы с хранилищем Big Data. Сервисы Big Data описаны в разделе 10.3.2.1.

#### 10.2.3.8 Службы резервного копирования

Система резервного копирования данных – программное обеспечения для непрерывного резервного копирования данных (backup), предназначенное для развертывания в рамках Платформы. Данное ПО создает резервные копии как самих серверов, так и данных которые хранятся внутри СУБД и других подсистем хранения. Также данное ПО предусматривает инструментарий для развертывания в эксплуатацию резервных копий в случае надобности.

Службы резервного копирования используются как для задач обеспечения резервного копирования ИКП ЭП, так и для предоставления услуг потребителям служб облачных вычислений.

#### 10.2.3.9 API VDC

Сервисы для работы с виртуальным датацентром. Предназначены для программного управления ресурсами виртуальных датацентров.

#### 10.2.3.10 Динамическое перераспределение ресурсов VDC

Динамическое масштабирование ресурсов виртуальных датацентров для обеспечения бесперебойной работы и оптимизации использования ресурсов. См. раздел 10.3.4.4

#### 10.2.3.11 Сервисы ИС ГО

Набор сервисов, предоставляющих доступ к реестрам, регистрам, справочникам и другим сервисам государственных органов для осуществления взаимодействия при разработке программных продуктов автоматизации государственных органов в «Среде разработки и тестирования» ИКП ЭП.

Не является компонентом ИКП ЭП, представляет собой службы обеспечения доступа к сервисам ИС ГО

#### 10.2.3.12 Стандартные решения

Разрабатываемые в «Среде разработки и тестирования» программные продукты автоматизации государственных органов должны проектироваться с учетом повторного использования их функционала другими программными продуктами. При разработке архитектуры программных продуктов автоматизации государственных органов должна осуществляться функциональная декомпозиция на сервисы. ИКП ЭП предоставляет слой доступа к данным сервисам, сами сервисы являются частью программных продуктов автоматизации государственных органов.

Сервисы становятся доступны разработчикам программных продуктов в «Среде разработки и тестирования». Как следствие разработка программных продуктов автоматизации государственных органов упрощается за счет повторного использования уже существующего функционала, опубликованного в виде сервисов.

**10.2.3.13 База данных как сервис (DBaaS)**

Служба, предоставляющая услугу «База данных как сервис» - доступ к программно-аппаратному комплексу, для размещения БД программных продуктов автоматизации государственных органов.

**10.2.3.14 Технологические компоненты**

Технологические компоненты - сервисы и информационные системы, используемые для развертывания решений для конечного пользователя и входящие в состав ИКП ЭП.

К технологическим компонентам относятся решения, позволяющие на своей базе реализовать полностью или частично автоматизацию бизнес-процессов для государственных органов с возможностью ее последующего включения в состав программных продуктов автоматизации государственных органов. Например, это могут быть:

1. Почтовый сервер
2. Блокчейн платформа

На базе блокчейн платформы могут создаваться функциональные компоненты, которые впоследствии будут включаться в состав программных продуктов автоматизации государственных органов.

### Функциональные компоненты уровня ресурса

#### Уровень ресурсов

Физические ресурсы включают аппаратные ресурсы, такие как серверы (центральный процессор и память), сети (маршрутизаторы, брандмауэры, выключатели, сетевые каналы и сетевые коннекторы, компоненты хранения (жесткие диски)) и другие физические элементы вычислительной инфраструктуры. Эти ресурсы могут включать ресурсы, находящиеся в центрах обработки данных облачных вычислений (например, вычислительные серверы, серверы хранения и сети внутри центра обработки данных), и ресурсы, находящиеся за пределами центров обработки данных, как правило, это сетевые ресурсы, такие как сети центры обмена и обработки данных и основные транспортные сети.

На рисунке ниже приведена схема, на которой представлено логическое представление ресурсов, которые будут участвовать в различных группах-системах платформы, а также взаимодействие между всеми участниками.



Рисунок 11 – Логическое представление ресурсов

**Функциональные компоненты** уровня ресурса включают:

- Среда виртуализация на уровне ОС;

* Абстрагирование ресурса и управление ресурсом (гипервизоры);
* Вычислительные ресурсы;
* Системы хранения данных (SDS, SAN-сеть);
* Сети и сетевое оборудование (SDN);
* Резервное копирование.



Рисунок 12 - Функциональные компоненты уровня ресурсов

#### Среда виртуализации на уровне ОС

Виртуализация на уровне ОС в контексте проекта Архитектура ИКП ЭП используется для обеспечения управления инфраструктурами информационных систем, СПП и других программных продуктов. Контейнер в контексте проекта является инфраструктурной единицей, размещаемой «поверх» аппаратной виртуализации. Данный подход обеспечивает необходимую гибкость в управлении инфраструктурами сложных систем, в части публикации, обновления, управления разработкой и тестированием.

Виртуализация на уровне ОС является базой для следующих модулей ИКП ЭП:

1. Модуль управления контейнерами;
2. RAD платформа;
3. Среда коллективного взаимодействия;
4. Среда облачной разработки и тестирования.

Технология виртуализации на уровне ОС позволяет осуществлять установку непосредственно на сервера без использования гипервизора. В ряде случаев, в особенности для приложений, производительность которых может деградировать при использовании гипервизора, такой вариант установки может быть предпочтителен. Он позволяет использовать преимущества управления виртуализированными ресурсами избежав накладных расходов гипервизоров.

Технология виртуализации на уровне ОС, которая будет использоваться при реализации ИКП ЭП должна поддерживать Container Runtime Interface и Container Network Interface.

#### Абстрагирование ресурса и управление ресурсом

Функциональный компонент абстрагирования ресурсом и управления ресурсом используются в ИКП ЭП, чтобы обеспечить доступ к физическим вычислительным ресурсам посредством программной абстракции. Абстрагирование ресурса должно гарантировать эффективное, безопасное и надежное использование нижележащей инфраструктуры. Для обеспечения используется виртуализация аппаратных ресурсов.

В аппаратной виртуализации базовый слой — гипервизор. Этот слой загружается на сервере и обеспечивает взаимодействие между аппаратным обеспечением сервера и виртуальными машинами. ИКП ЭП должна поддерживать следующие типы гипервизоров:

1. KVM
2. Hyper-V
3. VMware

В некоторых случаях, базируясь на рекомендациях вендоров ЛПО, возможен отказ от использования виртуализации с гипервизорами. В этом случае рассматривается установка ЛПО непосредственно на сервера без использования виртуализации, либо установка ЛПО на виртуализацию на уровне ОС.

#### Вычислительные ресурсы (Сервера)

Вычислительными ресурсами называются возможности, обеспечиваемые компонентами вычислительной системы, расходуемые в процессе её работы.

Для построения серверного комплекса типового ЦОД необходимо использоваться модель системы с многоуровневой архитектурой (Client-Middleware-Server).

Серверный комплекс типовой многоуровневой архитектуры должен состоит из следующих групп серверов:

* Серверы представления информации. Их функция состоит в реализации интерфейса между серверами приложений и пользователями системы. К этой группе серверов относятся терминальные серверы и web-серверы.
* Серверы приложений. Эта группа серверов обрабатывает данные, следуя логике системы. Например, к серверам приложения относятся серверы, которые выполняют модули SAP R/3 или Oracle Applications.
* Серверы информационных ресурсов (или ресурсные серверы). Серверы этой группы обеспечивают сохранение данных и предоставление их серверам приложений. К этой группе сервером относятся, например, серверы СУБД и файл-серверы.
* Служебные серверы. Серверы этой группы необходимы для обеспечения работы остальных подсистем, из которых состоит ЦОД. К этой группе относятся серверы управления системой резервного копирования.

