МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования
Московский технический университет связи и информатики

В.А. Докучаев, С.В. Запольских, В.В. Маклачкова, В.М. Матросов, А.В. Шведов, О.В. Щербина

АРХИТЕКТУРА ЦИФРОВЫХ ПЛАТФОРМ ДЛЯ ЗАЩИЩЁННЫХ ЦОД

Часть 1

ОБЩИЕ ПОДХОДЫ И ИСПОЛЬЗУЕМЫЕ ТЕХНОЛОГИИ

Учебное пособие

Москва 2021

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования
Московский технический университет связи и информатики

В.А. Докучаев, С.В. Запольских, В.В. Маклачкова, В.М. Матросов, А.В. Шведов, О.В. Щербина

АРХИТЕКТУРА ЦИФРОВЫХ ПЛАТФОРМ ДЛЯ ЗАЩИЩЁННЫХ ЦОД

Часть 1

ОБЩИЕ ПОДХОДЫ И ИСПОЛЬЗУЕМЫЕ ТЕХНОЛОГИИ

Учебное пособие

Направления подготовки:
05.12.13; 05.13.00; 05.13.01; 09.03.02; 09.04.01; 10.03.01; 11.03.02;11.04.02

Москва 2021

УДК 004

В.А. Докучаев, С.В. Запольских, В.В. Маклачкова, В.М. Матросов, А.В. Шведов, О.В. Щербина / Под ред. д.т.н., проф. В.А. Докучаева

Архитектура цифровых платформ для защищённых ЦОД. Ч. 1. Общие подходы и используемые технологии: учебное пособие / МТУСИ. – М., 2021. – 90 с.

Учебное пособие по дисциплинам «Архитектура центров обработки данных», «Основы построения защищенных инфокоммуникационных систем», «Архитектура информационных систем», «Принципы построения и архитектура информационных систем», «Системы сопровождения и поддержки инфокоммуникационных услуг», «Специальные средства контроля и мониторинга информационных систем», «Корпоративные инфокоммуникационные системы и услуги», «Теория построения инфокоммуникационных сетей и систем», «Администрирование в инфокоммуникационных системах», «Основы бизнес аналитики», «Основы построения современных систем хранения данных», «Технологии и средства облачных сервисов»:

для направлений подготовки бакалавров:
09.03.02 – «Информационные системы и технологии», профиль подготовки: «Информационные системы и сетевые технологии»;
10.03.01 – «Информационная безопасность»;
11.03.02 – «Инфокоммуникационные технологии и системы связи», профиль подготовки: «Инфокоммуникационные технологии в услугах связи».

для направлений подготовки магистров:
09.04.01 – «Информатика и вычислительная техника», профиль подготовки: «Распределённые информационно-коммуникационные системы и приложения»;
11.04.02 – «Инфокоммуникационные технологии и системы связи», профиль подготовки: «Программно-конфигурируемые инфокоммуникационные системы и сети».

для направлений подготовки аспирантов:
05.12.13 – Системы, сети и устройства телекоммуникаций;
05.13.00 – Информатика, вычислительная техника и управление;
05.13.01 – Системный анализ, управление и обработка информации (по отраслям).

В издании представлены материалы для освоения указанных выше дисциплин.

Ил. 22, табл. 2, список лит. 13 назв.

Издание утверждено Методическим советом университета в качестве учебного пособия. Протокол № 2 от 14.12.2021.

Рецензенты: Д.В. Гадасин, к.т.н., доцент (МТУСИ)

В.В. Шабанов, нач. департамента (НО АПОС)

Список сокращений

АРМ	Автоматизированное рабочее место
АПМДЗ	Аппаратный модуль доверенной загрузки (аппаратно-программное средство доверенной загрузки)
АСЗИ	Автоматизированная система в защищенном исполнении
БД	База данных
ВМ	Виртуальная машина
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
ЕГССПУ	Единая государственная система стратегического планирования и управления
ЗОС	Защищённая операционная система
ИР	Информационные ресурсы
КСА	Комплекс средств автоматизации
НСД	Несанкционированный доступ
НИОКР	Научно-исследовательская и опытно-конструкторская работа
ОС	Операционная система
ПСЗИ	Программное средство защиты информации
ПО	Программное обеспечение
СЗИ	Средства защиты информации
СОА	Система обнаружения компьютерных атак
СУБД	Система управления базой данных
СЦ	Ситуационный центр
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЦОД	Центр обработки данных
ЦПП	Цифровая программная платформа

Если враги нас ругают, значит
мы всё правильно делаем

Введение

В настоящее время человечество живет в условиях перехода от постиндустриальной к информационной стадии развития. Данный переход характеризуется следующими обстоятельствами:

- увеличение объема мировых данных по экспоненте - «информационный взрыв» (рисунок 1);
- быстрое «сжатие» времени (снижение сроков ввода в эксплуатацию новых технологий);
- доля цифровой экономики в развитых странах ежегодно растет на 3-7%;
- материальные затраты на получение, хранение, передачу и обработку данных уже превышают аналогичные расходы на энергетику.

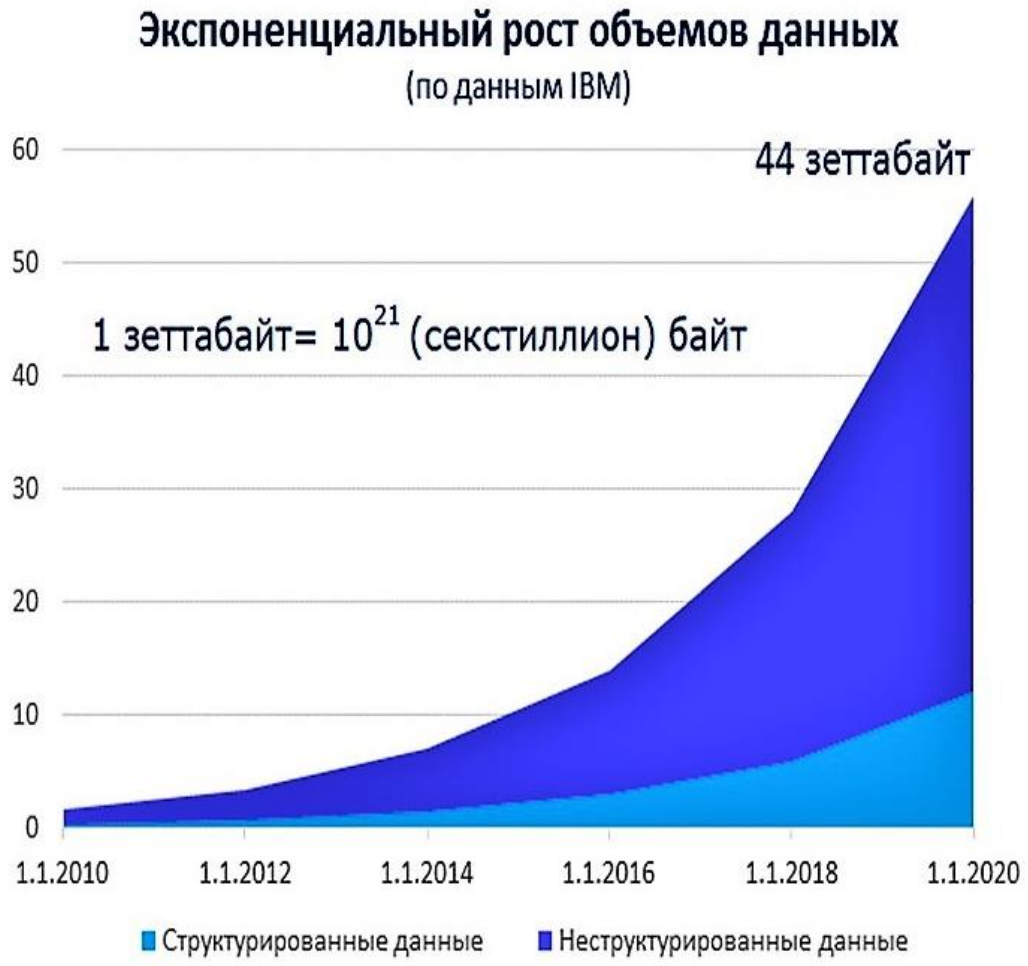

Рисунок 1 – Рост объёмов данных в мире

Таким образом:

- цифровые данные стали неотъемлемой частью любого бизнес-процесса;
- экономические связи, торговля, логистика, оказание государственных услуг и т.п. немыслимы без использования информационных технологий;
- потеря данных, искажение информации, несвоевременная ее обработка приводят к экономическим, финансовым, репутационным и иным потерям (ущербу).

Без специальных информационных технологий справиться с такой лавиной информации невозможно, для этого нужны специальные средства получения, хранения, передачи, обработки и защиты информации (в том числе ЦОД).

Защищенный ЦОД – это специализированный объект, представляющий собой связанную систему программной, информационно-телекоммуникационной (ИТ), инженерной инфраструктуры и инфраструктуры информационной безопасности, оборудование и части которых размещены в здании или помещении, подключенном к внешним сетям, как инженерным, так и телекоммуникационным (рисунок 2).

Рисунок 2 – Рост объёмов данных в мире

Защищенные ЦОД обеспечивают решение следующих задач:

- оперативный сбор, обработку и долговременное хранение данных;
- решение информационных и аналитических задач;
- информационную безопасность;
- оптимальное и масштабируемое размещение серверного и коммутационного оборудования;
- интеграцию с устойчивыми и скоростными каналами связи и передачи данных;
- гарантированные климатические условия, электроснабжение и заземление;
- комплексную защиту и охрану объектов и прилегающих территорий.

Разработка и техническая поддержка отечественных защищенных цифровых программных платформ является в настоящее время одной из наиболее актуальных задач, особенно в условиях цифровой трансформации общества и организаций.

Данное направление деятельности предопределено целями и задачами, указанными в программе «Цифровая экономика Российской Федерации» (утвержденная распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р), в которой зафиксировано, что «эффективное развитие рынков и отраслей (сфер деятельности) в цифровой экономике возможно только при наличии развитых платформ, технологий, институциональной и инфраструктурной сред».

В этой связи участие в развитии цифровой экономики, в том числе в сфере создания защищенных территориально распределенных центров обработки данных, является одной из приоритетных задач.

В настоящее время защищенные цифровые инфокоммуникационные платформы находят всё более широкое применение в деятельности многих Федеральных Регуляторов, государственных корпораций, крупных коммерческих организаций.

На базе таких платформ развёртываются ситуационные центры, успешно функционируют многоуровневые защищенные автоматизированные системы технического контроля обстановки, бизнес- и технологических процессов.

В качестве примера можно привести успешные нагрузочные испытания цифровой платформы «СинтезМ» российской компании АО «Финтех», которая рекомендована к использованию в системе взимания платы «ПЛАТОН» и деятельности ОАО «РЖД».

Особое внимание при развертывании цифровых инфокоммуникационных систем уделяется организации информационного взаимодействия с международными, федеральными, отраслевыми и иными автоматизированными и информационными системами.

Так, например, разрабатываются технологии и отрабатываются протоколы защищенного взаимодействия с такими системами, как: Национальные центры управления различных ФОИВ, Национальный центр управления кризисными ситуациями МЧС России, Отраслевая система мониторинга Росрыболовства, Информационная система «МоРе», Межведомственные региональные информационно-координационные центры и другие.

Вместе с тем, как показывает практика, при осуществлении цифрового взаимодействия между разрозненными системами существует большое число проблемных вопросов, на которые необходимо дать ответы. Перечислим основные из них:

– в масштабах государства отсутствуют унифицированные протоколы информационно-логического и технического взаимодействия, что существенно затрудняет двусторонний обмен данными между сопрягаемыми системами;

– существует различие в механизмах описания данных во взаимодействующих системах, что приводит к необходимости проведения дополнительных работ, а чаще к невозможности автоматического нормирования данных и, как следствие, к привлечению ручного труда для их обработки;

– отсутствует унифицированная система классификации и кодирования информации, ведения словарей, справочников и нормативно-справочной информации. Это приводит к невозможности автоматической обработки данных, получаемых из взаимодействующих систем;

– существует хорошо известная проблема с синхронизацией территориально-распределённых БД, без разрешения которой

организовать применение сквозных цифровых технологий на всю глубину управления органов власти и организаций весьма затруднительно;

– существует различие в классах защиты автоматизированных (информационных) систем, применяемых в них политик безопасности, правил разграничения доступа пользователей к защищаемой информации. Это накладывает значительные ограничения на порядок информационного обмена между ними;

– в настоящее время проведение любых работ на аттестованных системах приводит к необходимости их переаттестации и, как следствие, к привлечению предприятий-разработчиков, что в условиях динамической цифровой трансформации общества и экономики ведет к существенному ее замедлению и значительным неэффективным финансовым затратам.

Данное учебное пособие «Архитектура цифровых платформ для защищённых ЦОД» состоит из трёх частей:

часть 1 - Общие подходы и используемые технологии;

часть 2 - Применение платформы «СинтезМ» для построения технологической компоненты защищённых ЦОД;

часть 3 - Применение платформы «СинтезМ» для построения информационной инфраструктуры защищённых ЦОД;

Изучив все три части учебного пособия, студенты получат не только теоретические знания о представленных на российском рынке отечественных цифровых программных платформах и операционных системах, но также получат практические навыки в части установки, администрирования и использования цифровой программной платформы «СинтезМ», которая предназначена для создания территориально-распределённых защищённых ЦОД и АСЗИ.

Авторы выражают искреннюю благодарность руководству компании АО «ФИНТЕХ» и лично генеральному директору компании господину Лосеву В.Я. за предоставленные материалы, использованные в настоящем учебном пособии.

1. Основные цифровые платформы и операционные системы, разработанные в Российской Федерации

Объявленный государством курс на импортозамещение вдохнул новую жизнь в рынок программных платформ отечественной разработки. За последние несколько лет он пополнился множеством интересных продуктов — как оригинальных и созданных с чистого листа, так и построенных на основе Open Source-решений.

О необходимости форсированного развития отечественного рынка программного обеспечения (ПО), достижения максимальной независимости от иностранных разработок в сфере высоких технологий и сохранения информационного суверенитета впервые на высшем уровне заговорили в 2014 году, когда санкции США и Евросоюза резко повысили риски, связанные с применением зарубежного ПО в бизнесе и государственных организациях. Именно тогда в Министерстве связи и массовых коммуникаций РФ всерьёз озадачились решением этого стратегически значимого вопроса вместе со стимулированием спроса на национальные продукты и проработкой соответствующих мер поддержки отечественных разработчиков. Как результат — в кратчайшие сроки на законодательном уровне были утверждены ограничения на допуск иностранного ПО при осуществлении государственных и муниципальных закупок, а также правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных. Всё это положительным образом отразилось на рынке программного обеспечения в России, который за последнее время пополнился множеством интересных проектов и разработок. В том числе и в области операционных систем (ОС) и цифровых программных платформ (ЦПП).

Существуют два подхода к созданию российского ПО. Первый заключается в написании исходного кода продуктов с нуля, полностью силами отечественных специалистов. Второй вариант предполагает создание национального ПО на основе доработки заимствованных исходных кодов. Именно его и придерживаются многие работающие на ниве импортозамещения российские компании-производители ПО.

Наиболее критическим параметром разрабатываемого ПО являются защита данных, которые с его помощью будут обрабатываться, и возможность виртуализации как современного средства обеспечения

информационной безопасности, масштабируемости, конфигурирования и т.д.

Отметим, что приведённый в учебном пособии список ОС и ЦПП не является исчерпывающим. Работы в данном направлении ведут ООО «Р-Платформа», Раменское приборостроительное конструкторское бюро (входит в концерн «КРЭТ» Ростеха) и другие компании.

1.1. «Альт Линукс СПТ»

Разработчики: ООО «Свободные программы и технологии», «Базальт СПО» (сайт продукта: https://basealt.ru).

«Альт Линукс СПТ» представляет собой унифицированный дистрибутив на базе Linux для серверов, рабочих станций и тонких клиентов со встроенными программными средствами защиты информации, который может быть использован для построения автоматизированных систем по классу 1В включительно и информационных систем персональных данных (ИСПДн) по классу 1К включительно.

ОС позволяет одновременно хранить и обрабатывать на одном персональном компьютере или сервере конфиденциальные данные, обеспечивать многопользовательскую работу с разграничением доступа к информации, работать с виртуальными машинами, а также использовать средства централизованной авторизации.

Выданный ФСТЭК России сертификат подтверждает соответствие продукта требованиям следующих руководящих документов: «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации» — по четвертому классу защищённости; «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларированных возможностей» — по третьему уровню контроля и технических условий.

Техническая поддержка пользователей «Альт Линукс СПТ» осуществляется компанией «Свободные программы и технологии» через партнёра-разработчика «Базальт СПО».

1.2. Платформа «Альт»

Разработчик: компания «Базальт СПО» (сайт продукта: https://basealt.ru).

