Программно-техническое обеспечение развития ЕСИМО с учетом импортозамещения программно-технических средств и технологий (ФГБУ «ВНИИГМИ-МЦД», январь 2023 г.)

1 Применение облачной технологии

Ключевым элементом модернизации ЕСИМО и ее элементов является использование технологии облачных вычислений, что позволит решить принципиальную проблему ЕСИМО – устаревание и отказ локальной вычислительной техники, отсутствие квалифицированных кадров для поддержки программно-аппаратных комплексов на местах. Для ресурсного обеспечения сетевых сегментов ЕСИМО (центральный, СЗА, ДВ) планируется применить возможности дата-центров Государственной единой облачной платформы (ГЕОП, «ГосОблако»).

Переход ЕСИМО на применение облачных вычислений и других сквозных цифровых технологий не нарушит ранее установленный порядок предоставления информации и будет способствовать применению более работоспособных и менее затратных технологий.

Сетевые узлы ЕСИМО (РЦИТУ, РИТУ СЗА, РИТУ ДВ) будут предоставлять вычислительные мощности и другие ресурсы виртуальным узлам системы, эксплуатируемым ведомственными центрами ЕСИМО.

Предоставление услуг сетевыми узлами планируется выполнять с применением сервисной модели SaaS (от английского, Software-as-a-service, программное обеспечение как услуга), в рамках которой все работы будут виртуализированы и будут выполняться в облаке.

Модель SaaS реализуется путем предоставления доступа к ПО ВП ЕСИМО следующих категорий:

- ПО выполнения базовых и прикладных функций центрами (поставщиками информации) ЕСИМО;
- ПО реализации прикладных функций пользователями ЕСИМО.

Модель SaaS используется как основа решений по системному ландшафту ЕСИМО, её ключевые особенности в этом контексте состоят в следующем:

 Нормативный аспект. Пользователи ЕСИМО применяют программные компоненты и модули, данные на основе соглашений с оператором сетевых узлов системы;

 Техническая поддержка. Облачный провайдер ГЕОП предоставляет для функционирования ЕСИМО и обслуживает вычислительное и телекоммуникационное оборудование, общее ПО. Оператор сетевого узла ЕСИМО предоставляет и обслуживает общее и специализированное ПО, функциональные базовые и прикладные программные приложения, хранилища данных и метаданных сетевых и присоединенных виртуальных узлов системы;

 Многократное применение. Обеспечивается многопользовательский дистанционный доступ к вычислительным и информационным ресурсам сетевых узлов ЕСИМО как к виртуальным узлам единой системы;

 Унифицированность. Применяются: 1) единая система идентификации пользователей ЕСИМО; единая система средств и мер по обеспечению безопасности информации ЕСИМО; единая схема доступа: безусловный режим, выбранный период, постоянная лицензия;

 Снижение затрат. Инфраструктурная составляющая (серверы, ОПО, инженерные коммуникации и телекоммуникационная инфраструктура) предоставляется дата-центрами ГЕОП на длительный период, поддерживается только на стороне сетевых узлов системы, прикладная составляющая в формате виртуальных АРМ Администраторов/Операторов/Пользователей (конечных) не требуют инфраструктурных затрат. Очевидно, что ИТ компетенции персонала по сопровождению и применению ЕСИМО должны быть высокими только в контексте операторов сетевых узлов ЕСИМО;

 Доступность. Доступ к продуктам сетевых узлов ЕСИМО можно будет получить из любого места, где есть доступ к общим (Интернет) и (или) закрытым (СПД МО РФ) каналам связи;

 Масштабируемость (горизонтальная и вертикальная). Состав и вычислительные и информационные мощности виртуальных узлов назначаются настройками средств сетевых узлов подсистемы, исключая трудоёмкие и дорогостоящие процессы ввода в действие физических АПК.