Достоинством многоуровневой или облачной архитектуры, выгодно отличающими ее от одноуровневой и двухуровневой архитектуры, является масштабируемость. Масштабируемость увеличивается при добавлении приложений и серверов представления информации. Это происходит благодаря значительному количеству параллельных соединений с клиентами и за счет того, что нагрузка может распределяться между несколькими физическими серверами. При использовании многоуровневой архитектуры бизнес-логику можно концентрировать на втором уровне и при необходимости проводить ее модификацию.

Возможность многократного использования сервисов. Благодаря этой возможности существенно удешевляется разработка системы и ее администрирование.

Сохранение инвестиций. На начальных этапах можно работать на серверах класса «рабочих групп». Но со временем по мере возрастания рабочих нагрузок возникнет необходимость увеличить мощность ресурсных серверов. Тогда можно установить более мощные ресурсные серверы, а старые серверы переместить в группу серверов приложений. Таким образом, инвестиции, сделанные на начальных этапах, полностью сохраняться.

#### Системы хранения данных

**Виртуализация хранения данных** – это предоставление ресурса физической емкости накопителей в форме логического пространства хранения. Истинная структура системы хранения инкапсулирована – скрыта от внешней среды. Сервер (хост) освобождается от необходимости знать, где и как данные размещаются физически, он обращается к некоему общему пулу хранения, обладающему определенным качеством обслуживания QoS. Управление же фактическим размещением данных осуществляется исключительно на уровне СХД. Это свойство также именуют маскированием среды хранения. В числе прочего маскирование приводит к возможности независимого масштабирования и СХД, и серверного пула, и прочих составляющих программно-аппаратного комплекса. Изменения на одном уровне стека не привязаны к другим.

Виртуализация СХД выполняет следующие функции:

1. Упрощает подключение новых серверов к СХД (первоначальную инсталляцию и дальнейшее ее сопровождение);
2. Решает проблемы, связанные с выделением дополнительного дискового пространства серверу;
3. Облегчает процесс миграции данных между СХД (процесс миграции данных даже внутри одной системы хранения может быть осложнен различными обстоятельствами, например, остановкой работы сервера на длительное время);
4. Способствует повышению производительности СХД (более высокая производительность получается за счет перераспределения нагрузки - т. о. устраняются «перегретые» диски и данные распределяются по большему количеству дисков);
5. Повышает устойчивость СХД к аппаратным сбоям.

**Объектное хранилище** — это способ хранения данных без иерархии, который обычно используется в облачной среде. В отличие от других способов хранения данных, объектное хранилище не использует иерархию каталогов. Отдельные единицы данных (объекты) сосуществуют в пуле данных на одном уровне. Каждый объект имеет уникальный идентификатор, используемый приложением для обращения к нему. Кроме того, каждый объект может содержать метаданные, получаемые вместе с ним.

Ключевые особенности

1. Данные хранятся как отдельные объекты.
2. Данные не помещаются в иерархию каталогов, а располагаются в плоском адресном пространстве.
3. Приложения определяют отдельные объекты данных по их уникальным адресам.
4. Предназначено для доступа на уровне приложения с помощью API, а не на уровне пользователя.

##### SAN-сеть

**Сеть хранения данных**, или Storage Area Network — это система, состоящая из собственно устройств хранения данных — дисковых, или RAID — массивов, ленточных библиотек, среды передачи данных и подключенных к ней серверов. Обычно используется достаточно крупными компаниями, имеющими развитую IT инфраструктуру, для надежного хранения данных и скоростного доступа к ним.  
СХД — это система, позволяющая раздавать серверам надежные быстрые диски изменяемой емкости с разных устройств хранения данных.

##### SDS

Программно-определяемые системы хранения (SDS) — это один из основных компонентов программно-определяемого ЦОД. SDS принципиально отличаются от классических и блочных хранилищ. Главный принцип таких систем — полный перенос организации хранения с аппаратных контроллеров на программный уровень.

Основными преимуществами являются:

**Экономичность.** Программно-определяемые хранилища дают возможность отказаться как от проприетарных решений в пользу стандартизированного оборудования, так и от традиционной сети хранения данных (SAN) Fibre Channel в пользу более универсального стандарта Ethernet.

**Гибкость.** Программно-определяемые хранилища могут быть построены на оборудовании любого производителя или даже различных производителей в рамках одной системы. SDS легко масштабируются, поскольку программный уровень организации предоставляет очень широкие возможности по управлению ресурсами.

**Отказоустойчивость.** При возникновении проблем на основной SDS с помощью средств репликации данные легко и бесшовно переносятся на резервную систему.

**Удобство эксплуатации.** ИТ-служба расширяет SDS без оглядки на производителя каждой конкретной единицы оборудования, легко перераспределяет данные между разными уровнями хранения для наиболее рационального использования ресурсов.

**Производительность.** Программно-определяемые хранилища поддерживают подключение PCIe NVMe-карт, существенно увеличивающих возможности систем.

#### Сети и сетевое оборудование

**Сетево́е обору́дование** — устройства, необходимые для работы компьютерной сети, например: [маршрутизатор](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80), [коммутатор](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%82%D0%BE%D1%80), [концентратор](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BA%D0%BE%D0%BD%D1%86%D0%B5%D0%BD%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80), [патч-панель](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%82%D1%87-%D0%BF%D0%B0%D0%BD%D0%B5%D0%BB%D1%8C) и др. Можно выделить активное и пассивное сетевое оборудование.

Активное оборудование — это оборудование, содержащее электронные схемы, получающее питание от электрической сети или других источников и выполняющее функции усиления, преобразования сигналов и иные. Это означает способность такого оборудования обрабатывать сигнал по специальным алгоритмам. В сетях происходит пакетная передача данных, каждый пакет данных содержит также техническую информацию: сведения о его источнике, цели, целостности информации и другие, позволяющие доставить пакет по назначению. Активное сетевое оборудование не только улавливает и передает сигнал, но и обрабатывает эту техническую информацию, перенаправляя и распределяя поступающие потоки в соответствии со встроенными в память устройства алгоритмами. Эта «интеллектуальная» особенность, наряду с питанием от сети, является признаком активного оборудования.

Пассивное оборудование, как оборудование, не получающее питание от электрической сети или других источников, и выполняющее функции распределения или снижения уровня сигналов. Например, кабельная система: кабель (витая пара), вилка/розетка ([RG58](https://ru.wikipedia.org/wiki/RG58), [RJ45](https://ru.wikipedia.org/wiki/RJ45), [RJ11](https://ru.wikipedia.org/wiki/RJ11), [GG45](https://ru.wikipedia.org/wiki/GG45)), [патч-панель](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%82%D1%87-%D0%BF%D0%B0%D0%BD%D0%B5%D0%BB%D1%8C) и т. д.

##### SDN

Эта функция позволяет устранить ограничения виртуальной локальной сети и иерархического назначения IP - адресов при подготовке виртуальных машин к работе. Кроме того, функция виртуализации сети поддерживает необходимые требования изоляции и безопасности при использовании нескольких клиентов. Эта функция позволяет использовать концепцию не зависящей от расположения адресации, основанной на виртуализации IP-адресов. Она создает виртуальные топологии уровня 2 и уровня 3 в любой физической сети, поддерживающий двунаправленные IP-подключения. Это означает, что физические сети могут представлять собой иерархические трехуровневые сети с полной направленной полосой пропускания, сети Clos или большие инфраструктуры уровня 2. Преимущество такого подхода состоит в том, что по мере добавления виртуальных машин в облако можно динамически настраивать виртуальные сети с помощью программного обеспечения. Кроме того, такие сети могут распространяться на несколько физических подсетей и площадок.