Платформа «Альт» — это набор Linux-дистрибутивов уровня предприятия, позволяющих развернуть корпоративную IT-инфраструктуру любого масштаба.

В состав платформы входят три дистрибутива.

- Универсальный «Альт Рабочая станция», включающий в себя операционную систему и набор приложений для полноценной работы.
- Серверный дистрибутив «Альт Сервер», который может предоставлять три вида контроллеров домена (Samba-DC (контроллер домена Active Directory), FreeIPA, ALT-домен) и реализовывать поддержку групповых политик для интеграции в инфраструктуру Active Directory, а также содержит максимально полный набор служб и сред для создания корпоративной инфраструктуры (СУБД, почтовый и веб-сервер, средства аутентификации и организации групповой работы, управления виртуальными машинами и мониторинга и ряд других инструментов).
- «Альт Образование 8», ориентированный на повседневное использование при планировании, организации и проведении учебного процесса в учреждениях общего, среднего и высшего образования.

Помимо этого, в серии продуктов компании «Базальт СПО» представлены сертифицированный дистрибутив «Альт Линукс СПТ» и операционная система для домашних пользователей Simply Linux.

1.3. «ОСь»

Разработчик: Национальный центр информатизации (входит в госкорпорацию «Ростех», сайт продукта: отсутствует).

Российский проект по созданию экосистемы программных продуктов на базе дистрибутива Linux, предназначенных для комплексной автоматизации рабочих мест и ИТ-инфраструктуры организаций и предприятий, в том числе в дата-центрах, на серверах и клиентских рабочих станциях.

Платформа представлена в вариантах «ОСь.Офисная» и «ОСь.Серверная». Они различаются наборами включённого в дистрибутив прикладного ПО.

Офисная редакция продукта содержит собственно операционную систему, средства защиты информации, пакет программ для работы с документами, почтовый клиент и браузер. В состав серверной версии включены: операционная система, средства защиты информации, инструменты мониторинга и системного управления, сервер электронной почты и СУБД.

Достоверная информация о состоянии разработки операционной системы «ОСь» по состоянию на июнь 2021 года отсутствует.

1.4. Astra Linux

Разработчик: НПО «Русские базовые информационные технологии» (РусБИТех, сайт продукта: https://astralinux.ru).

Разработка научно-производственного объединения «РусБИТех», представленная в двух вариантах: Astra Linux Common Edition (общего назначения) и Astra Linux Special Edition (специального назначения).

Особенности последней версии ОС: развитые средства обеспечения информационной безопасности обрабатываемых данных, механизм мандатного разграничения доступа и контроля замкнутости программной среды, встроенные инструменты маркировки документов, регистрации событий, контроля целостности данных, а также прочие обеспечивающие защиту информации компоненты.

Astra Linux Special Edition — программная платформа, сертифицированная одновременно в системах сертификации средств защиты информации ФСТЭК России, ФСБ России, Минобороны РФ и позволяющая обрабатывать в автоматизированных системах всех министерств, ведомств и других учреждений Российской Федерации информацию ограниченного доступа, содержащую составляющие государственную тайну сведения с грифом не выше «совершенно секретно».

Поддерживаемые Astra Linux аппаратные платформы представлены на рисунке 3.

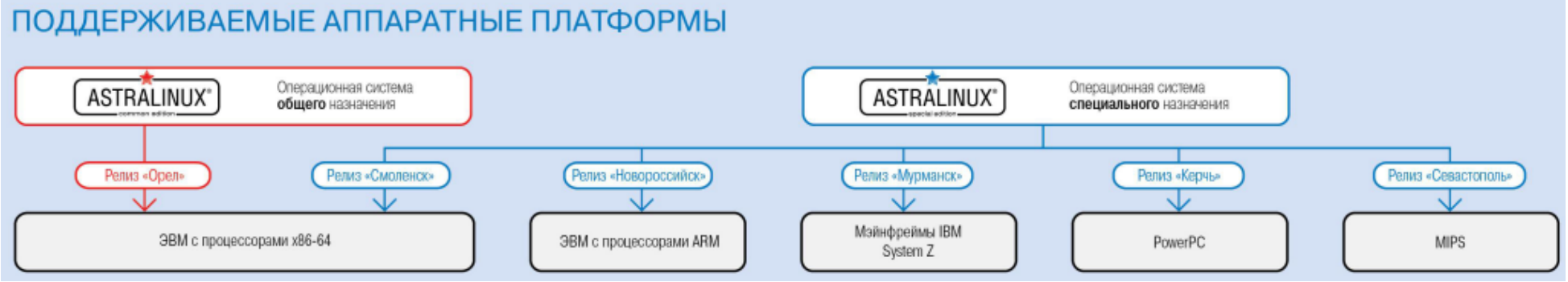

Рисунок 3 - Поддерживаемые Astra Linux аппаратные платформы

1.5. ROSA Linux

Разработчик: ООО «НТЦ ИТ РОСА» (сайт продукта: https://rosalinux.ru).

Семейство операционных систем ROSA Linux включает набор решений, предназначенных для домашнего использования (версия ROSA Fresh) и применения в корпоративной среде (ROSA Enterprise Desktop), развёртывания инфраструктурных ИТ-служб организации (ROSA Enterprise Linux Server), обработки конфиденциальной информации и персональных данных (РОСА «Кобальт»), а также составляющих государственную тайну сведений (РОСА «Хром» и «Никель»).

В основу перечисленных продуктов положены наработки Red Hat Enterprise Linux, Mandriva и CentOS с включением большого количества дополнительных компонентов — в том числе оригинальных, созданных программистами научно-технического центра информационных технологий «РОСА».

В частности, в составе дистрибутивов ОС для корпоративного сегмента рынка представлены средства виртуализации, ПО для организации резервного копирования, инструменты для построения частных облаков, а также централизованного управления сетевыми ресурсами и системами хранения данных.

1.6. Calculate Linux

Разработчик: компания «Калкулэйт» (сайт продукта: https://calculate-linux.ru).

Calculate Linux представлен в редакциях Desktop, Directory Server, Scratch, Scratch Server и ориентирован на домашних пользователей и организации малого и среднего бизнеса, предпочитающие использовать ПО с открытым исходным кодом вместо проприетарных решений.

Особенности платформы: полноценная работа в гетерогенных сетях, механизм перемещаемых профилей пользователей, инструментарий централизованного развёртывания программного обеспечения, простота администрирования, возможность установки на портативные USB-накопители и поддержка бинарных репозиториев обновлений Gentoo.

У пользователей имеется возможность принять участие в сообществе Calculate Linux, высказать свои замечания и принять участие в развитии платформы.

1.7. «Ульяновск.BSD»

Разработчик: Сергей Волков (сайт продукта: https://ulbsd.ru).

Операционная система, построенная на основе свободно распространяемой платформы FreeBSD и содержащая необходимый набор прикладных программ для домашних пользователей и выполнения офисных задач.

Разработчик позиционирует ОС как полностью адаптированную к потребностям именно русскоязычных пользователей.

Дистрибутив проекта распространяется на коммерческих условиях и осуществляется платная техническая поддержка.

ОС «Ульяновск.BSD» включена в реестр российского ПО и может применяться государственными организациями в рамках проектов по внедрению импортозамещающих технологий.

1.8. ICLinux

Разработчик: АО «АйСиЭл-КПО ВС» (сайт продукта: iclinux.icl.ru; https://icl.ru/).

Сертифицированная и защищённая операционная система, позволяющая обрабатывать информацию в соответствии с ФЗ № 152 «О персональных данных» и реализовывать системы обработки информации ограниченного доступа, не относящейся к государственной тайне.

ICLinux включает средства удалённого администрирования, имеет встроенный межсетевой экран, сертифицированный на соответствие РД МЭ по третьему классу защищённости, поддерживает RDP, X-Windows System, SSH, Telnet, VNC, VPN, NX, ICA и прочие протоколы.

Также в активе платформы значатся совместимость со средствами аутентификации компании «Аладдин Р.Д.» и модульная архитектура, которая позволяет гибко настраивать операционную систему под требования заказчика.

1.9. «Эльбрус»

Разработчик: АО «МЦСТ» (сайт продукта: http://mcst.ru/elbrus_os).

Программная платформа, разработанная специально для вычислительных комплексов с архитектурой SPARC и «Эльбрус». Особенностью системы является кардинально переработанное ядро Linux, в котором были реализованы особые механизмы управления процессами, виртуальной памятью, прерываниями, сигналами, синхронизацией, поддержкой тегированных вычислений.

Помимо этого, в ядро программной платформы «Эльбрус» встроен комплекс средств защиты информации от несанкционированного доступа, который позволяет использовать ОС для построения автоматизированных систем, отвечающих самым высоким требованиям информационной безопасности.

Также в составе системы представлены средства архивации, планирования заданий, разработки ПО и ряд других инструментов.

1.10. «Ред ОС»

Разработчик: ООО «Ред Софт» (сайт продукта: https://red-soft.ru).

Операционная система на основе ядра Linux, созданная с учётом обеспечения безопасности обрабатываемых данных. «Ред ОС» соответствует отечественным требованиям по защите информации, имеет преднастроенные конфигурации для каждой аппаратной архитектуры, использует алгоритмы ГОСТ 34.11-2012 в протоколах ssh и NX, а также поддерживает списки управления доступом.

Помимо этого, «Ред ОС» поддерживает сетевую аутентификацию с помощью подключаемых модулей аутентификации (PAM, Pluggable Authentication Modules) и имеет в своём составе специализированную подсистему распределённого аудита, которая позволяет отслеживать критичные события безопасности в корпоративной сети и предоставляет ИТ-администратору необходимые инструменты для оперативного реагирования на инциденты ИБ.

1.11. GosLinux («ГосЛинукс»)

Разработчик: ООО «Ред Софт» (сайт продукта: https://goslinux.fssprus.ru).

ОС GosLinux создана специально для нужд Федеральной службы судебных приставов Российской Федерации (ФССП России) и пригодна для использования во всех органах власти, государственных внебюджетных фондах и органах местного самоуправления.

Платформа построена на базе дистрибутива CentOS 6.4, включающего наработки Red Hat Enterprise Linux. Система представлена в двух редакциях — для серверов и рабочих станций, содержит упрощённый графический интерфейс и набор преднастроенных средств защиты информации.

Разработчик ОС — компания «Ред Софт», победившая в марте 2013 года в конкурсе на доработку, внедрение и сопровождение автоматизированных информационных систем ФССП России. В 2014 году система получила сертификат соответствия ФСТЭК России, подтверждающий, что «ГосЛинукс» имеет оценочный уровень доверия ОУД3 и соответствует требованиям руководящего документа Гостехкомиссии РФ по четвертому уровню контроля отсутствия недекларированных возможностей.

Дистрибутив ОС GosLinux для органов государственной власти размещён в национальном фонде алгоритмов и программ по адресу nfap.minsvyaz.ru. В настоящий момент платформа GosLinux активно развёртывается во всех территориальных органах и подразделениях ФССП России. Также ОС передана на опытную эксплуатацию представителям властей Нижегородской, Волгоградской и Ярославской областей.

1.12. AlterOS

Разработчик: ООО «Алми» (сайт продукта: https://alter-os.ru).

Операционная система AlterOS создана для решения задач по построению и оптимизации ИТ-инфраструктуры коммерческих и государственных организаций. AlterOS разработана в соответствии со всеми государственными стандартами РФ, что подтверждено внесением ее в Реестр отечественного ПО Приказом Минкомсвязи от 15.08.2017 № 421, как рекомендованного продукта для государственных заказчиков.

Операционная система соответствует требованиям по защите информации, предъявляемым к отечественному программному обеспечению. AlterOS соответствует требованиям доверия к ОС (профиль защиты ОС ИТ.ОС.А4.ПЗ) и включена в официальный реестр средств защиты информации (Сертификат № 4393).

Несмотря на то, что AlterOS в первую очередь предназначена для заказчиков из государственного сектора, к организации ИТ-структуры которых предъявляются особые требования, операционная система может быть использована как платформа для работы в любой коммерческой организации. Она интуитивно понятна, имеет привычный графический интерфейс, легко интегрируется в существующую ИТ-инфраструктуру, гарантируя стабильность и безопасность работы. Привычный недостаток Linux, заключающийся в сложности или невозможности подключения периферийного оборудования, в AlterOS преодолен – система совместима с большинством современных устройств.

В настоящее время ОС представлена в трех редакциях: AlterOS Desktop (для рабочих мест), AlterOS Desktop Lite (облегченная версия) и AlterOS Server (для серверов). ОС совместима со множеством востребованных в бизнес-среде программных решений, в том числе с «1С» и «Консультант Плюс», а также отечественными средствами криптозащиты (например, «КриптоПро»).

В версии платформы для госорганизаций отсутствует ПО, которое взаимодействует с иностранными серверами.

1.13. Мобильная система Вооружённых Сил (МСВС)

Разработчик: Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере им. В.В. Соломатина (ВНИИНС, сайт продукта: https://vniins.ru).

Защищённая операционная система общего назначения, предназначенная для построения стационарных и мобильных защищённых автоматизированных систем в Вооружённых Силах Российской Федерации (ВС РФ). Принята в эксплуатацию в ВС РФ в 2002 году.

В основу МСВС положены ядро и компоненты Linux, дополненные дискреционной, мандатной и ролевой моделями разграничения доступа к информации. Система функционирует на аппаратных платформах Intel

(x86 и x86_64), SPARC («Эльбрус-90микро»), MIPS, PowerPC64, SPARC64 и сертифицирована по требованиям безопасности информации Министерства обороны РФ.

Реализованные в МСВС средства защиты позволяют создавать на базе платформы автоматизированные системы, которые обрабатывают составляющие государственную тайну сведения, имеющие степень секретности «СС» (совершенно секретно).

1.14. «Заря»

Разработчик: ФГУП «Центральный научно-исследовательский институт экономики, информатики и систем управления» («ЦНИИ ЭИСУ», входит в «Объединённую приборостроительную корпорацию», сайт продукта: http://cniieisu.ru).

Семейство программных платформ на ядре Linux, которые представляют собой альтернативу зарубежным ОС, применяемым сейчас в силовых ведомствах, госсекторе и на оборонных предприятиях.

Настольная операционная система «Заря» совместима с большинством традиционных офисных приложений и программ. Серверная платформа «Заря-ЦОД» позволяет организовать сервер приложений или сервер базы данных.

Для построения центров обработки данных она предлагает стандартный набор серверного ПО, средства виртуализации, а также возможность работы на так называемом «большом железе», включая мейнфреймы.

Для встраиваемых систем, работающих без участия человека, которые должны обрабатывать информацию в режиме реального времени, разработана специальная ОС «Заря РВ».

Система соответствует третьему классу защиты от несанкционированного доступа и второму уровню контроля отсутствия недекларированных возможностей.

Платформа разработана по заказу Минобороны России и, как ожидается, будет востребована силовыми ведомствами, оборонным комплексом, а также коммерческими структурами, работающими с государственной тайной и персональными данными.

Внутренняя архитектура ОС «Заря» представлена на рисунке 4.

Рисунок 4 - Внутренняя архитектура ОС «Заря»

1.15. RAIDIX

Разработчик: компания «Рэйдикс» (сайт продукта: https://raidix.ru).

Специализированная программная платформа, предназначенная для создания высокопроизводительных систем хранения данных с использованием стандартных аппаратных компонентов.

ОС RAIDIX включена в реестр Минкомсвязи России, как рекомендованная для закупки отечественными компаниями и госструктурами и совместима с оборудованием различных производителей, в том числе с отечественными аппаратными решениями на платформе «Эльбрус».

Система позволяет управлять отдельными RAID-массивами и кластерами хранения, обеспечивает высокую доступность данных при последовательной и случайной нагрузках, поддерживает протоколы SAN (Fibre Channel, InfiniBand, iSCSI, 12G SAS) и NAS (NFS, SMB, AFP, FTP). RAIDIX предоставляет оптимальную скорость расчётов благодаря реализации патентованных уровней RAID 7.3 и RAID N+M.

Кроме того, программная технология включает в себя функцию упреждающей реконструкции данных без физического обращения к дискам, механизм поиска и устранения скрытых ошибок, интеллектуальный модуль QoSmic для распознавания и приоритизации приложений, а также другие возможности.

1.16. Kraftway Terminal Linux

Разработчик: компания Kraftway (сайт продукта: https://kraftway.ru).

Операционная система для терминальных станций. Создана на базе Linux и содержит только необходимый набор инструментов для организации рабочих мест с использованием тонких клиентов.

Все функции, выходящие за эти рамки, исключены из дистрибутива. Kraftway Terminal Linux поддерживает сетевые протоколы прикладного уровня (RDP, VNC, SSH, NX, XWindow, VMWare View PCoIP и др.), позволяет настраивать права доступа на проброс USB-носителей, обеспечивает возможность использования сетевых и локальных принтеров, содержит средства восстановления конфигурации ОС при перезагрузке, а также инструменты дистанционного группового

управления терминальными станциями и администрирования рабочих мест.