Ограничением является состав и объем вычислительных и телекоммуникационных мощностей ЕСИМО в ГЕОП, используемых виртуальными узлами. При этом операторы сетевых узлов ЕСИМО могут быстро изменить источники и объем потребления данных и услуг в любой момент;

 Безопасность. Децентрализованный характер облачных технологий защищает данные пользователей SaaS-сервисов от несанкционированного доступа. Конфиденциальная информация в таких областях, как морские операции, добыча водных биоресурсов, добыча на шельфе и транспортировка газа и нефти попадает в защищённые хранилища данных ЕСИМО как составляющая критических информационных ресурсов Российской Федерации;

 Удобство. Графические интерфейсов пользователей будут спроектированы на основе опыта ЕСИМО, а также с расчетом на широкую аудиторию, поэтому даже технически сложными приложениями в большинстве случаев можно будет пользоваться с минимальным запасом IT-компетенций;

 Совместимость. SaaS будет содержать средства взаимодействия и взаимосовместимости компонентов узлов системы между собой и с внешними информационными платформами и источниками данных. Тем самым модель будет хорошо приспособлена для решения экосистемных задач в области данных и услуг об обстановке в Мировом океане.

Функционирование модели SaaS основано на фундаментальном архитектурном подходе – мультиарендности (*multitenancy)*, где экземпляр программного комплекса (приложения) обслуживает множество организаций-клиентов («арендаторов»), в применение к ЕСИМО множество центров и поставщиков информации, пользователей единой системы. В общем случае каждый клиент, использующий платформу SaaS, считается арендатором и получает права доступа, действуя по соглашению (контекст центров ЕСИМО) или оплачивая подписку (коммерческий контекст применения сервисов клиентом).

В этой связи различают однопользовательскую и многопользовательскую архитектуру сервиса.

Однопользовательская архитектура предусматривает выделение своих экземпляров программного обеспечения, инфраструктуры, серверов и баз данных для каждого арендатора.

Многопользовательская архитектура является наиболее предпочтительным типом архитектуры приложений SaaS в применении к ЕСИМО и ее военной подсистемы. По определению каждый отдельный экземпляр этой модели SaaS обслуживает более одного арендатора. Это означает, что все клиенты совместно используют общую базу данных и приложения.

2 Вычислительное оборудование

Предварительный состав оборудования для создания сетевого узла ЕСИМО включает:

- Сервер – 6 шт.;
- Система хранения данных – 2 шт.;
- Коммутатор сети хранения – 2 шт.;
- Межсетевой экран – 2 шт.;
- Коммутатор локальный сети – 2 шт.;
- Источник бесперебойного питания – 6 шт.;

– Шкаф телекоммуникационный – 2 шт.;

– Рабочие станции – 4 шт.;

– Предоставление неисключительных прав на систему управления средой виртуализации – 6 шт.;

– Предоставление неисключительных прав на операционную систему – 22 шт.

Согласно предварительной оценке, суммарные вычислительные ресурсы и ресурсы хранения для организации узлов ЕСИМО должны быть не ниже следующих:

– виртуальный процессор vCPU (с учетом гипертрейдинга) – 1 300;

– виртуальная оперативная память vRAM (ГБ) – 2 700;

– виртуальное дисковое пространство (ГБ) – 20 2000.

3 Общее программное обеспечение (ПО, ОПО)

При модернизации ЕСИМО при назначении ОПО должны учитываться требования, связанные с импортозамещением и сертификацией ПО, применяемого в интересах Минобороны России. Предлагается применять следующие принципы:

– использовать версии ОПО, которые присутствуют в официальном репозитории выбранной операционной системы (ОС) с обеспечением сертификации ФСТЭК и МО РФ;

– при отсутствии в официальном репозитории необходимого программного обеспечения используется ОПО из единого реестра программного обеспечения Минцифры России (URL: https://reestr.digital.gov.ru/);

– при отсутствии необходимого программного обеспечения в едином реестре используется современные зарубежные версии ОПО с открытой лицензией и прорабатываются вопросы регистрации и сертификации продукта.