При сетевой изоляции с помощью виртуальной локальной сети все рабочие нагрузки в группе изоляции должны находиться в одной подсети. Кроме того, функция виртуализации сети позволяет задавать группы сетевой изоляции за пределами сети, например, в подсетях. Это повышает гибкость и позволяет устранить ограничения конфигурации физической сети при определении того, где необходимо размещать рабочие нагрузки.

Использование политики, основанной на программном обеспечении, в сочетании с основанными на политиках сетями центра обработки данных позволяют реализовать изоляцию без использования виртуальных локальных сетей.

Вы можете использовать гибкие средства размещения рабочих нагрузок, сохраняя текущую схему IP - адресов, так как она не ограничена конфигурацией физической IP-подсети или виртуальной локальной сети.

Устранив зависимость порядка размещения виртуальных машин от инфраструктуры физической сети, вы повысите гибкость размещения рабочих нагрузок и увеличите общую эффективность использования серверов и сети.

#### Резервное копирование

Резервное копирование необходимо для возможности быстрого и недорогого восстановления информации (документов, программ, настроек и т. д.) в случае утери рабочей копии информации по какой-либо причине. Система резервного копирования является служебной подсистемой ЦОД и имеет следующие особенности:

* Процесс резервного копирования не является критичным для решения задач ИС, т.е. сбой в системе резервного копирования не приводит к снижению доступности критичных информационных сервисов;
* Нагрузка на вычислительные средства, которую создает процесс резервного копирования, не является полезной с точки зрения предоставления информационных сервисов ИС.

Требования к системе резервного копирования

* Надёжность хранения информации — обеспечивается применением отказоустойчивого оборудования систем хранения, дублированием информации и заменой утерянной копии другой в случае уничтожения одной из копий (в том числе как часть отказоустойчивости).
* Многоплатформенность - полноценное функционирование системы резервного копирования в гетерогенной сети предполагает, что ее серверная часть будет работать в различных операционных средах и поддерживать клиенты на самых разных аппаратно-программных платформах.
* Простота в эксплуатации — автоматизация (по возможности минимизировать участие человека: как пользователя, так и администратора).
* Быстрое внедрение — простая установка и настройка программ, быстрое обучение пользователей.

Система резервного копирования должна иметь возможность представления сетевых блочных устройств посредством распространенных протоколов Ethernet, PCI Express, SAS, NVMeoF, FC, FCoE или InfiniBand с возможностью поддержки одинакового функционала:

* идентифицировать хост и СХД;
* иметь возможность маршрутизировать траффик;
* разделять сеть на подсети и изолировать в них траффик;
* обеспечивать возможность использования нескольких путей к СХД;
* управлять подключением устройств к сети;
* приоритизировать траффик.

Поддерживаемые протоколы хранения данных можно разделить на две условные группы:

1. используемые для подключения серверов приложений (FC, FCoE, iSCSI, NFS, SMB);
2. используемые для подключения в рамках кластера или в качестве интерконнекта внутри СХД (InfiniBand, NVMe, PCIe).

Протоколы iSCSI, NFS, SMB, FCoE используют Ethernet-сети для передачи данных, поэтому использовать данные протоколы в общих сетях не целесообразно. Это приводит к необходимости развёртывания выделенных сетей для использования их в качестве SAN.

**Fibre Channel** — протокол хранения, обеспечивающий низкие задержки и высокую пропускную способность за счёт своих архитектурных особенностей. Fibre Channel не требователен к ресурсам и отлично подходит для передачи большого объёма данных, так как все операции FC выполняются на стороне HBA, разгружая центральный процессор. Новые версии протокола Fibre Channel обратно совместимы с прошлыми редакциями, что открывает хорошие перспективы для модернизации и масштабирования. Например, если внедрять FC 32Гб/с, то всё ещё можно будет использовать FC 8Гб/с и 16Гб/с, т.е. можно поэтапно менять FC-коммутаторы и FC адаптеры.

**Fibre Channel over Ethernet** – протокол позволяет консолидировать операции ввода-вывода и, как следствие, обеспечить безопасное размещение в одном «проводе» различных типов траффика. Что подразумевает снижение совокупной стоимости владения системой (TCO) за счет уменьшения числа кабелей и адаптеров, а также снижения показателей по энергопотреблению. При этом показатели доступности и производительности FCoE не сопоставимы с показателями FC, так как передача данных требует дополнительных накладных расходов на инкапсуляцию в Ethernet. FCoE добавляет сложность в развёртывании и администрировании всей системы, повышая уровень требований к обслуживающему персоналу и поддержке решения.

**iSCSI (Internet Small Computer System Interface)** строится на двух наиболее часто используемых протоколах:

* SCSI — протоколе обмена блоками данных между компьютером и хранилищем
* IP — сетевом транспортном протоколе, широко применяемом в корпоративных сетях Ethernet.

iSCSI — это низкобюджетное решение для внедрения. Администрирование очень простое, хотя для обеспечения отказоустойчивости необходимо строить выделенную сеть для iSCSI, что приближает к сетевой реализации, очень похожей на FC SAN. Считается, что iSCSI 10Гбит обеспечивает такое же количество IOps и пропускную способность, как и сопоставимый ему FC 8Гбит, но это не совсем так. Хотя пропускная способность iSCSI и выше, но его эффективность ниже, чем у FC за счёт дополнительных накладных расходов. Производительность iSCSI зависит от существующий инфраструктуры Ethernet (на сегодняшний день минимально рекомендованная сеть для iSCSI – 10Гбит). В ближайшем будущем (по данным Gartner, 10–12 месяцев) стоит планировать переход на 25/40/50GbE, если будет необходимость использовать высокопроизводительные all-flash СХД.

**Network File System (NFS)** — протокол сетевого доступа к файловым системам,. NFS предоставляет клиентам прозрачный доступ к файлам и файловой системе сервера.  
NFS просто конфигурируется и администрируется, т.к. используется поверх сетей Ethernet. Как и в других протоколах, использующих Ethernet, скорость и задержки целиком зависят от реализации сети на нижнем уровне и чаще всего «упираются» в ограничения стандарта 10GbE. NFS часто используется как протокол начального уровня для построения SAN-сети для виртуализации. По прогнозам Gartner, такой тренд сохранится в течение последующих 10 лет.

**SMB (Server Message Block)** — это сетевой протокол для общего доступа к файлам, который позволяет приложениям компьютера читать и записывать файлы, а также запрашивать службы серверных программ в компьютерной сети. Разработан компанией Microsoft для реализации «Сети Microsoft Windows» и «Совместного использования файлов и принтеров». С увеличением пропускной способности сетей передачи данных SMB стал одним основных протоколов файлового доступа, применяемых в СХД. В системах хранения SMB чаще всего используется в сетях 10GbE, из-за этого его производительность сильно зависит от реализации, настроек и используемых компонентов сети. Как и NFS, SMB часто используется в качестве протокола начального уровня при построении SAN-сети для виртуализации. Эта тенденция также должна сохраниться в ближайшее десятилетие.

**InfinBand** — высокоскоростной протокол, обеспечивающий очень большую пропускную способность и низкие задержки. Используется, преимущественно, в отрасли высокопроизводительных вычислений (HPC) и в качестве интерконнекта при создании высокопроизводительных СХД. Наиболее явным недостатком этой технологии является сложность в настройке и администрировании. Как следствие, работа с IB требует квалифицированного персонала. В сравнении с FC и Ethernet протокол InfiniBand более «дорог» для внедрения и обслуживания. К тому же, существует лишь несколько считанных компаний, которые производят оборудование и программное обеспечение для работы с IB.