Особенность системы — высокая защищённость. Kraftway Terminal Linux поддерживает и аппаратные средства аутентификации пользователей: USB-ключи eToken PRO и eToken PRO Java от ЗАО «Аладдин Р.Д.», а также RuToken S и RuToken ЭЦП от ЗАО «Актив-софт».

Обновление ОС может осуществляться администратором через локальную сеть или с USB-накопителя. Возможна настройка автообновления как с локального сервера заказчика, так и с сервера компании Kraftway.

1.17. WTware

Разработчик: Андрей Ковалёв (сайт продукта: http://wtware.ru).

Программная платформа для развёртывания в ИТ-инфраструктуре предприятия рабочих мест с использованием недорогих терминальных решений.

В дистрибутив WTware включены службы для загрузки по сети, инструменты для работы с принтерами, сканерами штрих-кодов и прочим периферийным оборудованием.

Поддерживается перенаправление COM- и USB-портов, а также аутентификация по смарт-картам. Для подключения к серверу терминалов используется протокол RDP, а для оперативного разрешения возникающих при настройке операционной системы вопросов к дистрибутиву прилагается подробная документация.

WTware распространяется на коммерческих условиях и лицензируется по количеству рабочих станций. Для мини-компьютера Raspberry Pi разработчиком предлагается бесплатная версия ОС.

1.18. KasperskyOS

Разработчик: «Лаборатория Касперского» (сайт продукта: https://kaspersky.ru).

Безопасная операционная система, предназначенная для использования в критически важных инфраструктурах и устройствах. Платформа «Лаборатории Касперского» может быть задействована в автоматизированных системах управления технологическими

процессами (АСУ ТП), телекоммуникационном оборудовании, медицинских аппаратах, автомобилях и других гаджетах из мира Интернета вещей.

Данная ОС в силу своей архитектуры гарантирует высокий уровень информационной безопасности.

Основной принцип работы KasperskyOS сводится к правилу «запрещено всё, что не разрешено». Это позволяет исключить возможность эксплуатирования как уже известных уязвимостей, так и тех, что будут обнаружены в будущем. При этом все политики безопасности, в том числе запреты на выполнение определённых процессов и действий, настраиваются в соответствии с потребностями организации.

Платформа поставляется в качестве предустановленного программного обеспечения на различных типах оборудования, применяемого в индустриальных и корпоративных сетях.

В настоящее время безопасная ОС «Лаборатории Касперского» внедрена в маршрутизирующий коммутатор уровня L3, разработанный компанией Kraftway.

1.19. ОСРВ «МАКС»

Разработчик: «АстроСофт» (сайт продукта: https://astrosoft.ru).

Операционная система реального времени (ОСРВ), написанная программистами компании «АстроСофт» без заимствований чужого кода и предназначенная прежде всего для Интернета вещей и встроенных устройств. Кроме того, она подходит для робототехники, медицинского оборудования, систем «умного дома» и «умного города», потребительской электроники и т.п.

Впервые ОСРВ «МАКС» (аббревиатура расшифровывается как «мультиагентная когерентная система») была продемонстрирована в январе 2017 года.

Платформа не только реализует всю классическую функциональность продуктов данного типа, но и обладает рядом уникальных возможностей по организации взаимодействия множества устройств, позволяющих упростить создание необходимых во встраиваемых системах механизмов: резервирование, горячая замена оборудования и др.

Одна из особенностей ОСРВ «МАКС» — поддержка разделяемой памяти на уровне устройств. Данный механизм обеспечивает автоматическую, устойчивую к сбоям отдельных компонентов синхронизацию информации между узлами распределённой системы. ОСРВ «МАКС» включена в реестр отечественного программного обеспечения.

Также продукт зарегистрирован в Федеральной службе по интеллектуальной собственности (Роспатент) и в настоящее время (2021 г.) проходит сертификацию в Федеральной службе по техническому и экспортному контролю (ФСТЭК России) по четвёртому уровню контроля недекларированных возможностей (НДВ).

1.20. «СинтезМ»

Разработчик: АО «ФИНТЕХ» (сайт продукта: https://fintech.ru).

Цифровая программная платформа «СинтезМ» (защищённая операционная система) - это отечественная защищенная программная платформа, предназначенная для создания на основе виртуализации надежных, высокопроизводительных, отказоустойчивых, высоконагруженных, масштабируемых, территориально распределенных защищенных центров обработки данных, ситуационных центров и автоматизированных систем с разграничением прав доступа пользователей к защищаемой информации, удовлетворяющих требованиям российских регуляторов в области информационной безопасности.

Платформа разработана с учётом проблемных вопросов информационного взаимодействия на основе унифицированных сквозных технических решений.

Платформа «СинтезМ» сертифицирована ФСБ России по первому классу, ФСТЭК России по типу А и четвертому классу защиты.

Цифровая платформа «СинтезМ-Т» может развертываться на платформах: x86_64, IBM P- и Z-серий и др. В ближайшей перспективе предусматривается возможность сопряжения платформы с компьютерами на базе процессора «Эльбрус».

Со стороны разработчика (АО «ФИНТЕХ») обеспечивается круглосуточная техническая поддержка первого, второго и третьего

уровней для всех компонентов платформы. По требованию Заказчика производится доработка/адаптация компонентов платформы.

Подробно архитектура, основные компоненты, тактико-технические характеристики платформы «СинтезМ», её функциональные возможности и другие особенности будут рассмотрены в последующих разделах учебного пособия.

Контрольные вопросы к разделу 1

1. Что такое защищённый ЦОД?
2. Какие подходы в части создания российского ПО существуют в настоящее время?
3. Укажите основные цифровые платформы и операционные системы, разработанные в Российской Федерации
4. Какие цифровые платформы и ОС имеют сертификат, выданный ФСТЭК России, подтверждающий соответствие продукта требованиям следующих руководящих документов: «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации»?
5. Какие виды дистрибутивов входят в состав платформы «Альт»?
6. Какие из рассматриваемых цифровых платформ и ОС имеют сертификацию ФСБ России?
7. Какие из рассматриваемых цифровых платформ и ОС имеют сертификацию ФСТЭК России?
8. Какие решения и продукты положены в основу семейства операционных систем ROSA Linux?
9. Укажите особенности платформы Calculate Linux?
10. Дистрибутивы каких цифровых платформ и ОС размещены в национальном фонде алгоритмов и программ?
11. Дистрибутивы каких цифровых платформ и ОС внесены в Единый реестр российских программ для электронных вычислительных машин и баз данных?

12. Какие цифровые платформы и ОС могут быть использованы для построения информационных систем персональных данных (ИСПДн)?
13. Какие цифровые платформы и ОС соответствуют ФЗ № 152 «О персональных данных» и позволяют обрабатывать информацию в соответствии с данным ФЗ?
14. Какая ОС разработана специально для нужд Федеральной службы судебных приставов Российской Федерации (ФССП России)?
15. Какие цифровые платформы и ОС включены в официальный реестр средств защиты информации?
16. Какими основными свойствами обладает Платформа «СинтезМ»?
17. Какими регуляторами и по каким классам защиты сертифицирована Платформа «СинтезМ»?
18. На каких аппаратных платформах может быть осуществлено развёртывание Платформы «СинтезМ»?

2. Архитектура цифровой платформы «СинтезМ»

2.1. Состав программных компонентов защищенной программной платформы «СинтезМ»

Как уже отмечалось, цифровая программная платформа «СинтезМ» предназначена для построения защищенных территориально распределенных центров обработки данных, ситуационных центров, а также территориально распределенных автоматизированных систем в защищенном исполнении (АСЗИ) на основе ЦОД.

Рассмотрим основные программные компоненты цифровой программной платформы «СинтезМ» и их назначение.

Защищенная операционная система (ЗОС) «СинтезМ» представляет собой комплекс программ (КП), предназначенных для создания автоматизированных систем в защищенном исполнении в части обеспечения функционирования серверных группировок и автоматизированных рабочих мест пользователей, а также обеспечения выполнения требований по защите информации, обрабатываемой в АСЗИ, от несанкционированного доступа (НСД) и реализации защищенного вычислительного процесса.

ЗОС «СинтезМ» включает в себя программные комплексы «СинтезМ-Сервер» и «СинтезМ-Клиент»:

- *Программный комплекс (ПК) «СинтезМ-Сервер»* со средствами защиты, интегрированными в состав программного комплекса (на базе CentOS версии 7.7 с доработкой на базе ядра в части защиты информации от НСД), представляет собой серверную операционную систему, предназначенную для обеспечения функционирования серверов x86_64, виртуальных машин, менеджера виртуальных машин (ВМ), терминального сервера, терминальных клиентов, пользователей АСЗИ, серверов приложений, системы управления базами данных, системы хранения данных и подсистемы защиты информации. Изделие создает среду виртуализации, поддерживающую в качестве гостевых защищенных операционных систем «СинтезМ», Windows, Linux, а также обеспечивает изоляцию виртуальных машин и управляет всем жизненным циклом виртуальных машин;

- *Программный комплекс «СинтезМ-Клиент»* со средствами защиты, интегрированными в состав программного комплекса (на базе

CentOS версии 8 с доработкой на базе ядра в части защиты информации от НСД), представляет собой клиентскую операционную систему и предназначен для создания доверенной среды функционирования АРМ (рабочая станция, ноутбук) и применения в качестве гостевой операционной системы для виртуальных машин.

Необходимо отметить, что здесь и далее выражение «программное средство, созданное на базе…» означает, что разработчики провели комплексный анализ первоначального ПО на наличие потенциальных уязвимостей и глубоко переработали его с целью создания «доверенного ПО».

Также в состав цифровой программной платформы «СинтезМ» входят следующие программные комплексы.

Комплекс программных средств защиты информации, функционирующих в среде операционной системы «СинтезМ» (КП «ПСЗИ «СинтезМ») обеспечивает автоматизацию функций управления подсистемой защиты информации от несанкционированного доступа при её сопровождении администраторами безопасности в ходе эксплуатации АСЗИ, обрабатывающей сведения, составляющие государственную тайну, в составе которых применяется ЗОС «СинтезМ», а также с возможностью интеграции со средствами защиты информации других гостевых операционных систем Astra Linux, МСВС и др.

В свою очередь КП «ПСЗИ «СинтезМ» включает в себя:

- *Программный комплекс «Сервер безопасности» (ПК «СинтезМ-СБ»)* представляет собой серверный компонент ПСЗИ и предназначен для установки на виртуальные машины серверов безопасности, развернутых на комплексах средств автоматизации различных уровней, из состава АСЗИ, функционирующих под управлением ПК «СинтезМ-Клиент» из состава ЗОС «СинтезМ»;
- *Комплекс программ «Подсистема контроля и диагностирования» (КП «СинтезМ-ПКД»)* предназначен для контроля и диагностирования технических и программных средств, проведения комплексной оценки АСЗИ, управления конфигурациями КСА, ведения реестров баз данных, сервисов и технических средств;
- *Программный комплекс «Сервер управления доступом» (ПК «СинтезМ-ИПА»)* программный комплекс ПСЗИ, реализующий функции сервера управления доступом и устанавливаемый в виртуальную машину Серверов управления доступом, развернутых на комплексах средств

автоматизации различных уровней, из состава АСЗИ, функционирующих под управлением ПК «СинтезМ-Клиент» из состава ЗОС «СинтезМ»;

- *Программное средство «Управление конфигурацией», созданное на базе Ansible версии 2.9 (ПС «СинтезМ-УК»)*, программное средство защиты информации, реализующее интерпретацию сценариев управления конфигурацией КСА для автоматизации настройки физических серверов, среды виртуализации, рабочих станций, ВМ и установки на них требуемых дистрибутивов ПО. ПС «СинтезМ-УК» входит в состав комплекса ПСЗИ, функционирующих в среде операционной системы «СинтезМ», предназначенных для защиты информации ограниченного доступа, содержащей сведения, составляющие служебную тайну и/или государственную тайну до степени секретности «секретно», от несанкционированного доступа, а также для реализации функций обеспечения целостности и доступности данной информации.
- *Программное средство «Сервер управления доступа к сервисам» (ПС «СинтезМ-СУДС»)* предназначено для предоставления разрешенного сетевого клиент-серверного взаимодействия между приложениями («толстых» клиентов, веб-клиентов) к сетевым сервисам, расположенным на серверах приложений. Контроль сетевых взаимодействий обеспечивается как в рамках локальных вычислительных сетей, так и в рамках территориально распределенной АСЗИ.

Комплекс программных средств (КПС) «Функциональные сервисы» представляет собой комплекс программных средств, предназначенных для создания АСЗИ в части обеспечения функционирования серверных группировок и автоматизированных рабочих мест пользователей, и включает в себя:

- *Программное средство «Система управления базами данных» на базе PostgreSQL версии 10.6 (ПС «СинтезМ-СУБД»)* представляет собой систему управления объектно-реляционными базами данных, основанную на технологиях «PostgreSQL». Механизмами ПС «СинтезМ-СУБД» обеспечивается многопользовательский режим работы с разграничением доступа пользователей к объектам БД, сквозная аутентификация пользователей в БД, поддержка разграничения доступа пользователей к объектам БД на основе использования механизма меток безопасности и механизма разграничения доступа к записям;

- *Программное средство «Сервер приложений» на базе JBoss-EAP версии 7.0 (ПС «СинтезМ-СП»)* предназначено для развертывания и исполнения прикладных приложений, разработанных для среды исполнения/вычислительного окружения Java EE2;
- *Программное средство «Сервер приложений» на базе uWSGI версии 2.0.17, python3-jango версии 2.2.3 (ПС «СинтезМ-СП»)* предназначено для развертывания и исполнения прикладных приложений, разработанных для среды исполнения/вычислительного окружения Python;
- *Комплекс программ «Офисные средства» на базе LibreOffice версии 6.0 (КП «СинтезМ-О»)* представляет собой комплекс программ, обеспечивающий решение задач подготовки и вывода на бумажные носители текстовых, табличных и презентационных документов в электронной форме. Программа обеспечивает решение задач для автоматического форматирования документов, вставки рисованных объектов и графики в текст, составления оглавлений и указателей, проверки орфографии, шрифтового оформления, подготовки шаблонов документов, специализированной обработки (встроенные функции, статистическая обработка данных и др.);
- *Комплекс программ «Контроль и управление функционированием» (КП «СинтезМ-КУФ»)* предназначен для мониторинга и управления сетевым, серверным и периферийным оборудованием, а также виртуальными машинами. Предоставляет возможность мониторинга состояния технических и программных средств, виртуальных машин и программного обеспечения на основе собранных данных и включает в себя:

✓ Программное средство «Сервер контроля и управления функционированием» на базе Zabbix версии 3.2.3 (ПК «СинтезМ-КУФ.С») предназначено для мониторинга и управления сетевым и серверным оборудованием закрытого контура, а также для передачи данных мониторинга с последующим анализом, составлением отчётов и графиков;

✓ Программный комплекс «Прокси-сервер контроля и управления функционированием» (ПК «СинтезМ-КУФ.ПС») предназначен для сбора данных мониторинга от одного или нескольких ПС «СинтезМ-КУФ.А», SNMP агентов, IPMI агентов, хранения полученных метрик в собственной СУБД и отправки данных на ПК «СинтезМ-КУФ.С»;

✓ Программное средство «Агент контроля и управления функционированием» (ПС «СинтезМ-КУФ.А») предназначено для сбора информации о состоянии объектов контроля (физические серверы, виртуальные машины, АРМ, работающие под управлением ВМ) и отправки данных на ПК «СинтезМ-КУФ.ПС» или ПК «СинтезМ-КУФ.С» для дальнейшей обработки. По запросу сервера КУФ или прокси-сервера КУФ агент КУФ собирает информацию о состоянии объекта контроля, используя системные вызовы операционной системы;

- *Программное средство «Система хранения данных» на базе GlusterFS версии 3.12 (ПС «СинтезМ-СХД-01»)* предназначено для обеспечения создания и функционирования программной системы хранения данных с функцией репликации и возможностью использования дисковых ресурсов типовых серверов виртуализации. Возможен вариант исполнения для двух серверов виртуализации;
- *Программное средство «Система хранения данных» на базе Ceph версии 14.0 (ПС «СинтезМ-СХД-02»)* предназначено для обеспечения создания и функционирования программной системы хранения данных с функцией репликации и возможностью использования дисковых ресурсов типовых серверов виртуализации. ПС «СинтезМ-СХД-02» представляет собой совокупность аппаратно-программных средств на базе ПК «СинтезМ-Сервер», обеспечивающих отказоустойчивое хранение данных с возможностью масштабирования изделия. В минимальный состав изделия для выполнения функциональных задач и задачи отказоустойчивости должны входить три ПК «СинтезМ-Сервер». Масштабируемость изделия обеспечивается путем увеличения количества ПК «СинтезМ-Сервер», коммутационного оборудования (при необходимости) и дооснащения изделия жесткими дисками. ПС «СинтезМ-СХД-02» представляет возможность выбора нескольких вариантов исполнения: для трех и более серверов виртуализации;
- *Программное средство «Система резервного копирования» на базе bareos версии 17.3 (ПС «СинтезМ-СРК»)* представляет собой программное средство, обеспечивающее создание резервных копий данных (файлов и каталогов АРМ и дампов баз данных) с возможностью их дальнейшего просмотра и восстановления посредством WEB-интерфейса;
- *Программное средство «Система резервного копирования образов виртуальных машин» (ПС «СинтезМ-СРК-ОВМ»)* представляет собой программное средство, обеспечивающее создание резервных

копий образов виртуальных машин с возможностью их дальнейшего просмотра и восстановления посредством WEB-интерфейса;

- *Комплекс программ «Защищенная электронная почта» (КП «СинтезМ-ЗЭП»)* обеспечивает защищённый обмен почтовыми сообщениями между пользователями с разграничением доступа к сообщениям и возможностью настройки регламента (правил) обмена для пользователей АСЗИ. Регламент обмена настраивается относительно пользователей и определяет, каким пользователям разрешено отправлять почтовые сообщения другим пользователям.