Предварительный стек продуктов системного ОПО включает:

− операционная система – AstraLinux или аналогичная российская ОС семейства Linux;

− среда функционирования – LibericaJDK, OpenJDK, сервер приложений – WildFly или аналогичная российская;

− ПО виртуализации zVirt;

− ПО контейнеризации Docker или аналогичное российское;

Системное ОПО обеспечивает работу:

– технология контейнеризации, обеспечивающая эффективное применение аппаратных ресурсов в плане минимизации состава виртуальных машин;

– технология микросервисов, позволяющая решить проблемы поддержки и развития монолитных программных комплексов ЕСИМО посредством применения независимых и не связанных между собой сервисов;

– технология параллельного использования сервисов цифровой платформы для обеспечения работы операторов одновременно в случае использования виртуальных центров;

– технологии хранения больших данных и искусственного интеллекта.

Инструментальное ОПО предназначено для автоматизации выполнения функциональных задач по работе с информацией и использования специализированного ПО. Предварительный стек продуктов инструментального ОПО включает:

– среда управления (прием, обработка/трансформация, передача) данными и сообщениями – Apache NiFi или аналогичная российская;

– среда диспетчеризации сообщений и микросервисов (сервисная шина) – Apache Kafka или аналогичная российская;

– среда индексирования информации – OpenSearch, ElasticSearch или аналогичная российская;

– провайдер авторизации, аутентификации и SSO Keycloak или аналогичный российский продукт;

– среда управления информационным производством Camunda или аналогичная российская;

– средство подготовки визуальных графических представлений Grafana или аналогичное российское ПО;

– система мониторинга аппаратных и программных ресурсов – Zabbix или аналогичная российская.

Инструментальное ОПО предоставят следующие платформы:

– информационно-коммуникационная платформа в составе Apache NiFi, Apache Kafka или их аналогов, реализующая сквозные локальные и распределенные back-end процессы управления данными и метаданными, системной технической информацией по всему функционалу ЕСИМО;

– платформа расчетов и моделирования в составе Camunda, Apache Kafka, Apache Nifi, Apache Spark, Geoserver, Grass и расчетно-модельные библиотеки на языке R или их аналоги, реализующая back-end локальные и распределенные процессы обработки данных и информационного производства;

– платформа мониторинга в составе Apache Kafka, Zabbix, cAdvisor или их аналогов, реализующая back-end локальные и распределенные процессы контроля и централизованного сбора метрик и показателей работы сети, оборудования и ПО, актуальности и доступности данных и сервисов ЕСИМО;

– платформа визуализации в составе React, Grafana или их аналогов, реализующая единые в контексте средств и стилей табличного, графического и картографического отображения информации front-end процессы по всему функционалу ЕСИМО, включая системную техническую информацию;

– платформа ведения разработки в составе Jira, Git или их аналогов, обеспечивающая автоматизацию процесса разработки, правки, обслуживания и резервного восстановления ПО;

ОПО реализует сквозные цифровые технологии:

– облачная технология, предоставляющая базовые методы и средства построения новой архитектуры присоединенной сети узлов (виртуальных и (или) физических);

– технология больших данных (Big Data), реализующая хранение и обработку большого объема структурированной и неструктурированной информации в реальном времени;

– технология искусственного интеллекта, применяющая средства формирования и представления знаний в виде экспертных систем и машинное обучение для реализации алгоритмов и средств интерактивного отображения информации сервисами цифровой платформы.

СПО будет состоять из программных приложений, разработанных в среде ОПО и использующих функции из набора платформ инструментального ОПО:

– базовые средства для осуществления функциональных задач ЕСИМО;

– прикладные средства для осуществления прикладных задач.