**NVMe (NVM Express)** — это новый высокопроизводительный протокол доступа к твердотельным накопителям, подключенным по шине PCI Express. Аббревиатура «NVM» в названии обозначает энергонезависимую память (Non-Volatile Memory), в качестве которой в SSD повсеместно используется флеш-память типа NAND. На данный момент технология NVMe еще не получила широкого распространения. В основном протокол используется для внутреннего соединения в серверах и СХД. Спецификация NVMe также позволяет инкапсулировать его в другие протоколы, такие как Ethernet, FC и InfiniBand, и масштабировать протокол в более крупных сетях. Поскольку NVMe использует прямой доступ к памяти (RDMA), латентность протокола несущей должна быть очень низкой для нормальной работы протокола. В 2017 году многие производители серверных платформ представили новые модели СХД с поддержкой двухпортовых NVMe-устройств, что позволит проектировать отказоустойчивые решения для хранения. Ожидается, что в ближайшие несколько лет NVMe будет использоваться в качестве внешнего межсетевого интерфейса, аналогичного PCIe и InfiniBand. Гораздо шире NVMe будет использоваться в качестве внутреннего интерконнекта.

**PCIe** имеет очень низкие задержки и используется преимущественно в серверах для подключения плат расширения, в том числе и высокопроизводительных NVMe дисков. Некоторые новые продукты от известных производителей используют PCIe в качестве протокола подключения серверов через небольшие PCIe коммутаторы, т.е. PCIe получается использовать только в небольших SAN-сетях. Так как PCIe не использует SCSI и требует собственного протокола для передачи данных, он может увеличить пропускную способность за счёт уменьшения задержек, по сути, работая на скорости чистой PCIe-линии. Такие решения требуют применения проприетарных драйверов, что делает их сложно администрируемыми и приводит к невозможности создавать гетерогенные инфраструктуры, а также встраивать такие решения в существующие SAN сети. По количеству линий PCIe масштабируется от 1ГБ/с до 16ГБ/с. В 2017 году выходит новый стандарт PCIe 4.x, который увеличит производительность в 2 раза, т.е. максимальная производительность достигнет 32ГБ/с.

Дополнительно необходимо выделить рекомендации касательно хранения данных на ленточных накопителях посредством стандартов записи на магнитные носители. **LTO** (Linear Tape-Open) — стандарт записи на магнитную ленту, которому удовлетворяет большинство современных стримеров. Практически используемым форматом записи данных в этом стандарте является Ultrium.

##### Требования к компонентам ЦОД и их функциям

Требования к компонентам ЦОД ИКП ЭП описаны в документе «Аналитический отчет и рекомендации»

## Многоуровневые функции

### Функциональные компоненты систем безопасности

**Функциональные компоненты** систем безопасности ответственны за применение средств управления, связанных с безопасностью, для противодействия угрозам безопасности в среде окружения **облачных вычислений**. **Функциональные компоненты** систем безопасности охватывают все средства безопасности, требуемые для поддержания **облачных вычислений**.

**Функциональные компоненты** систем безопасности включают:

* аутентификацию и управление идентификацией;
* авторизацию и управлению политикой безопасности;
* управление шифрованием.

#### Аутентификация и управление идентификацией

**Функциональный компонент** аутентификации и управления идентификацией обеспечивает возможности, связанные с идентификацией пользователей и их идентификационными данными, требуемыми для аутентификации пользователей, когда они получают доступ к **службам облачных вычислений**. Сервис аутентификации пользователей ИКП ЭП публикуется на ВШЭП

#### Авторизация и управление политикой безопасности

**Функциональный компонент** авторизации и управления политикой безопасности обеспечивает возможности для контроля и применения авторизации для пользователей при получении доступа к определенным возможностям или данным. Управление политикой службы предусматривает определение и применение политики безопасности, которая связана со **службами облачных вычислений**. Сервис авторизации пользователей ИКП ЭП публикуется на ВШЭП

#### SSO (единая точка входа)

Сервис ИКП ЭП, позволяющий пользователю, прошедшему авторизацию и аутентификацию получать доступ ко всем службам облачных вычислений в соответствии с его правами, без повторной авторизации и аутентификации.

Функционал модуля «SSO» описан в документе «Архитектура среды разработки и тестирования»

#### Управление шифрованием

**Функциональный компонент** управления шифрованием обеспечивает возможности, связанные с шифрованием данных, независимо от того, находятся ли данные в покое или в движении. Управление ключами шифрования и выбор схемы шифрования — некоторые из предоставляемых возможностей.

#### Требования к исходным кодам

Технологические компоненты, использованные в объекте ИКИ, должны иметь открытые исходные коды, т.е. исходный код должен быть доступен для просмотра, изучения и изменения. Исходные коды и техническая документация технологических компонентов должны быть предоставлены в РГП ГТС для проведения испытания анализа их исходного кода технологического компонента согласно Методике и правил проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы «электронного правительства», интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности, утвержденных Приказом Министра оборонной и аэрокосмической промышленности Республики Казахстан от 14 марта 2018 года № 40/НК.

Изменение или добавление технологических компонентов не влияет на ежегодную аттестацию ИКП ЭП.

В случае изменения технологического компонента Партнер должен подать заявку в РГП «ГТС» на проведение повторного испытания анализа исходного кода.

#### Обеспечение информационной безопасности

В соответствии со стандартом, СТ РК ИСО/МЭК 27002-2015 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации» информационная безопасность определяется как защита конфиденциальности, целостности и доступности информации. Информационная безопасность защищает информацию от широкого диапазона угроз с целью обеспечения уверенности в непрерывности бизнеса, минимизации риска бизнеса, получения максимальной отдачи от инвестиций, а также реализации потенциальных возможностей бизнеса.

Информационная безопасность достигается путем реализации соответствующего комплекса мер и средств контроля и управления, которые могут быть представлены политиками, процессами, процедурами, организационными структурами, а также функциями программных и аппаратных средств.

Применение технологий облачных вычислений в сфере оказания государственных услуг становится мировой тенденцией, а облачная безопасность является неотъемлемым элементом облачной стратегии. В проектируемой облачной Платформе безопасность рассматривается в качестве оболочки для полноты решения.

На данный момент существует свод стандартов ISO по обеспечению информационной безопасности облачных вычислений, в частности в данном документе используется международный стандарт ISO/IEC 27002 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации».

Облачная ИС имеет многоуровневую архитектуру, в которой учитываются подходы, описанные в стандарте ISO/IEC 17789 «Информационные технологии. Облачные вычисления. Эталонная архитектура».

Безопасность информации в облаке должна комплексно обеспечиваться на всех уровнях архитектуры. Рассмотрим систему защиты информации облака в привязке к многоуровневой архитектуре.

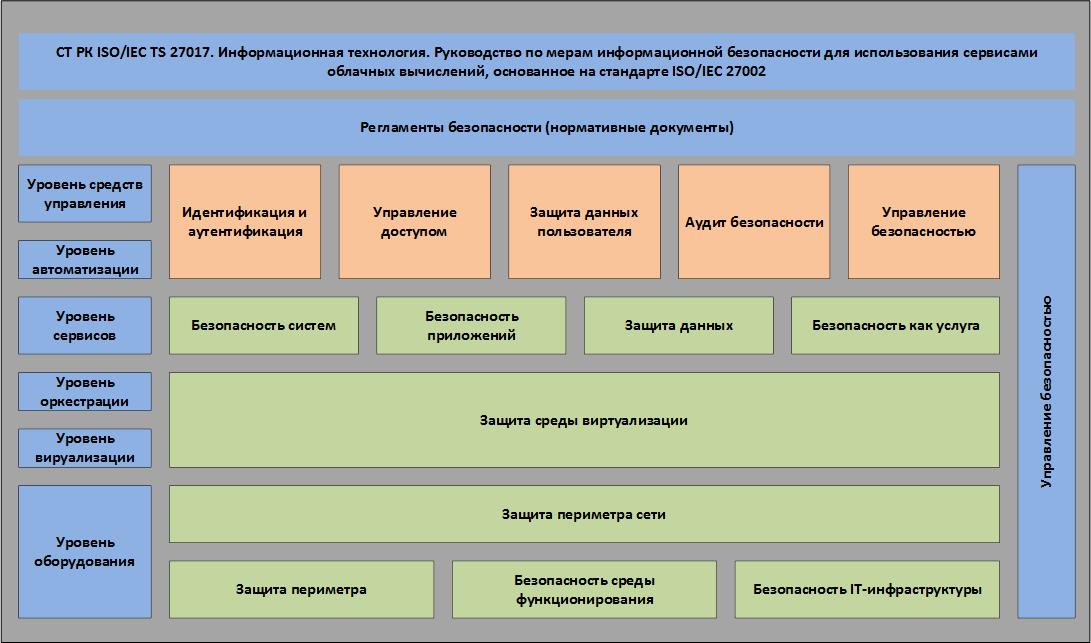


Рисунок 13 - Общая диаграмма безопасности облачной инфраструктуры по слоям

Состав системы на каждом из уровней архитектуры представлен в таблице 2 ниже.