КП «СинтезМ-ЗЭП» включает в себя:

- Программное средство «Сервер защищенной почты» на базе Dovecot версии 2.2.10-6, postfix версии 2.10.1-7 (ПС «СинтезМ-ЗЭП.С») представляет собой компонент КП «СинтезМ-ЗЭП» без графического интерфейса, предназначенный для обработки, хранения и пересылки почтовых сообщений;
- Программное средство «Клиент защищенной почты» на базе Evolution версии 2.32.3-40 (ПС «СинтезМ-ЗЭП.К») представляет собой компонент КП «СинтезМ-ЗЭП» с графическим интерфейсом, предназначенный для обмена почтовыми сообщениями, отправку их компоненту «Почтовый сервер» и показ писем авторизованным пользователям;

- *Программный комплекс «Транспортная подсистема» на базе RabbitMQ версии 3.7.23, Erlang версии 21.3.8.11 (ПК «СинтезМ-ТПС»)* предназначен для обеспечения хранения сообщений от каждого приложения в отдельной очереди, взаимодействия прикладных систем в территориально распределенных системах с гарантированным доведением сообщений и квитированием факта доставки, отслеживания статуса доведения сообщений на каждом этапе передачи, обеспечения маршрутизации сообщений между серверами ТПС;
- *Программное средство «Средство синхронизации баз данных» (ПС «СинтезМ-СС»)* функционирует на сервере баз данных и выполняет обмен данными с другими ПС «СинтезМ-СС» (работающими с соответствующими базами данных) по заданным регламентам (регламенты разрабатываются посредством ПС «СинтезМ-СУС»), обеспечивая синхронизацию территориально распределенных баз данных. ПС «СинтезМ-СС» устанавливается на каждом сервере баз данных, задействованным в синхронизации;

- *Программное средство «Сетевое файловое хранилище» (ПС «СинтезМ-СФХ»)* предназначено для создания и ведения централизованного сетевого файлового хранилища АСЗИ, обеспечивающего хранение ресурсов и их метаданных пользователей системы, а также различных модулей специального программного обеспечения;
- *Комплекс программ «Защищенный портал» (КП «СинтезМ-ЗП»)* предназначен для создания защищенных порталов в территориально распределенных АСЗИ, обеспечивающих выполнение функциональных задач должностных лиц (пользователей);
- *Программное средство «Конструктор экранных форм» (ПС «СинтезМ-КЭФ»)* предназначено для решения в автоматизированном режиме службой эксплуатацией АСЗИ задач по созданию, модернизации экранных форм для решения задач по вводу и визуализации разнородных данных;
- *Программное средство «Конструктор тематических баз данных» (ПС «СинтезМ-КТБД»)* предназначено для разработки и модификации шаблонов тематических баз (ТБД), перечня информационных ресурсов, перечня сервисов (включаемых в шаблоны ТБД), перечня расчетных процедур (включаемых в шаблоны ТБД) и версий шаблонов ТБД, а также определения совместимости ранее созданных ТБД с создаваемыми, в части возможности их синхронизации и определения совместимости ранее созданных ТБД с создаваемыми, в части возможности синхронизации;
- *Программное средство «Средство администрирования защищенного портала» (ПС «СинтезМ-САЗП»)* предназначено для визуализации информации о развернутых на объектах АСЗИ защищенных порталов, информации по составу разделов порталов для различных объектов автоматизации, информации по составу тематических баз данных, информации о сервисах доступа к данным тематических баз данных, ведения состава разделов порталов, ввода исходных данных по правам доступа групп пользователей по информационным ресурсам тематических баз данных, определения конфигураций сервисов доступа к данным тематических баз данных для групп пользователей;
- *Аппаратно-программное средство «Персональный идентификатор пользователя» (АПС «СинтезМ-ТК/ПИ»)* представляет собой самостоятельное средство криптографической защиты информации с реализацией криптографических алгоритмов

непосредственно на USB-ключе. АПС «СинтезМ-ТК/ПИ» предназначен для обеспечения защиты информации от несанкционированного доступа в АСЗИ.

При использовании платформы «СинтезМ» обеспечивается многопользовательский режим функционирования ЦОД и АСЗИ, а также обработка информации с уровнем конфиденциальности «Секретно», «Конфиденциальная информация».

Платформа и компоненты из её состава сертифицированы по требованиям ФСБ России, ФСТЭК России.

Сравнительный анализ состава и назначения компонент ОС Astra Linux и платформы «СинтезМ»

В настоящее время на отечественном рынке присутствует ряд цифровых программных платформ (подробно описаны в разделе 1 данного учебного пособия) аналогичных ЦПП «СинтезМ». Однако к числу уникальных встроенных возможностей ЦПП «СинтезМ», в отличие от большинства рассмотренных платформ, следует отнести доверенную среду виртуализации, программные средства защиты информации, интегрированные средства управления, а также состав функциональных сервисов.

Имеющиеся аналоги ЦПП «СинтезМ» (ОС Astra Linux, “Циркон-36С” и ряд других) существенно уступают платформе «СинтезМ» по характеристикам операционной системы, по возможностям среды виртуализации и не содержат в себе требуемый состав компонентов, обеспечивающий построение, масштабирование и эксплуатацию отказоустойчивых, высоконагруженных ЦОД и в целом территориально-распределенных АСЗИ.

Сравнительный анализ состава и назначения компонент платформы ОС Astra Linux и ЦПП «СинтезМ» приведен в таблице 1.

Соответствие платформ ОС Astra Linux и «СинтезМ» требованиям к построению территориально распределенных автоматизированных систем и отказоустойчивых, высоконагруженных ЦОД приведен в таблице 2.

Применение ЦПП «СинтезМ» при построении территориально распределенных защищённых ЦОД обеспечивает возможность поэтапного их развития, масштабирования и расширения возможностей

посредством наращивания группировки технических средств (серверов, сетевого оборудования, узлов систем хранения данных и резервного копирования) и программного обеспечения без выведения из эксплуатации и без необходимости организации дорогостоящих НИОКР по их модернизации и дальнейшей дополнительной аттестации.

Платформа «СинтезМ» обеспечивает адекватную замену среды виртуализации VMware, Hyper-V, а также программных средств интеграции и управления этими средами (например, IBM Tivoli для VMWare), что подтверждается результатами нагрузочных испытаний, проведенных ОАО «РЖД» и ООО «РТ-Инвест Транспортные системы».

Таблица 1 - Сравнительный анализ программных платформ Astra Linux и «СинтезМ»

№ п/п	Наименование компонента	Astra Linux	«СинтезМ»
1	Базовые библиотеки	• базовая библиотека изделия libc; • библиотека базы данных; • библиотеки и программы для работы с ФС ext2, ext3, ext4; • библиотека для чтения заголовков файлов ELF; • библиотеки системы OpenLDAP; • библиотека функций сжатия zlib; • библиотеки для управления терминалами ncurses	Содержит тот же состав базовых библиотек, что и Astra Linux: • базовая библиотека изделия libc; • библиотека базы данных; • библиотеки и программы для работы с ФС ext2, ext3, ext4; • библиотека для чтения заголовков файлов ELF; • библиотеки системы OpenLDAP; • библиотека функций сжатия zlib; • библиотеки для управления терминалами ncurses. Дополнительные библиотеки: • Lib GSS-API – обеспечение сквозной аутентификации и идентификации; • поддерживаемые файловые системы: XFS, NFS, GlusterFS, CEPHFS
2	Базовые утилиты	• системный загрузчик GRUB2; • системная оболочка Bash; • консольные утилиты для работы с модулями ядра; • консольные утилиты для создания образов инициализации изделия; • консольные программы для работы с файлами; • консольные программы настройки сети; • консольные программы для работы с ФС; • консольные программы для работы с сетевыми устройствами; • консольные программы управления фоновой работой; • консольные программы архивирования; • консольные программы настройки работы жестких дисков; • консольные программы управления логическими томами;	Содержит тот же состав базовых утилит, что и Astra Linux: • системный загрузчик GRUB2; • системная оболочка Bash; • консольные утилиты для работы с модулями ядра; • консольные утилиты для создания образов инициализации изделия; • консольные программы для работы с файлами; • консольные программы настройки сети; • консольные программы для работы с ФС; • консольные программы для работы с сетевыми устройствами; • консольные программы управления фоновой работой; • консольные программы архивирования; • консольные программы настройки работы жестких дисков;

№ п/п	Наименование компонента	Astra Linux	«СинтезМ»
		• консольные программы управления RAID-массивами; • консольные программы для монтирования и управления ФС; • консольные программы для работы с устройствами PCI; • консольные программы распределения дисковых квот; • консольные текстовые редакторы; • консольные потоковые редакторы; • консольные программы для записи CD/DVD-дисков	• консольные программы управления логическими томами; • консольные программы управления RAID-массивами; • консольные программы для монтирования и управления ФС; • консольные программы для работы с устройствами PCI; • консольные программы распределения дисковых квот; • консольные текстовые редакторы; • консольные потоковые редакторы; • консольные программы для записи CD/DVD-дисков; Дополнительные утилиты: • OpenSSL с реализацией криптоалгоритмов ГОСТ
3	Встроенные средства защиты информации	• Базовым решением является использование в качестве средства разграничения доступа – модуля мандатного разграничения доступа PARSEC; • механизмы защиты информации ядра GNU/Linux; • библиотека проверки паролей; • библиотеки Kerberos; • библиотеки подключаемых модулей аутентификации PAM; • консольные программы добавления/удаления пользователей и групп; • консольные программы для работы со списками прав доступа; • консольные программы для смены пароля и управления конфигурацией групп	В отличие от Astra Linux вместо модуля мандатного разграничения доступа PARSEC используется система принудительного контроля доступа к файлам, папкам, объектам БД, программному обеспечению, сокетам на основе политик безопасности SELinux. Политики безопасности формируются на основе правил разграничения доступа Администратором безопасности в соответствии с исходными данными функционального Заказчика и доводятся в автоматическом режиме до физических серверов и ВМ. В остальном состав встроенных средств защиты информации, что и Astra Linux: • механизмы защиты информации ядра GNU/Linux; • библиотека проверки паролей; • библиотеки Kerberos; • библиотеки подключаемых модулей аутентификации PAM; • консольные программы добавления/удаления пользователей и групп; • консольные программы для работы со списками прав доступа;

№ п/п	Наименование компонента	Astra Linux	«СинтезМ»
			• консольные программы для смены пароля и управления конфигурацией групп;
4	Сетевые службы	• доменных имен DNS; • bootparamd; • автоматического выделения IP-адресов DHCP с поддержкой bootp; • передачи файлов FTP и TFTP; • сетевой файловой системы NFS и Samba/CIFS; • синхронизации времени NTP; • удаленного доступа SSH и telnet; • преобразования программных номеров RPC в номера портов протокола DARPA; • туннелирования «точка-точка»; • сервисы электронной почты SMTP, POP3 и IMAP	Содержит тот же состав сетевых служб, что и Astra Linux: • доменных имен DNS; • bootparamd; • автоматического выделения IP-адресов DHCP с поддержкой bootp; • передачи файлов FTP и TFTP; • сетевой файловой системы NFS и Samba/CIFS; • синхронизации времени NTP; • удаленного доступа SSH и telnet; • преобразования программных номеров RPC в номера портов протокола DARPA; • туннелирования «точка-точка»; • сервисы электронной почты SMTP, POP3 и IMAP
5	Графическая система	• графический сервер Xorg, включающий драйверы, утилиты и библиотеки; • комплект шрифтов и библиотек для их отрисовки и управления; • библиотека, реализующая стандарт OpenGL (Mesa), и библиотека для создания интерактивных 3D-приложений (freeglut); • библиотеки для создания приложений с графическим интерфейсом (Qt, GTK+); • полнофункциональный рабочий стол с расширенным набором приложений Fly (на основе KDE)	Содержит тот же состав графической системы, что и Astra Linux, за исключением графического рабочего стола – mate (на основе GNOME): • графический сервер Xorg, включающий драйверы, утилиты и библиотеки; • комплект шрифтов и библиотек для их отрисовки и управления; • библиотека, реализующая стандарт OpenGL (Mesa), и библиотека для создания интерактивных 3D-приложений (freeglut); • библиотеки для создания приложений с графическим интерфейсом (Qt, GTK+); • полнофункциональный рабочий стол с расширенным набором приложений Fly (на основе KDE)
6	Средства работы с периферийным оборудованием	• сервис печати CUPS; • средства настройки службы печати; • программные модули поддержки печатных устройств; • средства для работы с устройствами сканирования;	Содержит тот же состав средств работы с периферийным оборудованием, что и Astra Linux: • сервис печати CUPS; • средства настройки службы печати;

№ п/п	Наименование компонента	Astra Linux	«СинтезМ»
			• программные модули поддержки печатных устройств; • средства для работы с устройствами сканирования;
7	Средства разработки и отладки	• утилита automake для создания файлов Makefile; • утилита autoconf для создания скриптов configure; • ассемблер, компоновщик и утилиты binutils; • генератор-компилятор bison; • система контроля версий svn; • инструмент создания документации к исходному коду на C/C++, Java, Python и других языках doxygen; • лексический анализатор flex; • компиляторы gcc/g++ • сценарии сопровождения библиотек libtool; • утилита make; • интерпретаторы языков Perl, Python, Ruby, PHP, Lua	Содержит тот же состав средств разработки и отладки, что и Astra Linux: • утилита automake для создания файлов Makefile; • утилита autoconf для создания скриптов configure; • ассемблер, компоновщик и утилиты binutils; • генератор-компилятор bison; • система контроля версий svn; • инструмент создания документации к исходному коду на C/C++, Java, Python и других языках doxygen; • лексический анализатор flex; • компиляторы gcc/g++ • сценарии сопровождения библиотек libtool; • утилита make; • интерпретаторы языков Perl, Python, Ruby, PHP, Lua. Также средства разработки и отладки могут добавляться в репозиторий по требованию Заказчика
8	Средства установки и удаления приложений	• с отслеживанием зависимостей APT • менеджер пакетов dpkg	• с отслеживанием зависимостей YUM • менеджер пакетов RPM
9	Средства справочной электронной документации	• набор документации manpages-ru на русском языке в формате man; • утилита предоставления документации info; • графическая электронная справка	Содержит тот же состав средств справочной электронной документации, что и Astra Linux: • набор документации manpages-ru на русском языке в формате man; • утилита предоставления документации info; • графическая электронная справка
10	Средства защиты информации	• средства реализации единого пространства пользователей (централизованное управление учетными записями пользователей, сквозная аутентификация пользователей в сети, централизованное хранение файлов и настроек пользователей); • контроль целостности объектов ФС и аутентичности	Программные средства защиты информации платформы «СинтезМ» (ПСЗИ «СинтезМ») реализуют выполнение требований по обеспечению безопасности информации для многопользовательских систем с различными правами доступа (1Б, 1Г, 1В) в соответствии с требованиями приказа № 31 ФСТЭК России.