Функциональная составляющая базовых средств состоит их сгруппированных по функциям средств общего и специализированного программного обеспечения процессов:

– Сбор и интеграция данных;
– Информационное производство;
– Информационная безопасность;
– Информационное обслуживание;
– Управление работой системы.

Архитектура программного обеспечения и основные бизнес-процессы (workflow) типового сетевого узла ЕСИМО показана на рисунке 1.

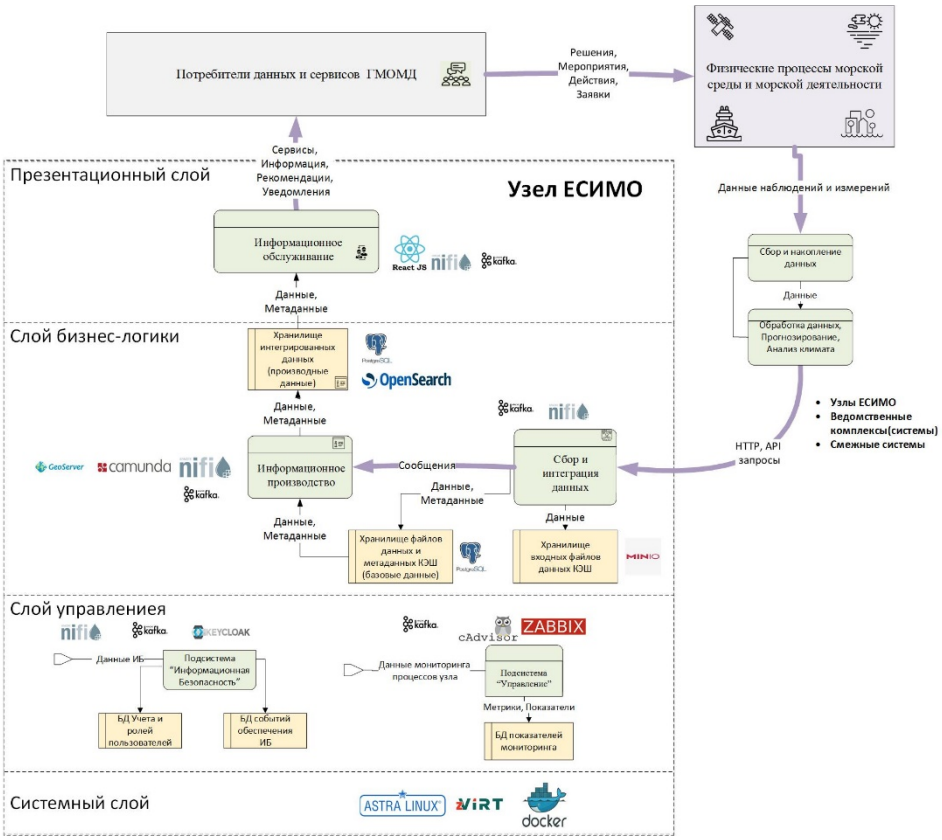

Рисунок 1 - Архитектура программного обеспечения типового сетевого модернизированного узла ЕСИМО

Процессы управления данными выполняются в режиме реального времени или в задержанном режиме в зависимости от специфики данных с применением потоковой (конвейерной) обработки данных, основанной на сквозном принципе: процессы отдельного потока данных формируются подсистемой сбора и интеграции данных и завершаются предоставлением данных и сервисов в рамках гидрометеорологического обеспечения (ГМО) подсистемой информационного обслуживания. Бизнес-процессы ЕСИМО будут выполняться конвейерами обработки, сгенерированными средствами платформ ЕСИМО и применяющими компоненты (модули) подсистем как прикладные обработчики данных.