Таблица – Комплексная система защиты информации в облачной ИС

|  |  |
| --- | --- |
| Управление безопасностью | Нормативные правовые акты; процессы управления и обеспечения ИБ (PLAN, DO, CHECK, ACT), локальные нормативные правовые акты (политики, процедуры, инструкции), направленные на реализацию процессов |
| Защита периметра | Контроль и управление доступом, видеонаблюдение, охранная сигнализация |
| Безопасность среды функционирования | Пожарная сигнализация, автоматика здания, мониторинг ресурсов, кабельная система, электроснабжение, распределение питания, охлаждение, освещение, связь |
| Безопасность ИТ-инфраструктуры | Высокая доступность, непрерывность функционирования, резервное копирование и восстановление, доверенные вычисления (RoT, TPM, TXT) |
| Защита периметра сети | Защита от DDoS-атак, межсетевое экранирование, обнаружение и предотвращение вторжений, поточный антивирус, защита данных от утечек (DLP), фильтрация web-трафика и защита web-приложений, защита каналов передачи данных |
| Защита среды виртуализации | Защита от несанкционированного доступа, контроль целостности, резервное копирование, антивирусная защита, межсетевые экраны, системы обнаружения и предотвращения вторжений |
| Безопасность систем/приложений | Контроль целостности, антивирусная защита, межсетевые экраны, управление уязвимостями, системы обнаружения и предотвращения вторжений |
| Защита данных | Защита от несанкционированного доступа, контроль целостности, криптографическая защита, защита от утечек |
| Защита системы автоматизации и средств управления | Идентификация, аутентификация, управление доступом, доверенный канал связи, защита данных пользователя, регистрация событий, мониторинг и оповещение |
| Безопасность как услуга | Идентификация и управление доступом, предотвращение утечек информации, веб-безопасность, защита почты, обнаружение вторжений, шифрование, непрерывность бизнеса и аварийное восстановление, защита сети, управление информационной безопасности и событиями безопасности |

Для реализации облачной безопасности необходимо определить методы, направленные на выполнение мониторинга, анализ подозрительной активности и защиту от вредоносных программ. В этом помогают различные инструменты или конфигурационные опции:

1. Виртуальные IP-адреса. Использование виртуальных IP-адресов позволяет разделять сети на внутренние и внешние.
2. Межсетевые экраны, балансировщики нагрузки и прокси. Данные средства определяют границы зон безопасности и дают возможность управлять трафиком.
3. SSL. Для шифрования HTTP-трафика и мониторинга сетевой активности своевременного обнаружения вторжения.
4. Защита от вредоносных программ на уровне гипервизора. Специализированное ПО обнаруживает и нейтрализует вредоносные программы и приложения.

Стоит отметить, что одним из важнейших аспектов работы любой среды является развитый план по поддержанию безопасности инфраструктуры. Очень часто его частью является регулярное обновление программного обеспечения и внесение исправлений, мониторинг компонентов безопасности, а также проведение тестов на определение уязвимостей.

В разделах ниже приведены и систематизированы механизмы и способы обеспечения информационной безопасности Платформы. Каждой из известных типов угроз, возникающих при использовании виртуальных сред, можно противопоставить средства защиты. Основополагающими инструментами для обеспечения информационной безопасности являются специализированные программные решения. Ассортимент защитных программных продуктов достаточно обширен, но составить их чёткую классификацию на данный момент сложно – любая классификация будет достаточно условной. Часть антивирусных продуктов содержат в себе функциональность систем защиты от вторжений. Системы защиты от вторжений содержат в себе средства мониторинга за действиями пользователей, а также иногда и антивирусную составляющую. Для эффективного решения данной проблемы следует применять целый комплекс программного обеспечения. Каждая часть такого комплекса в свою очередь обеспечивает определенную, узкоспециализированную функциональность для обеспечения безопасности передачи, хранения или оперирования информацией в рамках системы и её подсистем.

В проектируемой Платформе предлагается использовать следующие решения по обеспечению информационной безопасности, для предотвращения рисков указанных в Таблице 3:

1. Система обнаружения вторжений (IDS);
2. Система предотвращения вторжений (IPS);
3. Предотвращение утечек информации (DLP);
4. Межсетевой экран (Firewall);
5. Системный мониторинг;
6. Резервное копирование;
7. Web Application Firewall;
8. SSL/TLS сертификаты;
9. Виртуальная частная сеть (VPN);
10. Двухфакторная аутентификация;
11. Система управления событиями информационной безопасности (SIEM).

#### Система обнаружения вторжений

Система обнаружения вторжений (англ. Intrusion Detection System, IDS) – это программное обеспечение для обнаружения попыток вторжения в защищенные сети либо комплексы, внутри которых развертываются такого рода решения. Основной целью является мониторинг сетевого траффика и другой активности с целью обнаружения умышленных действий подозрительного характера с последующим оповещением и журналированием данных событий. Для ИКП ЭП применимы следующие требования:

1. Мониторинг и журнал входящих и исходящих пакетов в IP сетях;
2. Сканирование пакетов на предмет содержания заданных сигнатур;
3. Сигнализация событий об обнаруженных, потенциальных нарушениях;
4. Анализ сетевого траффика в режиме реального времени (real time);
5. Обнаружение аномалий посредством анализа используемого протокола;
6. Поддержка возможности поиска в содержимом пакета (content search);
7. Поддержка возможности сопоставления содержимого (content match);
8. Возможность расширения спектра с помощью задания правил (rules).

IDS-системы состоят из:

1. Системы сбора событий;
2. Системы анализа собранных событий;
3. Хранилища, в котором накапливаются собранные события и результаты их анализа;
4. Базы данных об уязвимостях (этот параметр является ключевым, так как чем больше база у производителя, тем больше угроз способна выявлять система);
5. Консоли управления, которая позволяет настраивать все системы, осуществлять мониторинг состояния защищаемой сети, просматривать выявленные нарушения и подозрительные действия.

#### Система предотвращения вторжений

Система предотвращения вторжений (англ. Intrusion Prevention System, IPS) – это программное обеспечение для предотвращения вторжений и атак как на отдельные узлы системы, так и на сети целиком, в рамках которых развернуты компоненты системы. Типовые решения данной категории используют IDS решения для получения информации об угрозах, и на её основе выполняют действия для попытки предотвращения вторжений, в том числе и путем блокировки источников. Для проектируемой Платформы применимы следующие требования:

1. Средства для обеспечения взаимодействия с системами обнаружения;
2. Реагирование с помощью блокировки потенциального источника атак;
3. Реагирование с помощью блокировки потоков траффика в данной сети;
4. Реагирование с помощью выполнения сброса сомнительных соединений;
5. Возможность выполнять дефрагментацию раздробленных пакетов;
6. Переупорядочивание пакетов TCP для предотвращения спуфа SEQ/ACK.