№ п/п	Наименование компонента	Astra Linux	«СинтезМ»
		исполняемых модулей; • система протоколирования событий; • система надежного удаления информации из файловой системы и оперативной памяти; • средства реализации ограниченного режима работы пользователя (режим киоска)	Функционал ПСЗИ «СинтезМ» значительно превосходит функционал средств защиты информации Astra Linux
11	Многофункциональный рабочий стол	• менеджер окон; • файловый менеджер; • графические средства администрирования системы; • средства реализации многомониторного режима работы; • реализации коллективной работы пользователей на одной рабочей станции	Содержит те же возможности многофункционального рабочего стола, что и Astra Linux: • менеджер окон; • файловый менеджер; • графические средства администрирования системы; • средства реализации многомониторного режима работы; • реализации коллективной работы пользователей на одной рабочей станции
12	Средства поддержки виртуальных рабочих станций	Среда виртуализации основана на KVM. Менеджер виртуализации virt-manager, предназначенный для управления локальной средой виртуализации, имеет следующие недостатки: • не управляет средой виртуализации в автоматическом режиме; • нет контроля и управления серверами виртуализации (гипервизорами) в режиме реального времени, все действия осуществляются только по запросу администратора; • нет возможности создавать кластеры серверов виртуализации (гипервизоров) и дата-центров; • нет возможности управления хранилищами данных; • нет возможности управления сетями; • нет возможности управления доступом пользователей к виртуальным машинам; • нет средств обеспечения кластеризации на уровне виртуализации; • нет средств обеспечения высокой доступности виртуальных машин;	Среда виртуализации основана на KVM. Средство управления виртуализации – oVirt. Применение менеджера oVirt имеет следующие преимущества относительно virt-manager: • управляет средой виртуализации в автоматическом режиме; • контроль и управление серверами виртуализации в режиме реального времени (управление питанием, балансировка нагрузки, контроль состояния и т.д.); • есть возможность управления дата-центрами; • есть возможность управления хранилищами данных; • есть возможность управления сетями; • есть возможность штатными средствами разграничивать права доступа пользователей к виртуальным машинам; • есть средства обеспечения кластеризации на уровне виртуализации; • есть средства обеспечения высокой доступности виртуальных машин; • есть средства обеспечения миграции виртуальных

№ п/п	Наименование компонента	Astra Linux	«СинтезМ»
		• нет средств обеспечения миграции виртуальных машин (виртуальные машины жестко фиксированы на хостах виртуализации); • нет средств обеспечения живой (без прекращения функционирования) миграции виртуальных машин; • существенные ограничения на количество виртуальных машин; • сложность в наращивании среды виртуализации	машин (виртуальные машины жестко фиксированы на хостах виртуализации); • есть средства обеспечения живой (без прекращения функционирования) миграции виртуальных машин; • размер кластера серверов виртуализации – 16 гипервизоров; • количество виртуальных машин – не ограничено; • легкое масштабирование среды виртуализации, достаточно просто добавить гипервизор в менеджер
13	***Состав общесистемного программного обеспечения:***		
	Система управления базами данных PostgreSQL	Имеется	Имеется Изделие ПС «СинтезМ-СУБД», имеющее в своем составе библиотеку разграничения доступа sepgsql
	Графический клиент гипертекстовой обработки данных - браузер	Имеется	Имеется в составе клиентской операционной системы ПК «СинтезМ-Клиент»
	Сервис гипертекстовой обработки данных HTTP	Имеется (apache)	Имеется (apache, nginx) В составе клиентской операционной системы ПК «СинтезМ-Клиент» и серверной операционной системы ПК «СинтезМ-Сервер»
	Набор офисных программ (текстовый процессор, электронная таблица, система презентаций) OpenOffice или LibreOffice	Имеется	Имеется В составе КП «СинтезМ-О»

№ п/п	Наименование компонента	Astra Linux	«СинтезМ»
	Система верстки текстов TeX/LaTeX	Имеется	Имеется В составе клиентской операционной системы ПК «СинтезМ-Клиент»
	Почтовый сервер	Отсутствует	Имеется с возможностью разграничения доступа В составе сервера защищенной электронной почты ПС «СинтезМ-ЗЭП.С»
	Графический почтовый клиент	Имеется	Имеется с интеграцией с подсистемой безопасности информации В составе клиента защищенной электронной почты ПС «СинтезМ-ЗЭП.К»
	Torrent-клиент с графическим интерфейсом	Имеется	Имеется Добавляется по требованию заказчика
	Менеджер загрузок	Имеется	Имеется
	Графический клиент-сервисов мгновенных сообщений	Имеется	Имеется Добавляется по требованию заказчика
	Сервер и клиент сервиса jabber	Имеется	Имеется
	Мультимедиа проигрыватель	Имеется	Имеется
	Векторный графический редактор	Имеется	Имеется В составе КП «СинтезМ-О»
	Растровый графический редактор	Имеется	Имеется
	Система резервного копирования	Отсутствует	Имеется Система резервного копирования ПС «СинтезМ-СРК» (поддерживаются файлы, папки, дампы БД, образы

№ п/п	Наименование компонента	Astra Linux	«СинтезМ»
			виртуальных машин)
	Средства контроля и управления функционирование	Отсутствует	Имеется Контроль и управление функционированием КП «СинтезМ-КУФ»
	Сервер приложений, обеспечивающий исполнение приложений, разработанных в соответствии со спецификациями JavaEE2	Отсутствует	Имеется Сервер приложений ПС «СинтезМ-СП»
	Средства, обеспечивающие работу защищенной видеоконференц-связи	Отсутствует	Имеется Защищенная видеоконференцсвязь КП «СинтезМ-ЗВКС»
14	Сетевая система хранения данных и средства создания кластеров	• средство организации подключения к СХД по протоколу iSCSi; • средства кластеризации: Pacemaker, Corosync.	Содержит тот же состав средств, что и Astra Linux: • средство организации подключения к СХД по протоколу iSCSi; • средства кластеризации: Pacemaker, Corosync. Помимо перечисленных средств, содержит средства организации и управления территориально распределенных систем хранения данных (ПС «СинтезМ-СХД.01», ПС «СинтезМ-СХД.02») для организации системы хранения данных общим объемом до 1000ПБ на одном узле

Таблица 2 – Соответствие платформ Astra Linux и «СинтезМ» требованиям к построению территориально распределенных АСЗИ и отказоустойчивых, высоконагруженных ЦОД

№ п/п	Наименование компонента	Astra Linux	«СинтезМ»
1	Серверная операционная система с доверенной средой виртуализации и механизмами обеспечения отказоустойчивости и высокой доступности серверной группировки КСА или сегмента ЦОД (при выходе из строя одного или нескольких физических серверов)	-	+
2	Доверенные программные средства хранения данных, обеспечивающие построение территориально распределенной системы хранения данных большой емкости	-	+
3	Средства управления программной средой в серверных группировках ЦОД за счет автоматической инсталляции требуемого программного обеспечения на физических серверах, виртуальных машинах и рабочих станциях в соответствии с требуемой программной архитектурой защищенного вычислительного процесса по команде администраторов системы	-	+
4	Средства резервного копирования образов виртуальных машин и управления ими	-	+
5	Средства создания хранилищ резервных копий образов виртуальных машин, каталогов и дампов баз данных большой емкости	-	+
6	Интегрированные средства управления территориально распределенной АСЗИ (информационная безопасность, контроль и управление функционированием, резервное копирование, управление конфигурациями системы, ведение репозитория эталонных дистрибутивов АСЗИ)	-	+
7	Масштабирование системы за счет наращивания технических средств (сервера, АРМ и т.д.), программного обеспечения (эталонные дистрибутивы программного обеспечения со сценариями автоматической инсталляции на физических серверах, рабочих станциях и виртуальных машинах) в рамках обеспечения технических условий на систему	-	+
8	Формирование администратором правил разграничения доступа субъектов (групп пользователей, пользователей) к объектам доступа (программное обеспечение, каталоги и файлы, объекты баз данных, адреса электронной почты/белые списки), автоматическое формирование на их основе политик безопасности (содержат настроечные данные по разграничению) и их доведение на требуемые физические серверы, виртуальные машины и рабочие станции для реализации этих правил соответствующими механизмами разграничения доступа	-	+
9	Управление настройками межсетевого обмена, управление сетевым трафиком и правилами фильтрации сетевого трафика	-	+

Контрольные вопросы к разделу 2

1. Укажите основные компоненты цифровой программной платформы «СинтезМ» и их назначение.
2. Какие программные комплексы включает в себя ЗОС «СинтезМ»? Кратко охарактеризуйте их.
3. Каково назначение «СинтезМ-Сервер»?
4. Каково назначение «СинтезМ-Клиент»?
5. Что обеспечивает КП «ПСЗИ «СинтезМ»?
6. Укажите программные компоненты, входящие в состав КП «ПСЗИ «СинтезМ».
7. Какой комплекс программных средств в составе «СинтезМ» предназначен для создания АСЗИ в части обеспечения функционирования серверных группировок и автоматизированных рабочих мест пользователей?
8. Укажите программные компоненты, входящие в состав комплекса программных средств (КПС) «Функциональные сервисы».
9. Какие средства в составе КП «ПСЗИ «СинтезМ» обеспечивают резервное копирование?
10. С помощью какого программного средства можно осуществлять мониторинг и управление сетевым, серверным и периферийным оборудованием, а также виртуальными машинами?
11. Укажите уникальные встроенные возможности ЦПП «СинтезМ».
12. Что позволяет обеспечить применение ЦПП «СинтезМ» при построении территориально распределенных АСЗИ в интересах органов государственной власти и ФСО России?
13. Каким требованиям к построению территориально распределенных АСЗИ и отказоустойчивых, высоконагруженных ЦОД соответствует ЦПП «СинтезМ»?

3. Технологии создания защищённых центров обработки данных

3.1. Технологии, реализованные в цифровой программной платформе «СинтезМ»

Основным назначением программной платформы «СинтезМ» является ее применение при построении территориально распределенных автоматизированных систем в защищенном исполнении, в том числе защищённых ЦОД, в соответствии с требованиями нормативной базы ФСБ России, ФСТЭК России (в т.ч. приказ ФСТЭК России № 31, профилям защиты операционных систем и т.д.), на базе сервис-ориентированной программной архитектуры ЦОД (рисунок 5), что позволяет создать дата-центричную инфраструктуру защищенного ЦОД (рисунок 6).

Под дата-центричной инфраструктурой понимается архитектура, ориентированная на данные, которая позволяет корректировать бизнес-правила в ходе эксплуатации информационной системы, гибко изменяя как структуру данных, с которыми работает приложение, так и логику их обработки. Внедрение подобных элементов дата-центричной структуры, управляемой с помощью модели, дает возможность пользователю быстро получить выгоду от новых решений. Такая архитектура должна строиться на следующих принципах:

– основа архитектуры — данные, а не приложения;
– каждый бизнес-объект (как основных данных, так и транзакционных) должен быть представлен только единожды;
– представление каждого бизнес-объекта должно содержать все возможные точки зрения на него, в явном виде выделяя как его общие признаки, используемые для нескольких точек зрения, так и уникальные;
– структура данных должна следовать структуре концептуальных представлений бизнес-пользователей о предметной области; лучший способ формализации и обработки таких представлений — онтологическое моделирование и технологии «семантической сети», включающие графовые СУБД как хранилища онтологических моделей, языки доступа к ним и машины логического вывода;
– приложения не имеют собственных хранилищ данных и представляют собой не монолитные решения, а сервисы, предназначенные для решения конкретных бизнес-задач; для автоматизации бизнес-процессов формируются цепочки взаимодействующих сервисов, работающих с единым хранилищем;

Рисунок 5 - Сервис-ориентированная программная архитектура ЦОД

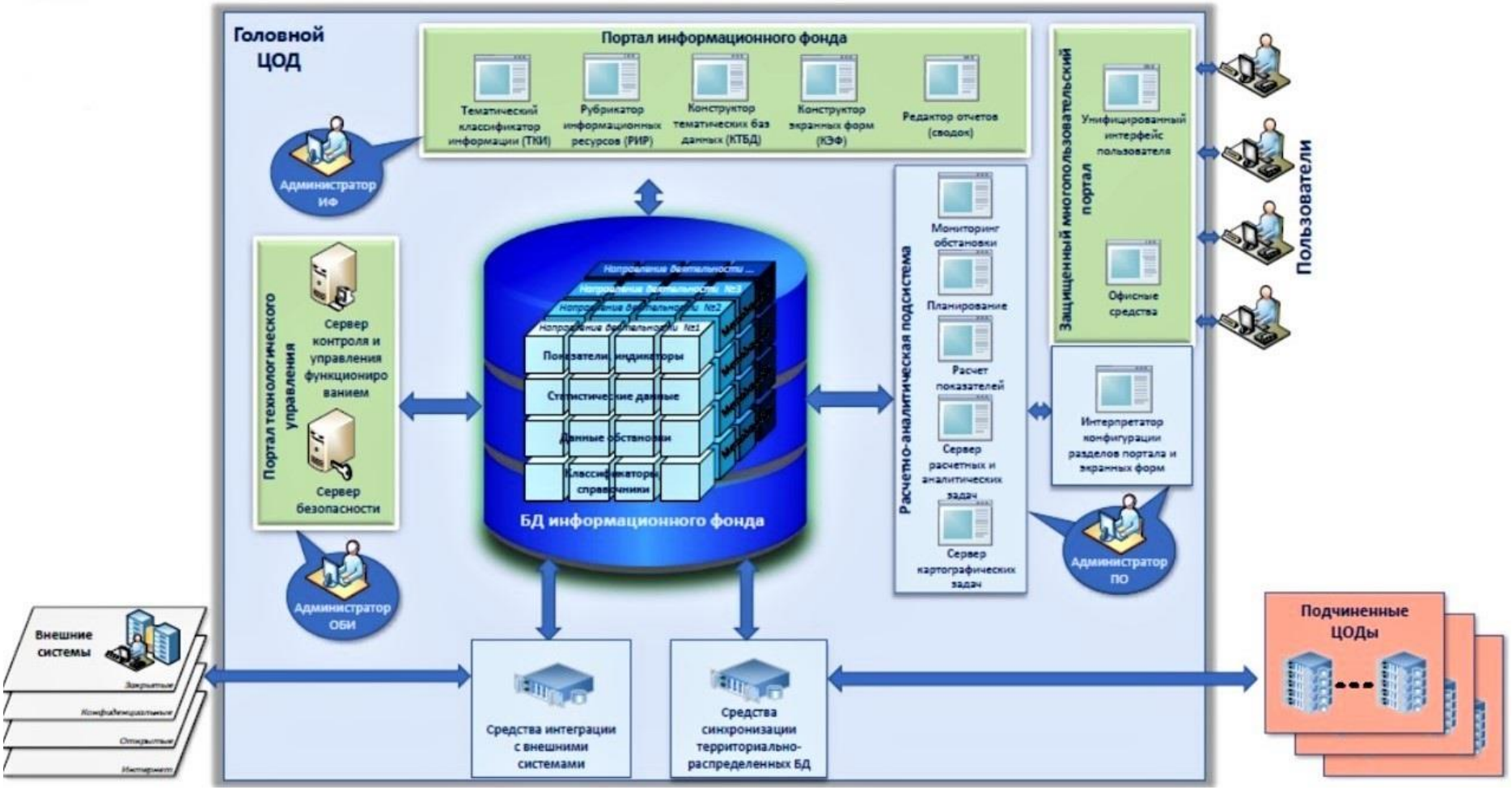

Рисунок 6 – Дата-центричная инфраструктура защищенного ЦОД

– приложения должны быть готовы к изменению структуры данных, получая для этого ее машиночитаемое представление из центрального репозитория и меняя алгоритмы своей работы в соответствии с изменениями структуры данных;
– как можно больше логики бизнес-алгоритмов должно быть вынесено из кода в онтологическую модель, что позволит настраивать алгоритмы обработки данных одновременно с изменением их структуры; прежде всего это касается настроек пользовательского интерфейса, алгоритмов преобразования данных и правил предоставления доступа к ним.

При такой архитектуре не нужны копии одних и тех же информационных объектов, а значит — не требуются сложные интеграционные механизмы; не нужны дополнительные усилия для формирования аналитических представлений; исчезает зависимость от производителей ПО, поскольку одни и те же данные смогут обрабатывать разные приложения; компании смогут не только экономить на поддержке ИТ-инфраструктуры, но и получить преимущества за счет быстрой адаптации своих инструментов к новым функциональным требованиям и более совершенной аналитике. Пример вариантов информационного обмена существующих АИС с создаваемым защищённым территориально-распределённым ЦОД представлен на рисунке 7. Пример интеграции данных внешних систем в создаваемый защищённый ЦОД представлен на рисунке 8.