Для реализации ГМО осуществляются сквозные потоки данных с сегментами (рисунок 2):

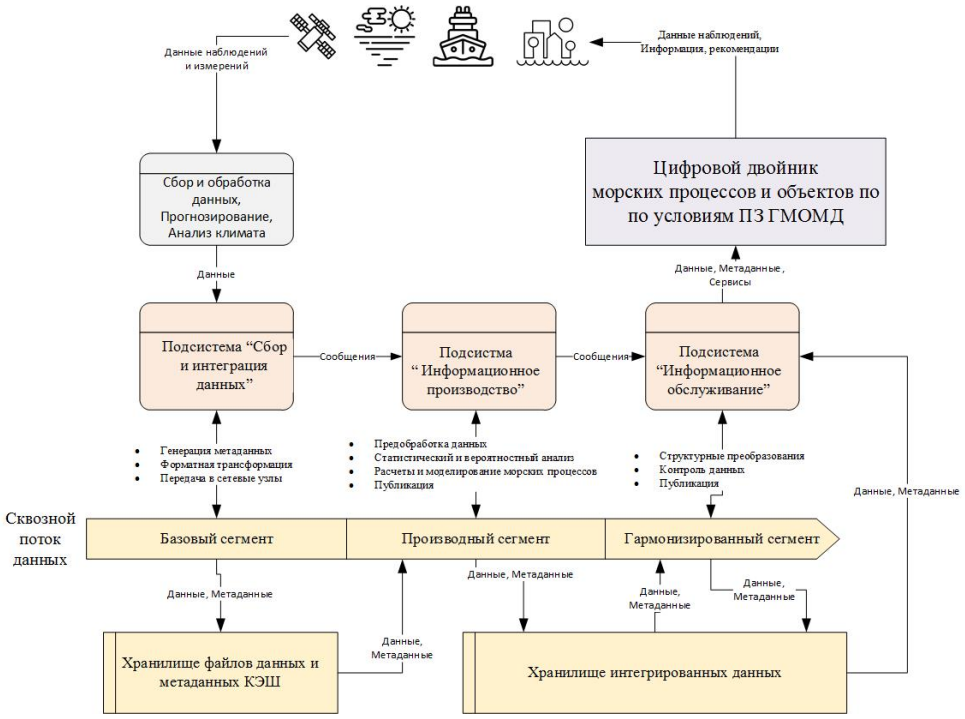

Рисунок 2 – Общая схема управления и конвейерной обработки данных средствами сетевого узла модернизированной ЕСИМО

– подсистема сбора и интеграции данных ведет процессы сбора и унификации данных источников с сохранением входных файлов данных и данных в виде целевых информационных ресурсов ГМО (базовый сегмент потока) в КЭШ хранилищах. Применяется информационно-коммуникационная платформа;

– подсистема информационного производства обрабатывает базовые данные по алгоритмам гармонизации и обогащения данных, получает новые данные (производный сегмент потока), ведет хранилище интегрированных данных. Для получения производных данных применяется информационно-расчетная платформа;

– подсистема информационного обслуживания будет играть роль маркетплейса потребителей и поставщиков данных и сервисов. Интерфейсная (front-end, навигация, управление и отображения процессов) составляющая и бизнес-процессы (back-end, база знаний, поддержки решений) виртуального представления цифрового двойника выполняются средствами прикладных сервисов соответствующих прикладных задач ГМО

(гармонизированный сегмент потока). Для процессов собственно обслуживания применяется информационно-визуализационная платформа;

– подсистема информационной безопасности узла ЕСИМО включает средства: 1) защиты от несанкционированного доступа к информации; обеспечение безопасного межсетевого взаимодействия, антивирусная защита, обнаружение вторжений; 2) контроля защищенности информации, доступности информации, криптографической защиты информации. Для организации процессов подсистемы применяется информационно-коммуникационная платформа;

– подсистема управления системой содержит средства, выполняющие техническое сопровождение аппаратно-программного комплекса и обеспечение его работоспособности, обратную связь с потребителями информации (услуг) ГМО, ведение отчетности о состоянии и производительности ЕСИМО. Для организации процессов подсистемы применяется информационно-коммуникационная платформа.