Использование IPS-систем преследует несколько целей:

1. Обнаружить вторжение или сетевую атаку и предотвратить их;
2. Спрогнозировать возможные будущие атаки и выявить уязвимости для предотвращения их дальнейшего развития;
3. Выполнить документирование существующих угроз;
4. Обеспечить контроль качества администрирования с точки зрения безопасности, особенно в больших и сложных сетях;
5. Получить полезную информацию о проникновениях, которые имели место, для восстановления и корректирования вызвавших проникновение факторов;
6. Определить расположение источника атаки по отношению к локальной сети (внешние или внутренние атаки), что важно при принятии решений о расположении ресурсов в сети.

Рекомендуется использовать комплексное решение, которое решает следующие проблемы:

1. Мгновенную фильтрацию в режиме In-Line и мониторинг копии трафика;
2. Предотвращение всех видов внешних атак, в том числе неизвестных — «атак нулевого дня»;
3. Обновление программного обеспечения и сигнатур;
4. Всестороннее обнаружение угроз с помощью сигнатурного и эвристического анализа, выявления аномалий и отклонений от нормы поведения;
5. Поддержку виртуализации;
6. Возможность применять различные политики безопасности для отдельных каналов связи и участков сети;
7. Мониторинг событий ИБ и создание отчетности.

#### Предотвращение утечек информации

DLP - (англ. Data Leak Prevention) – технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек.

DLP как сервис расширяет действие по предотвращению утечки данных на облачные среды и все уязвимые каналы передачи информации, обеспечивая более полный и эффективный поиск, мониторинг и защиту информации.

Для проектируемой Платформы применимы следующие требования:

1. Обнаружение данных в облаке и в локальных средах;
2. Отслеживание использования данных независимо от того, подключены ли сотрудники к корпоративной сети;
3. Защита данных от утечки или кражи - независимо от их расположения или способа использования.

DLP как сервис позволяет решить следующие задачи:

1. **Защита форм, содержащих конфиденциальные данные.** DLP Form Recognition, продукт для обнаружения содержимого на основе интеллектуальных методов обработки изображений, определяет и блокирует конфиденциальные данные в отсканированных или сфотографированных формах.
2. **Удобное управление политиками в разных средах.** Благодаря новой функции импорта и экспорта политик можно без труда переносить политики между экземплярами.
3. **Защита фрагментов документов в конечных точках.** Поиск по индексированным документам в конечных точках — это высокоэффективное средство обнаружения конфиденциальной информации как в оригинальных, так и в модифицированных версиях документов на основе идентификационного кода данных.
4. **Реализация более безопасных правил использования данных на компьютерах.** Копаненты обеспечивающие расширенную поддержку новых операционных систем, типов файлов и наиболее популярных приложений для обмена конфиденциальной информацией в организациях.
5. **Более детальное представление о данных, передаваемых по зашифрованным каналам.** Улучшенные функции мониторинга информации, передаваемой по SSL-соединениям, для веб-сайтов, электронной почты, FTP и мгновенных сообщений благодаря новым средствам интеграции DLP и продуктов для расшифровки данных SSL.

Ключевые преимущества

Максимально упрощена процедура защиты конфиденциальной корпоративной информации и обеспечения соответствия требованиям. Комплексный подход к защите информации учитывает расплывчатые границы современных систем безопасности, растущее число направленных атак, а также изменения в привычках и требованиях пользователей.

Расширяет область действия функций предотвращения утечки данных на облачные среды.

Расширяет границы применения политик обеспечения безопасности и соблюдения требований за пределы собственной сети.

Предоставляет проверенные методики развертывания, интуитивно понятные инструменты управления инцидентами и политиками, а также обширную поддержку каналов с высокой степенью риска при минимальной общей стоимости владения.

#### Межсетевой экран

Межсетевой экран (Firewall) – программное обеспечение для реализации контроля над сетевым траффиком и его маршрутизацией. Управление осуществляется на основе заданного набора правила (rule set). Типовое использование в серверной среде – это гранулированный контроль доступа к узлам, а также строгое регламентирование сетевого сообщения между разными узлами одного, масштабного программно-аппаратного комплекса. Для проектируемой Платформы применимы следующие требования.

1. Поддержка основных версий IP протокола, а именно IPv4 и IPv6;
2. Поддержка отслеживания состояния соединений (statefull firewall);
3. Поддержка спецификации портов TCP и UDP – source и destination;
4. Поддержка нескольких цепочек маршрутизации: input, forward, output;
5. Поддержка маркировки пакетов, также известной как packet tagging;
6. Возможность установки базовой политики доступа (accept/deny).

#### Политики резервного копирования

В части обеспечения информационной безопасности определяются политики резервного копирования.

Система резервного копирования данных – программное обеспечения для непрерывного резервного копирования данных (backup), предназначенное для развертывания в рамках Платформы. Данное ПО создает резервные копии как самих серверов, так и данных которые хранятся внутри СУБД и других подсистем хранения. Также данное ПО предусматривает инструментарий для развертывания в эксплуатацию резервных копий в случае надобности.

#### Web Application Firewall

Web application firewall - брандмауэр веб-приложения (WAF) — это компонент шлюза приложений, обеспечивающий централизованную защиту веб-приложений от распространенных эксплойтов и уязвимостей.

Ниже перечислены основные преимущества шлюза приложений и брандмауэра веб-приложения:

1. **Защита:**

* Защита веб-приложения от сетевых уязвимостей и атак без изменения в коде серверной части.
* Одновременная защита нескольких веб-приложений с помощью шлюза приложений.

1. **Мониторинг:**

* Выполняет мониторинг веб-приложения для защиты от атак, используя журнал WAF в режиме реального времени.

1. **Настройка:**

* Возможность настройки правил и групп правил WAF согласно требованиям приложения для уменьшения числа ложноположительных результатов.

Основные Функции:

* Защита от внедрения кода SQL.
* Защита от межсайтовых сценариев.
* Защита от распространенных сетевых атак, в том числе от внедрения команд, несанкционированных HTTP-запросов, разделения HTTP-запросов и атак с включением удаленного файла.
* Защита от нарушений протокола HTTP.
* Защита от аномалий протокола HTTP, например, отсутствия агента пользователя узла и заголовков accept.
* Защита от программ-роботов, программ-обходчиков и сканеров.
* Обнаружение распространенных неправильных конфигураций приложений (Apache, IIS и т. д.).

#### SSL/TLS сертификаты

SSL/TLS сертификат – это цифровая подпись доменного имени. SSL (Secure Sockets Layer) и TLS (Transport Level Security) сертификаты обеспечивают безопасное соединение и передачу данных между сервером и клиентом. Технология передачи данных гарантирует защиту, сохранность и целостность передаваемых данных.

Соединение, защищенное протоколом TLS, обладает одним или несколькими следующими свойствами:

1. **Безопасность:** симметричное шифрование защищает передаваемую информацию от прочтения посторонними лицами.
2. **Аутентификация:** "личность" участника соединения можно проверить с помощью асимметричного шифрования.
3. **Целостность:** каждое сообщение содержит код (Message Authentication Code, MAC), с помощью которого можно проверить, что данные не были изменены или потеряны в процессе передачи.

#### Виртуальная частная сеть

Виртуальная частная сеть (англ. Virtual Private Network, VPN) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений).

#### Двухфакторная аутентификация

Сервис двухфакторной аутентификации должен быть разработан таким образом, чтобы сделать кражу учётных данных пользователя бесполезной, и при этом не хранить пароли на стороне Сервиса.

При использовании Сервиса к учётным данным пользователя добавляется второй фактор аутентификации - одноразовый пароль, использование которого позволяет добиться того, что даже в случае перехвата злоумышленником учётных данных он не сможет ими воспользоваться, поскольку одноразовый пароль уже недействителен. Таким образом резко возрастает контролируемость доступа к информации.