В состав ЦПП «СинтезМ» входят компоненты, обеспечивающие выполнение всех функций, необходимых для построения, функционирования и эксплуатации АСЗИ (см. раздел 2.1):

- защищенная серверная операционная система «СинтезМ» с сертифицированной средой виртуализации, обеспечивающая построение защищенных отказоустойчивых центров обработки данных (ЦОД), а также применение гостевых операционных систем в т.ч. с унаследованным специальным программным обеспечением, функционирующим в среде ОС Windows, Linux-Centos, Linux-RedHat, Linux-Debian и др.;

- программные средства защиты информации (ПСЗИ), обеспечивающие построение АСЗИ как многопользовательских систем с разными правами доступа. Данные системы соответствуют требованиям по классу защищённости – не менее 1Г, а также требованиям приказа ФСТЭК России № 31;

- интегрированные средства управления АСЗИ, обеспечивающие: сбор, обработку данных мониторинга состояния АСЗИ (технические и программные средства, виртуальная среда, комплексы средств автоматизации и АСЗИ в целом); обеспечение безопасности информации; подготовку и управление конфигурацией системы и ее отдельных частей; управление средой виртуализации в высоконагруженных ЦОД; управление режимами работы системы; резервное копирование образов виртуальных машин, дампов баз данных и файловых хранилищ;

- средства ведения территориально распределенных репозиториев эталонных дистрибутивов программного обеспечения, которые входят в состав ПСЗИ «СинтезМ», функционирующего в среде ОС Linux и Windows с целью обеспечения версионности программного обеспечения АСЗИ, управления дистрибутивами при создании новых виртуальных машин, физических серверов и рабочих станций, а также обновления программного обеспечения с учетом требований по разграничению прав доступа (включая необслуживаемые территориально распределенные программно-аппаратные комплексы);

- средства ведения реестров сервисов в территориально-распределенных системах с обеспечением управления доступом к этим сервисам различных пользователей, а также доступ к сервисам в высоконагруженном, отказоустойчивом режиме работы;

- функциональные сервисы: защищенная электронная почта, система хранения данных, система резервного копирования, система защищенной видеоконференцсвязи (возможно расширение перечня сервисов по требованию заказчика).

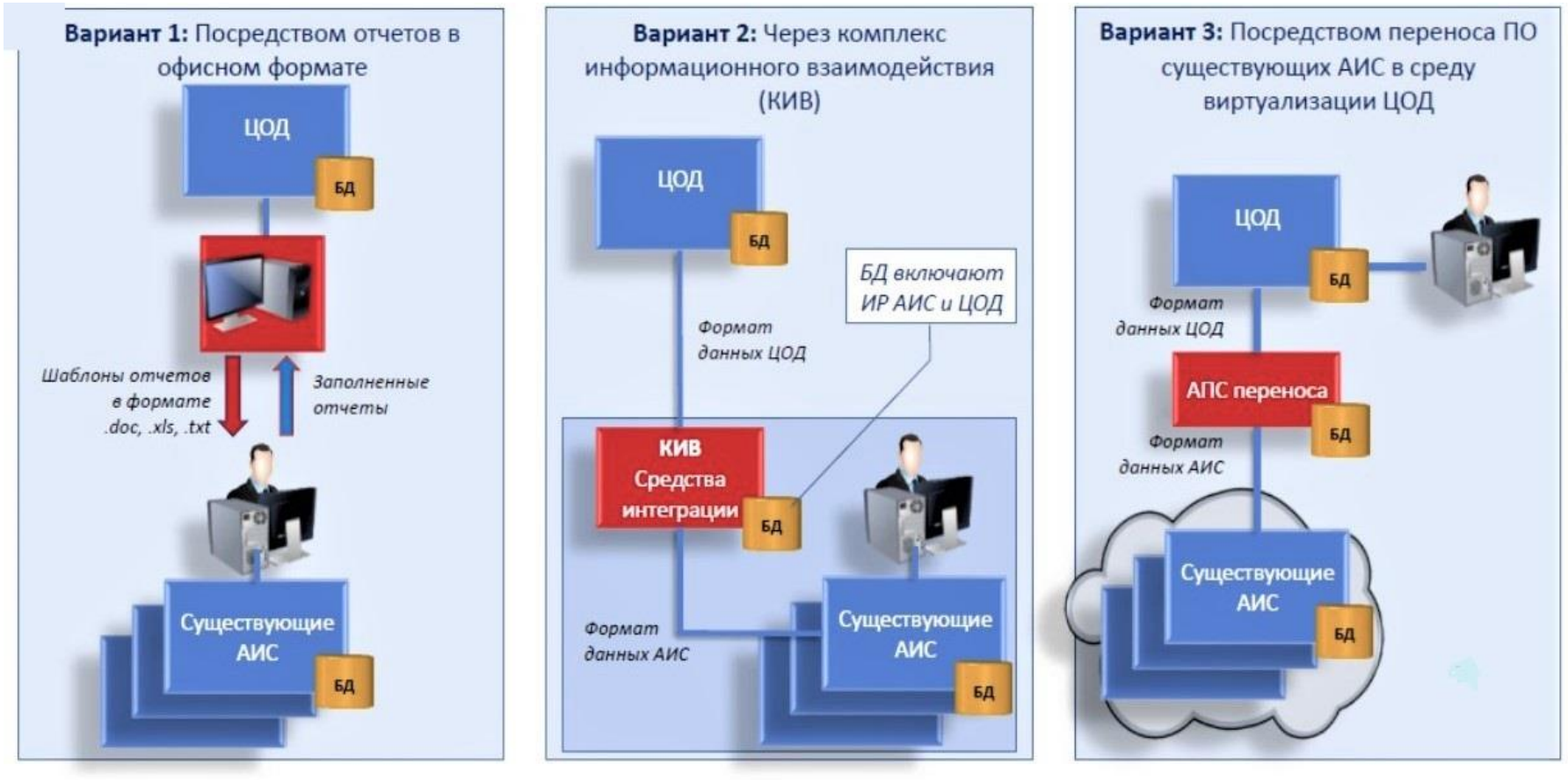

Рисунок 7 - Варианты информационного обмена существующих АИС с защищённым ЦОД

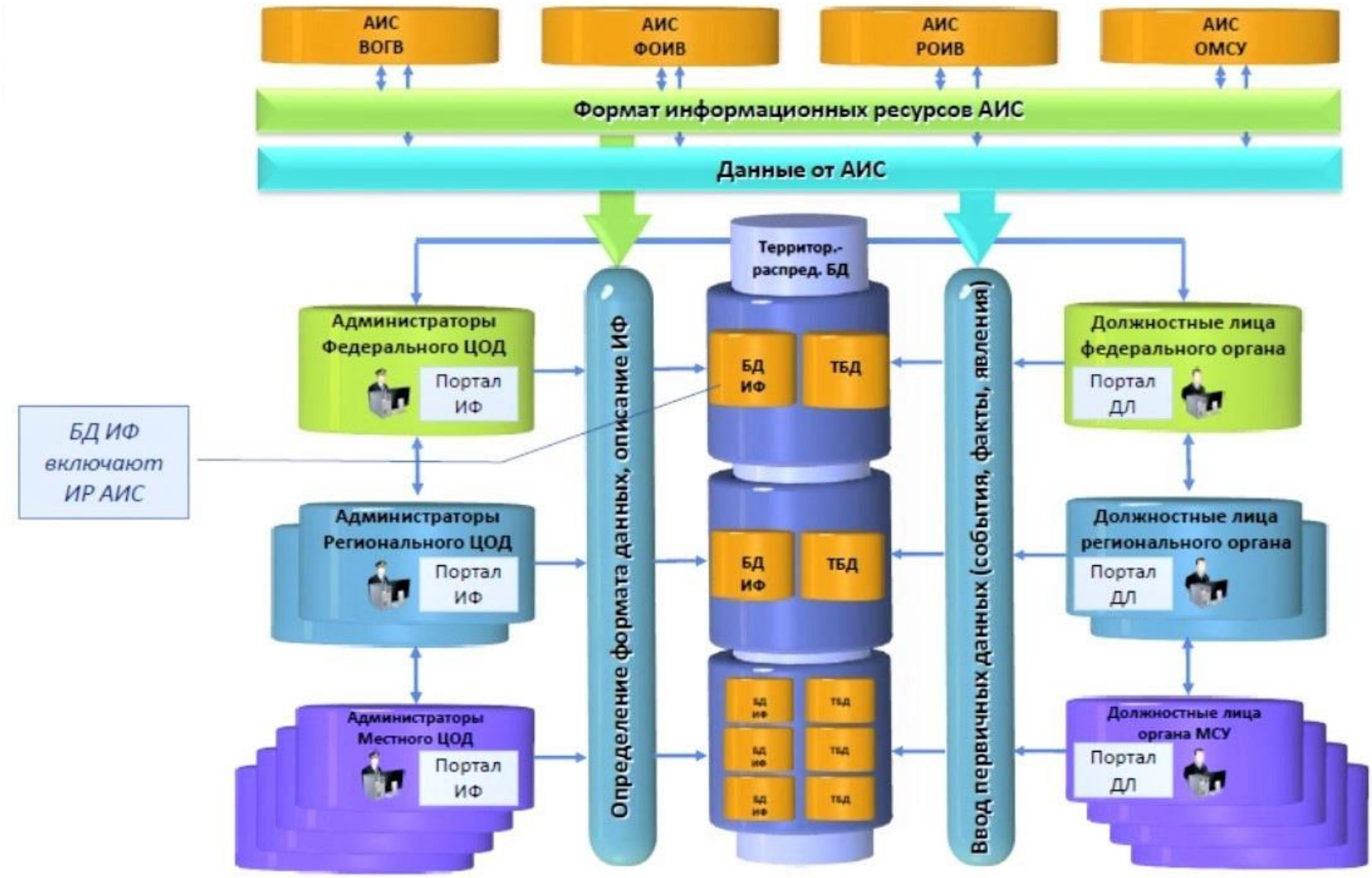

Рисунок 8 - Интеграция данных внешних систем в защищённый ЦОД

В цифровой программной платформе «СинтезМ» реализованы следующие технологии, которые могут быть использованы как сквозные при построении защищённых ЦОД:

- унифицированный протокол информационно-логического и технического взаимодействия и технология его ведения;
- универсальная технология форматно-логического описания и ведения данных любой предметной области;
- унифицированная система классификации и кодирования информации, ведения словарей, справочников и нормативно-справочной информации;
- портальная технология управления конфигурацией многоуровневых территориально распределенных аппаратно-программных комплексов защищенных ЦОД и СЦ;
- портальная технология управления подсистемой защиты информации;
- технология создания службой эксплуатации территориально распределенных ЦОД (СЦ) шаблонов тематических баз данных, отчетов, сводок, экранных форм, аналитических панелей, карт, схем и др. без необходимости проведения дополнительной сертификации (тематических исследований) эксплуатируемых систем.

Защищенные ЦОД создаются с использованием следующих основных средств:

- виртуализации, обеспечивающих организацию защищенного вычислительного процесса в ЦОД в виде изолированных виртуальных машин;
- инфраструктурных сервисов управления ЦОД: защиты информации, хранения данных, резервного копирования, мониторинга состояния технических и программных средств, управления конфигурациями и режимами работы ЦОД, единого времени;
- масштабирования ЦОД за счет наращивания технических средств и программного обеспечения;
- переноса существующих АС в ЦОД в виде программных и информационных ресурсов централизованного доступа (рисунок 9);
- создания единой системы защиты информации (рисунок 10);

• интеграции подсистем защиты информации, существующих автоматизированных систем в подсистему защиты информации ЦОД (рисунок 11).

Перечисленное выше позволяет создавать на базе ЦПП «СинтезМ» защищенные ЦОД, обладающие следующими основными свойствами.

Виртуализация (рисунки 12-13):

- управление виртуальными машинами / контейнерами;
- обеспечение переноса унаследованного ПО в среду виртуализации;
- функционирование гостевых ОС (Windows, Linux, Astra Linux и др.).

Комплексная безопасность:

- управление СЗИ от НСД, СОА;
- сопряжение с ГосСОПКА;
- взаимодействие с внешними системами; централизованное управление, мультипротокольным оборудованием, межсетевыми экранами;
- противодействие техническим разведкам.

Импортозамещение:

- отечественное общее, общесистемное и прикладное ПО;
- отечественные аппаратные платформы.

Масштабируемость (рисунок 14):

- наращивание технических средств;
- расширение функциональных задач за счет применения нового ПО;
- поэтапная автоматизация органов власти за счет подключения их к средствам автоматизации ЦОД;
- бесшовная интеграция существующих АИС в ЦОД.

Адаптивность:

- перенос в ЦОД ранее созданного ПО;
- включение ИР существующих АИС в реестр ИР ЦОД;
- модификация ПО и БД;
- адаптация ЦОД под функциональные задачи органов власти.

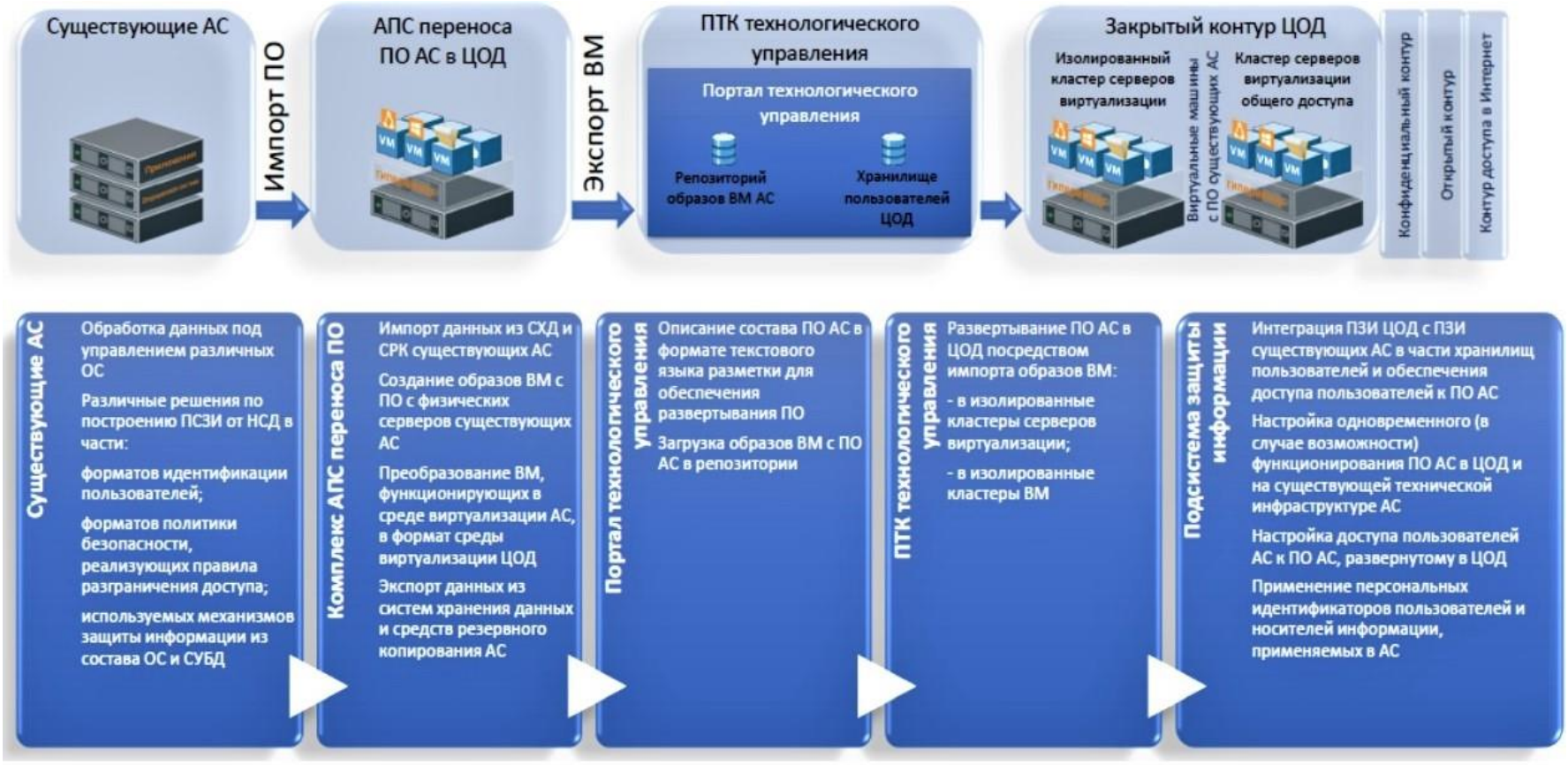

Рисунок 9 - Перенос ПО, существующих АС в ЦОД

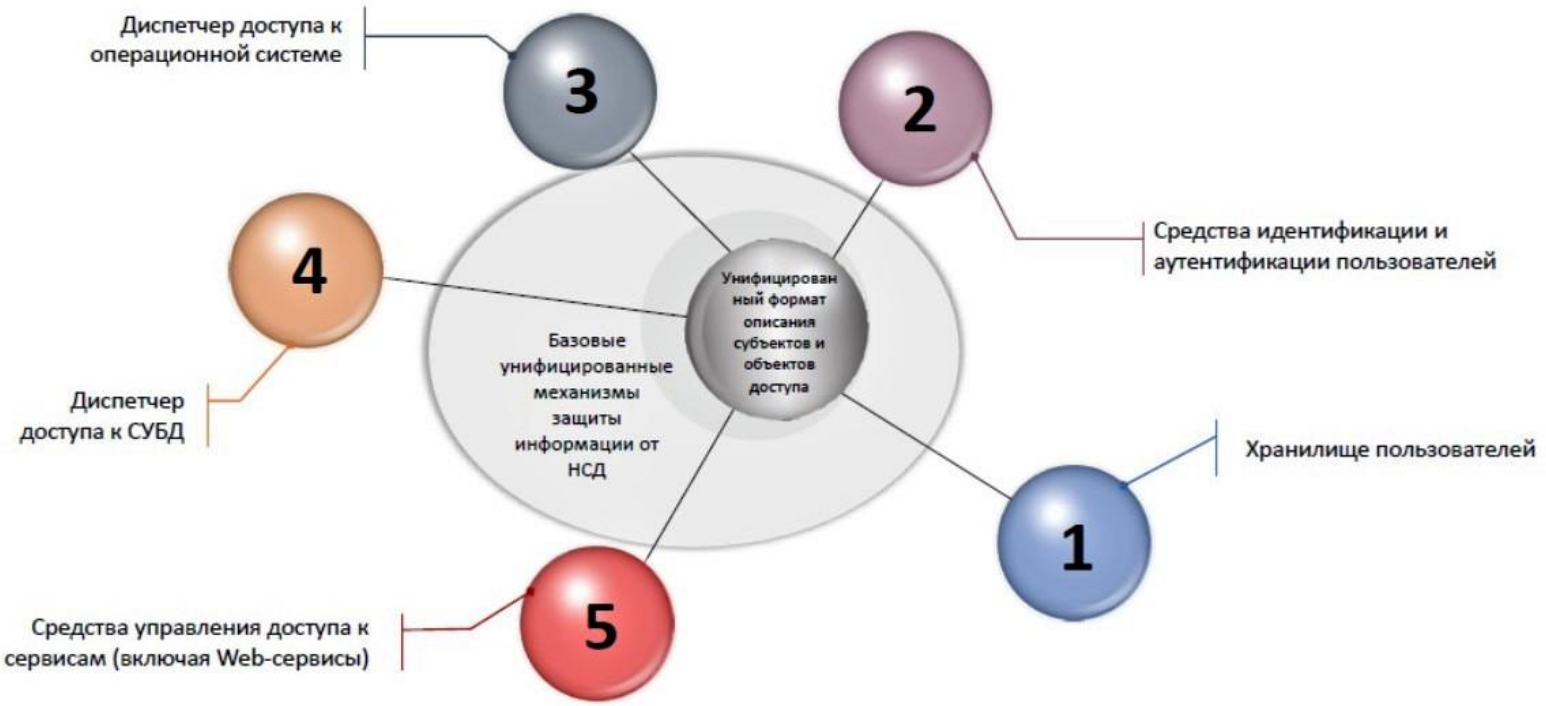

Рисунок 10 - Средства создания единой системы идентификации и аутентификации пользователей ЦОД