Очевидно, что подбор или кража пароля в такой ситуации практически бессмысленны, что серьёзно затрудняет доступ к закрытой информации со стороны посторонних лиц.

Чтобы двухфакторная аутентификация была по-настоящему надёжной и соответствовала современным требованиям безопасности, необходимо выполнение ряда особых условий и требований к характеристикам системы.

Сервис должен предложить пользователю следующие возможности:

1. полный контроль над процессом аутентификации своих приложений;
2. отсутствие необходимости хранения таких учётных данных пользователя, как пароль, на стороне Сервиса;
3. возможность отправки журналов доступа на инфраструктуру пользователя;
4. возможность использовать простое и удобное мобильное приложение для генерирования одноразовых паролей;
5. поддержка основных производителей физических генераторов одноразовых паролей;
6. удобный API/SDK для встраивания Сервиса в работу приложений;
7. поддержку протоколов интеграции с внешними системами, таких как Radius и LDAP(s).

#### Система управления событиями информационной безопасности

Система управления событиями информационной безопасности SIEM – программное обеспечение или аппаратно-программный комплекс, предназначенные для автоматизированного выявления событий информационной безопасности и инцидентов информационной безопасности путем сбора и анализа журналов регистрации событий объекта информатизации. Требования к процессу журналирования событий описаны в пункте 10.3.3.5 Мониторинг по обеспечению информационной безопасности.

Таблица

|  |  |  |  |
| --- | --- | --- | --- |
| **Архитектурный уровень** | **Риски/Угрозы** | **Контроль** | **Описание** |
| Уровень сетей | Сетевые вторжения, DDos | IPS, IDS, NGFW | IPS - аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них;  IDS - программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими;  NGFW - Брандмауэр следующего поколения является частью технологии брандмауэра третьего поколения, сочетающей традиционный брандмауэр с другими функциями фильтрации сетевых устройств; |
| Уровень ППО | HTTP/HTTPS, SQL инъекции, недоступность, риск потери ключевых данных | WAF, IPS, NGFW, обновление конфигурации, резервное копирование. | WAF - защитный экран уровня приложений, предназначенный для выявления и блокирования современных атак на веб-приложения, в том числе и с использованием уязвимостей нулевого дня;  Резервное копирование - процесс создания копии данных на носителе, предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения. |
| Уровень СУБД | Fraud, недоступность, риск потери ключевых данных | Anti-fraud, контроль внесения изменений администратором, резервное копирование. | Anti-fraud - специализированные программные или программно-аппаратные комплексы, обеспечивающий мониторинг, обнаружение и управление уровнем фрода. |
| Уровень ОС | Эксплоиты, вирусы, использование флэш-накопителей, риск потери ключевых данных | DLP, Антивирусы виртуальных машин, обновление конфигурации ОС, резервное копирование. | Эксплоит - компьютерная программа, фрагмент программного кода, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему.  DLP - технологии предотвращения утечек конфиденциальной информации из информационной системы вовне. |
| Уровень среды виртуализации | Эксплоиты , Dos атаки, атаки на SDN, вирусы | Антивирус виртуальной среды, системы управления виртуальными сетями | Антивирусы виртуальной среды - для виртуальных и облачных сред обеспечивает безопасность на всех уровнях и этапах применения облачных структур. |
| Уровень физического доступа | Несанкционированный доступ | СКУД, Видеонаблюдение | СКУД – система контроля управления доступом |

### **Функциональные компоненты Big Data (анализ больших данных)**

Размещение программных продуктов автоматизации государственных органов на одной площадке предоставляет возможность разработки единого хранилища данных. Следствием реализации единого аналитического хранилища, станет консолидация больших объемов, данных порождаемых бизнес-процессами государственных органов на одной площадке. Единое хранилище данных предоставляет возможность мониторинга и контроля данных и процессов, в масштабе государства.

Данные из единого хранилища могут использоваться в процессе разработки программных продуктов автоматизации государственных органов, размещаемых в последствии в среде ИКП ЭП.

Цель реализации хранилища Big Data и инструментов для его наполнения и работы с ним – предоставление единого, контролируемого Сервисным Интегратором и Оператором источника данных для использования в системах поддержки принятия решений, аналитики и машинного обучения, разрабатываемых для автоматизации государственных органов.

Единое хранилище предоставляет разработчикам программных продуктов автоматизации государственных органов необходимые инструменты для реализации витрин данных и хранилищ, и их интеграции в разрабатываемые приложения.

В случаях, не противоречащих законодательству, к размещенным в ИКП ЭП витринам данных может быть предоставлен доступ для их использования при проектировании витрин и хранилищ в других системах. Это возможно, если данные не представляют собой государственную тайну или не содержат персональной информации граждан. Как пример, может быть предоставлен доступ к статистической информации обезличенного характера: объемы потребления определенных групп товаров в масштабе государства и подобные им.

Дополнительно функционал единого хранилища и инструментов для работы с ним позволит существенно снизить себестоимость разработки функционала аналитики в программных продуктах автоматизации государственных органов. Данный функционал будет предоставляться поставщикам программных продуктов автоматизации государственных органов как опциональная возможность для разработки хранилищ и витрин данных и процессов для заполнения их данными, в среде разработки и тестирования.

#### Инструменты BigData как сервисы Платформы

К сервисам BigData относятся: средства подготовки данных, построения аналитических моделей, создания отчетов и интерактивных информационных панелей, построения прогнозных математических моделей и искусственного интеллекта, интегрированные со средствами разработки, поддержки жизненного цикла программных продуктов автоматизации государственных органов, ИКП ЭП.

Как следствие использования предоставляемых ИКП ЭП инструментов для работы с большими данными и единого хранилища и самих данных, при разработке программных продуктов автоматизации государственных органов, будет существенно снижена себестоимость разработки сложных решений, работающих с большими объемами данных. Сократится и время разработки, за счет моментального развертывания необходимых модулей в облачной среде.

К таким инструментам относятся:

1. Инструменты моделирования витрин данных
2. Инструменты моделирования ETL процессов
3. Конструкторы отчетов

В целях экономии средств блок будет реализован путем развертывания в ИКП ЭП системы анализа Smart Data Ukimet.

##### Сервисы параллельной обработки

Необходимы для параллельной обработки больших данных и параллельного выполнения вычислительных аналитических задач. Представляют собой, отдельные программные модули, использующие API для доступа к сервисам хранения, так и опции обработки данных сервисов хранения.

### Мониторинг

#### **Мониторинг аппаратных ресурсов**

Для мониторинга ИКП ЭП будет использоваться существующая у Заказчика «Единая система мониторинга».

Необходимые метрики, применяемы для мониторинга hardware

1. мониторинг потери пакетов через интерфейсы;
2. мониторинг времени отклика на команду ping.
3. мониторинг трафика через сетевые интерфейсы устройства;
4. мониторинг загрузки сетевых интерфейсов;
5. использование оперативной памяти RAM;
6. загрузка центрального процессора CPU;
7. заполнение разделов жестких дисков HDD;
8. использование виртуальной памяти SWAP.
9. мониторинг СУБД, (критерий table spaсe, alert log).
10. мониторинг времени отклика http адреса ресурса;
11. мониторинг кода ответа на http запрос.

#### Компоненты мониторинга виртуальной инфраструктуры

Критерии к основным метрикам мониторинга виртуальных машин:

Группа General:

1. Device availability;
2. Configuration status;
3. Overall status;
4. System uptime;
5. Configuration status;
6. Guest heartbeat status;
7. Guest power status;
8. Heartbeat;
9. Overall status;
10. System uptime.