Рисунок 11 - Интеграция подсистем защиты информации существующих АС в подсистему защиты информации ЦОД

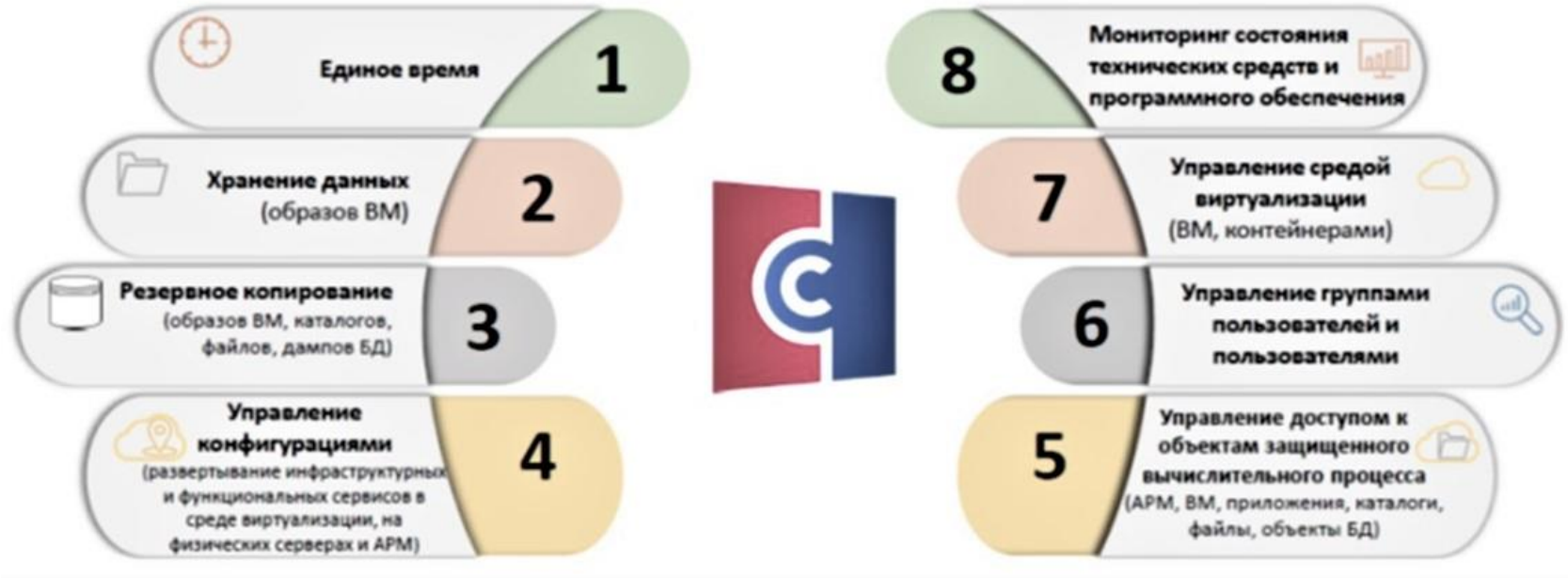

Рисунок 12 - Виртуализация в защищенном ЦОД

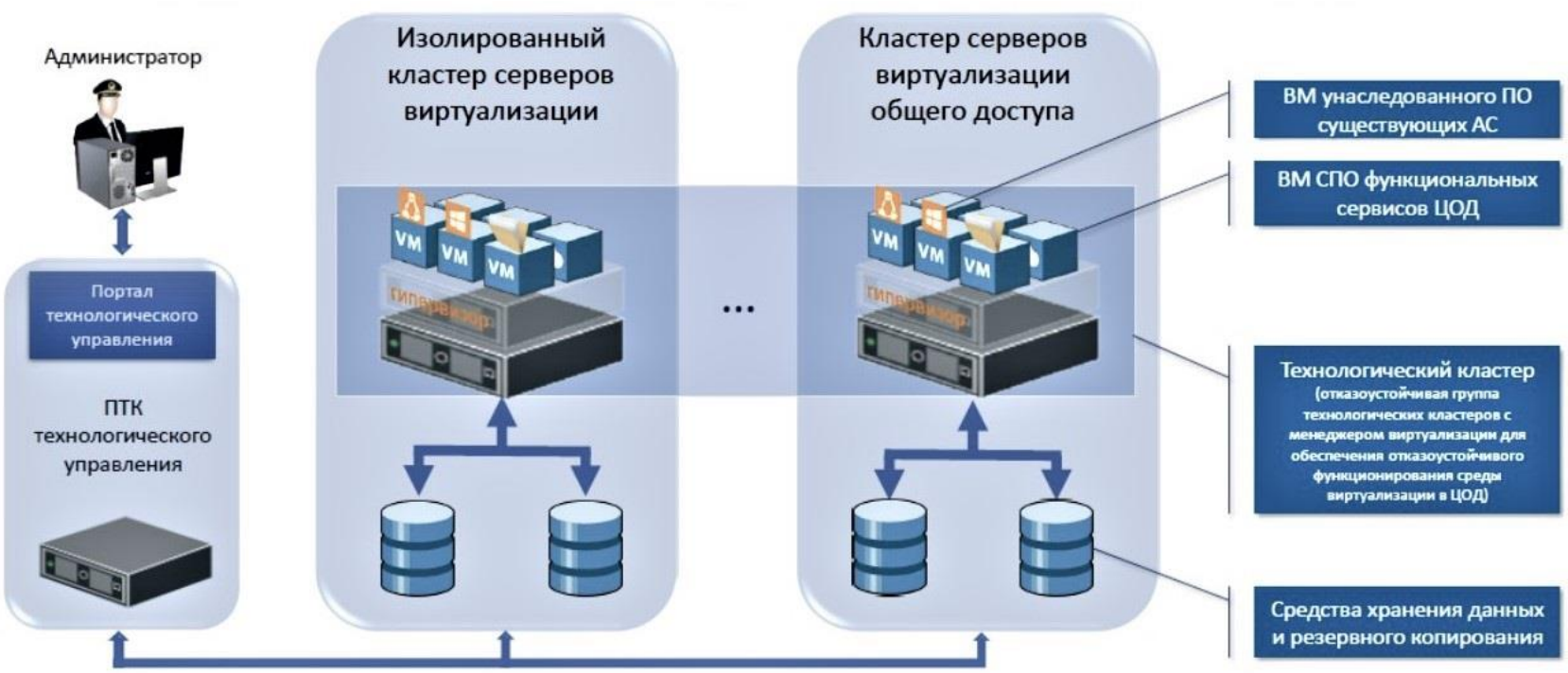

Рисунок 13 – Подсистемы виртуализации в защищенном ЦОД

Технологичность:

- технология построения и функционирования ЦОД;
- использование средств виртуализации;
- управление конфигурациями;
- подключение новых технических средств (ТС) и ПО;
- распределенное хранение данных;
- сопряжение территориально распределенных БД.

Унификация:

- применение унифицированных форматов, протоколов, стандартов;
- создание единого информационного пространства (единый формат ИР и БД);
- унификация программных и технических средств.

Экономичность:

- снижение эксплуатационных расходов;
- энергоэффективность;
- оптимизация расходов за счет применения унифицированных решений и их масштабирования.

Надежность:

- обеспечение резервирования;
- эксплуатация 24/7/365;
- информационный обмен с гарантированным доведением, в т.ч. синхронизация и репликация данных.

Таким образом, к ключевым свойствам технологий, используемых для создания защищённых ЦОД на базе ЦПП «СинтезМ», можно отнести:

- многоуровневую иерархическую или сетевую структуру;
- единую среду виртуализации;
- единое информационное пространство;
- распределенные базы данных;
- сквозную аутентификацию и идентификацию пользователей.

Структура территориально-распределенных защищенных ЦОД, созданных на базе цифровой платформы «СинтезМ» представлена на рисунке 15.

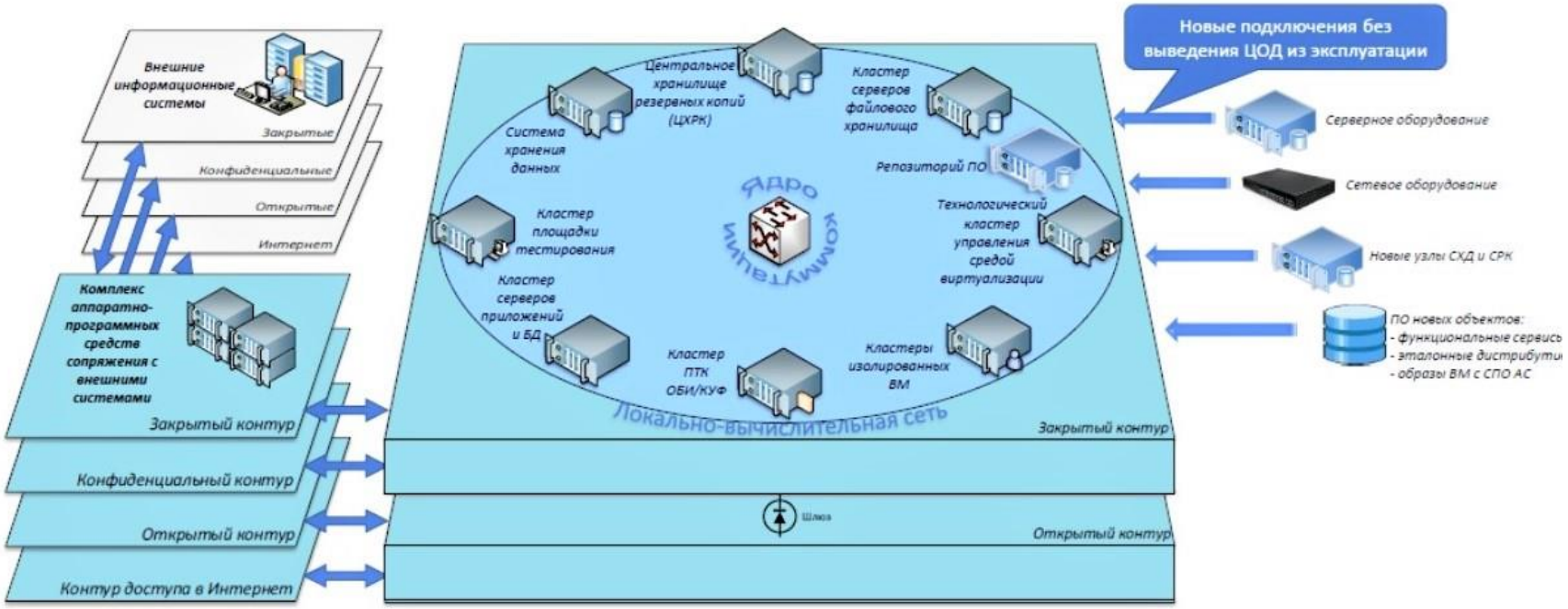

Рисунок 14 - Масштабирование защищённого ЦОД

3.2. Программная архитектура цифровой платформы «СинтезМ» для построения территориально распределенных ЦОД

Программные компоненты «СинтезМ» разработаны по модульному принципу с применением программного обеспечения с открытым кодом промышленного уровня (на базе ОС Linux), доработанного в части реализации требований по информационной безопасности.

Построение защищённых территориально распределенных ЦОД и СЦ на базе платформы «СинтезМ» осуществляется на основе виртуализации, что позволяет осуществлять удаленное администрирование всех объектов системы, контроль и управление функционированием, управлять политиками безопасности, осуществлять разграничение прав доступа пользователей, масштабировать и модифицировать систему, в том числе обеспечивая наращивание новых программных и аппаратных средств, а также миграцию ранее созданных других систем.

Программная архитектура платформы «СинтезМ» построена таким образом, что в каждом из взаимодействующих защищённых ЦОД (СЦ) применяются следующие портальные решения:

– портал технологического управления, обеспечивает технологическое управление системой и информационной безопасностью;

– портал информационного фонда, предназначен для ведения информационного фонда (классификаторов, кодификаторов, словарей, справочников, рубрикатор информационных ресурсов), создания шаблонов тематических баз данных, отчетов, расчетных процедур;

– защищенный многопользовательский портал, обеспечивает организацию доступа различных пользователей с различными правами к данным предметной области, а также представление информации в необходимом формате.

При построении защищённых ЦОД используются два основных функциональных компонента цифровой программной платформы «СинтезМ» (защищенной операционной системы): технологическая платформа «СинтезМ-Т» и информационная платформа «СинтезМ-И» (рисунок 16).