Группа CPU:

1. CPU usage (MHz)
2. CPU usage percentage
3. CPU usage (MHz)
4. CPU usage percentage
5. CPU Jumps
6. Context switches per second
7. Interrupts per seconds

Группа Memory:

1. memory swap usage
2. memory usage percentage
3. memory active
4. memory balloon
5. memory granted
6. memory swapin
7. memory swapout
8. memory usage percentage

Группа Disk:

1. disk usage
2. disk usage

Группа Network:

1. network usage
2. network usage
3. PcNet data receive rate
4. PcNet data transmit rate

#### **Мониторинг среды виртуализации на уровне ОС и ее компонентов**

Мониторинг среды виртуализации на уровне ОС и ее компонентов состоит из:

1. Сервиса сбора логов с запущенных контейнеров. Данный сервис должен осуществлять поиск запущенных контейнеров и при их обнаружении осуществлять подключение к интерфейсу сбора логов.
2. Сервиса сбора метрик с запущенных контейнеров и сбора метрик оркестратора. Данный сервис предназначен для сбора основных метрик таких как:

* количество контейнеров в кластере;
* количество сервисов в кластере;
* количество нод в кластере;
* количество дата центров в кластере;

По каждой ноде кластера необходимо собирать информацию:

* имя хоста;
* статус;
* доступность;
* принадлежность к дата центру;
* количество cpu;
* количество ОЗУ;

Также необходимо собирать подробную информацию о каждом запущенном контейнере:

* название контейнера;
* название сервиса;
* название образа;
* используемая ОЗУ;
* метка дата центра;
* входящий/исходящий трафик;
* количество IO операций чтении/записи;

1. Сервис сбора метрик с ПО запущенного внутри контейнеров. Данный сервис должен иметь плагинную архитектуру. В зависимости от установленных плагинов он должен обнаруживать процессы, запущенные внутри контейнера и использовать специализированные протоколы для сбора метрик специфичных для запущенных приложений.

Собранные логи собираются в файлы для передачи в Единую Систему Мониторинга

#### **Интеграция с Единой Системой Мониторинга**

Результаты мониторинга передаются сохраняются в лог-файлы, которые собираются Единой Системой Мониторинга.

#### Мониторинг по обеспечению информационной безопасности

Мониторинг безопасности объектов ИКП ЭП должен реализовываться в соответствие с Правилами проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры, утвержденными Приказом Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ и соответствовать Рисунку 14.



Рисунок 14 Схема взаимодействий с ИС ИБ

### Обеспечение отказоустойчивости

#### Поддержка синхронной репликации данных

Поддержка синхронной репликации данных зависит от ЛПО, используемого в ИС или СПП и размещенного на Платформе. Компоненты Платформы должны поддерживать синхронную репликацию данных.

#### Поддержка отказоустойчивости

Отказоустойчивость — свойство системы сохранять свою работоспособность после отказа одного или нескольких составных компонентов.

Отказоустойчивость определяется количеством любых последовательных единичных отказов компонентов, после которого сохраняется работоспособность системы в целом.

Базовый уровень отказоустойчивости подразумевает защиту от отказа одного любого элемента — исключение единой точки отказа.

Единая точка отказа - любая конфигурационная единица (функциональный компонент ИКП ЭП), отказ которой может вызвать инцидент, для которого не определена контрмера.

Для обеспечения данного требования платформа должна поддерживать развертывание ПО в географически распределенных дата центрах.

Основной способ повышения отказоустойчивости — избыточность. Наиболее эффективный метод избыточности — аппаратная избыточность, которая достигается путём резервирования. ИКП ЭП должна поддерживать резервирование вычислительных ресурсов как на уровне виртуализации (динамическое резервирование), так и на уровне контейнеризации (статическое резервирование).

Отказоустойчивость обеспечивается за счет резервирования аппаратных ресурсов Платформы и размещения управляющих компонентов ИКП ЭП на двух комплектах оборудования: основном и резервном. Резервные мощности используются оркестратором облака для восстановления на них вышедших из строя виртуальных машин.

#### Поддержка отказоустойчивости в среде виртуализации на уровне ОС и ее компонентов

Для реализации отказоустойчивости, среда виртуализации на уровне ОС предоставлять следующую функциональность:

* + 1. Поддержку инфраструктуры с множеством дата центров. Если ПО требует высокой отказоустойчивости и автоматического восстановления, то платформа должна развернуть такое ПО минимум в 3-х дата центрах.
    2. Сервис резервирования нод кластера для быстрой подмены нод в случае сбоя, если данный функционал не реализован средствами слоя классической виртуализации. Данный сервис должен отслеживать состояние нод текущего кластера. В случае выхода ноды из строя, сервис должен осуществить поиск резервной ноды в том же дата центре и скопировать все метки (labels) со сломанной ноды на резервную и после этого перевести её в активное состояние. Сломанную ноду необходимо деактивировать и если её восстановление невозможно, то удалить из кластера.

Оркестратор контейнерной платформы должен поддерживать два основных сценария обеспечения отказоустойчивости и масштабируемости системы:

1. Выход узлов системы (контейнеров) из строя;
2. Выход системных метрик за пределы критических значений.

В первом случае оркестратор обеспечивает развертывание вышедшего из строя контейнера на резервной ноде и включение его в соответствующий сервис информационной системы или СПП. Таким образом достигается отказоустойчивости системы.

Второй сценарий ориентирован на обеспечения автоматической масштабируемости.

Масштабируемость - означает способность системы, сети или процесса справляться с увеличением рабочей нагрузки (увеличивать свою производительность) при добавлении ресурсов.

Платформа контейнеризации должна предусматривать унифицированный способ масштабирования ПО развертываемого из реестра шаблонов развертывания. Также необходимо, чтобы образы развертываемого ПО были совместимы с алгоритмами масштабируемости используемыми в платформе контейнеризации.

Для поддержки динамической масштабируемости необходима согласованная работа 2-х уровней:

1. Уровень виртуализации должен иметь возможность выделять необходимое количество виртуальных ресурсов по запросу от уровня контейнеризации.
2. Уровень контейнеризации должен иметь возможность отслеживать основные показатели потребляемых ресурсов и основываясь на них, а также на подготовленных прогнозах запрашивать дополнительные ресурсы от системы управления виртуализацией.

#### Поддержка динамической масштабируемости

Масштабируемость означает способ системы, сети или процесса справляться с увеличением рабочей нагрузки (увеличивать свою производительность) при добавлении ресурсов.

Достигается за счет резервирования ресурсов, на которые по мере возрастания нагрузки на компонентах Платформы оркестратор облака размещает дополнительные узлы кластера данных компонентов.

#### Поддержка динамической масштабируемости средствами среды виртуализации уровне ОС

Оркестратор среды виртуализации на уровне ОС (оркестратор контейнеров) должен посредством специально разработанных программных агентов, осуществлять мониторинг основных метрик на нодах сервисов среды виртуализации уровня ОС. Основные метрики:

1. Утилизация CPU
2. Утилизация оперативной памяти
3. Утилизация дискового пространства

В шаблонах развертывания (см. документ «Архитектура среды разработки и тестирования») для элементов инфраструктур программных продуктов указываются погоровые значения данных метрик, при которых оркестратор должен осуществить масштабирование – добавить ноды в сервис. Ноды добавляются из резервного пула среды виртуализации на уровне ОС. При снижении нагрузки (значений контролируемых метрик), оркестратор должен освободить ноды и вернуть их в резервный пул.

### Оркестрация облака

Оркестрация облака связывает функциональные компоненты ИКП ЭП, позволяя автоматизировать взаимодействие между процессами служб облачных вычислений и создавать сложные, комбинированные службы. Оркестратор облака связывает функции, предоставляемые различными службами облачных вычислений во взаимосвязанные, кросс-уровневые процессы (workflow).



**Рисунок 15 – Оркестрация облака**