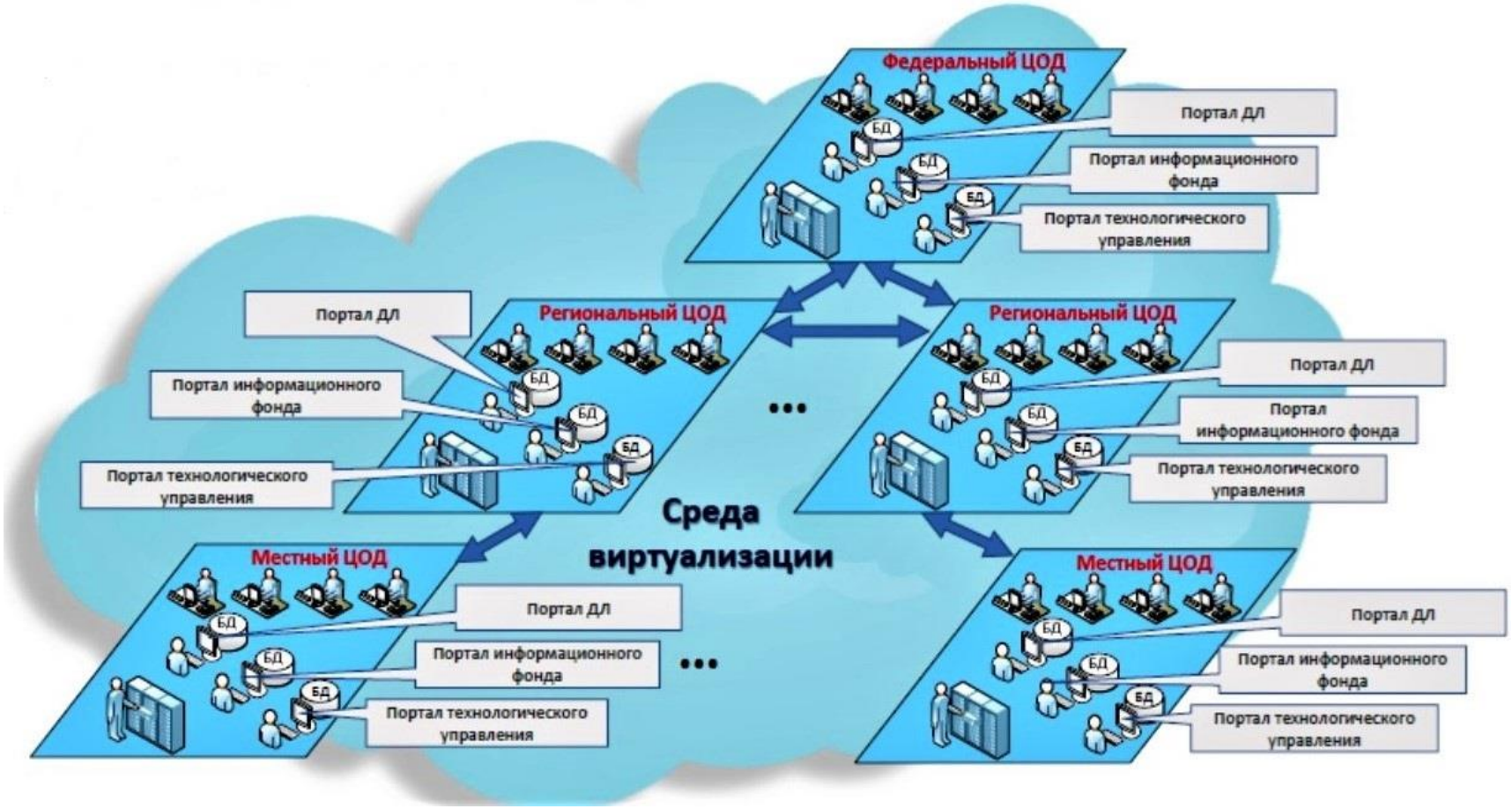

Рисунок 15 - Структура территориально распределенных защищенных ЦОД, созданных на базе цифровой платформы «СинтезМ»

Технологическая платформа обеспечивает создание, функционирование, удобное управление и эксплуатацию высоконагруженных, высокопроизводительных, территориально распределенных защищенных ЦОД и СЦ.

В состав «СинтезМ-Т» входят следующие составляющие, подробно описанные в разделе 2.1 данного учебного пособия:

- серверная и клиентская операционные системы;
- серверы приложений;
- система управления базами данных;
- система хранения данных;
- система резервного копирования;
- транспортная подсистема;
- система синхронизации территориально распределенных баз данных и другие программные средства.

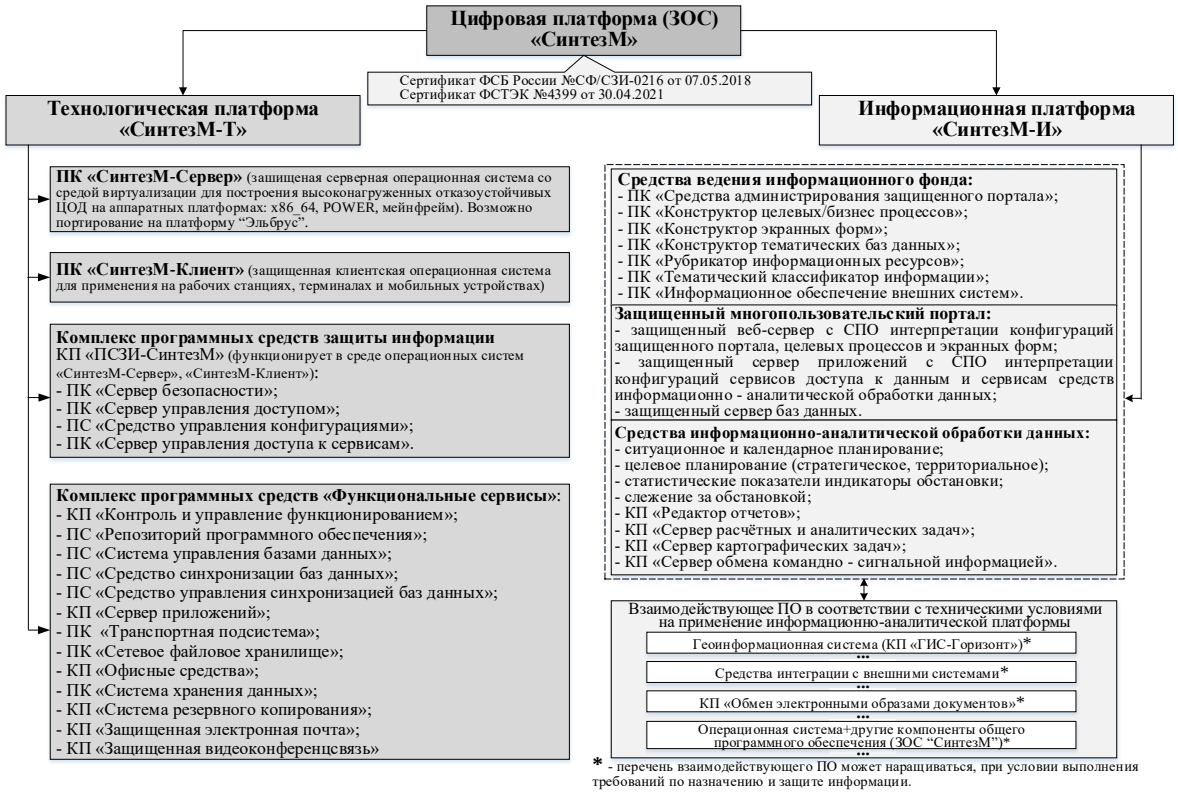

Рисунок 16 – Функциональные модули цифровой платформы «СинтезМ»

Кроме того, технологическая платформа включает встроенные программные средства защиты информации, которые позволяют вести данные о защищённом ЦОД (СЦ), управлять пользователями, группами пользователей и виртуальными машинами, разграничивать доступ субъектов к объектам системы, разрабатывать и применять политики безопасности, обеспечивать безопасный обмен с внешними информационными системами и др.

Следует подчеркнуть, что в отличие от других отечественных операционных систем в «СинтезМ», подсистема защиты информации «пронизывает» всю систему: от ядра до конечного пользователя. Что позволяет осуществлять аудит абсолютно всех процессов, происходящих в системе, в том числе контролировать все клиент-серверные соединения (включая удаленные), запрещая их, если они не соответствуют примененной политике безопасности.

Технологически защищенные ЦОД и СЦ на любом уровне строятся с учетом нескольких контуров информации: интернет, открытого, конфиденциального и закрытого - и включают в себя ядро коммутации, кластеры серверов и виртуальных машин, а также аппаратно-программные средства сопряжения с внешними системами.

Информационная платформа «СинтезМ-И» обеспечивает решение прикладных информационных задач любого уровня сложности. При определенных условиях она может работать под управлением не только защищённой операционной системы (ЗОС) «СинтезМ», но и любой операционной системы, созданной на базе ядра Linux (Astra Linux, Alt Linux, BaseAlt, МСВС и др.).

3.3. Информационно-аналитическая работа с использованием «СинтезМ-И»

В состав «СинтезМ-И» включены программные средства, обеспечивающие создание и ведение информационного фонда ведомства (организации), конструирование тематических баз данных, генерацию экранных форм, отчетов (сводок), формирование целевых (бизнес) процессов, разработку офисных документов, ведение электронного документооборота с применением электронной подписи, ведение сеансов защищенной видеоконференцсвязи и использование защищенной электронной почты.

Информационно-аналитическая работа с использованием «СинтезМ-И» заключается в следующем.

На первой стадии (рисунок 17) осуществляется информационное описание предметной области ведомства (организации): наполнение классификатора информации и реестра информационных ресурсов, создание шаблонов тематических баз данных, экранных форм, отчетов, планов, расчетных процедур, регламентов информационного обмена.

На второй стадии (рисунок 18) организуется фиксация и сбор информации о событиях, явлениях и процессах, являющихся базисом многомерного массива данных соответствующей предметной области деятельности ведомства (организации).

На третьей стадии (рисунок 19) проводится обработка данных в целях обеспечения получения достоверной информации о состоянии предметной области и принятия своевременных управленческих решений.

Таким образом, применение отечественной программной платформы «СинтезМ» для создания защищенных ЦОД, ситуационных центров и автоматизированных систем в защищенном исполнении обеспечивает:

- эффективное управление объектами и ресурсами на основе получения актуальных данных (показателей деятельности) в любой предметной области;

- использование унифицированных технологий, обеспечивающих единообразное представление данных;

- защиту персональных и других охраняемых законом данных;

- экономию и рациональное использование финансовых средств, за счет отсутствия необходимости привлечения промышленности для модернизации, модификации или масштабирования систем (все эти задачи решаются службой эксплуатации ведомства (организации)).

Стадии информационно-аналитической работы в среде «СинтезМ-И»

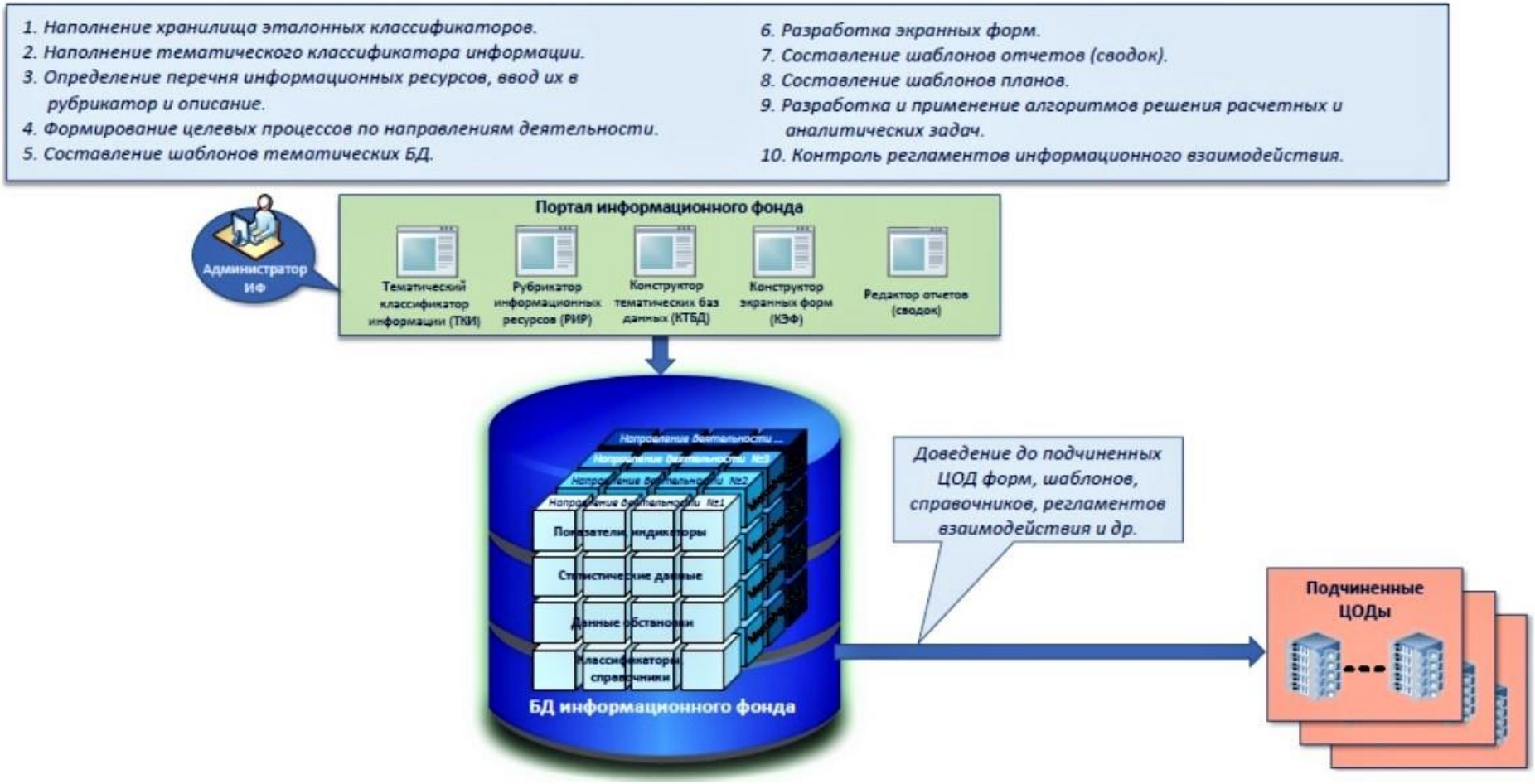

Рисунок 17 - Стадия 1: Описание информационных ресурсов предметной области

Стадии информационно-аналитической работы в среде «СинтезМ-И»

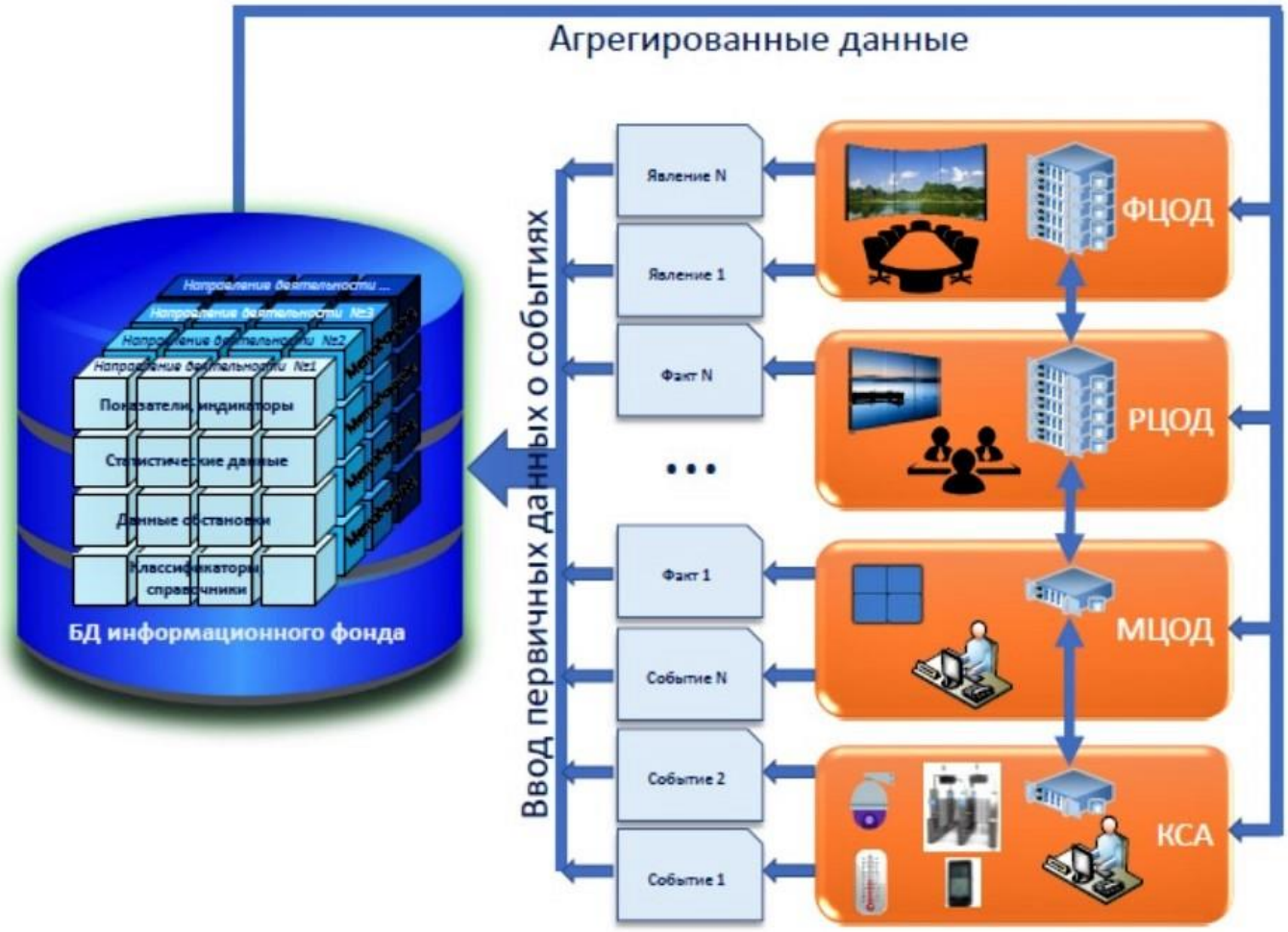

Рисунок 18 - Стадия 2: Фиксация, сбор и обработка первичной информации о событиях, фактах, явлениях

Стадии информационно-аналитической работы в среде «СинтезМ-И»

Рисунок 19 - Стадия 3: Информационная поддержка управленческой деятельности

Контрольные вопросы к разделу 3

1. Что собой представляет дата-центричная инфраструктура защищенного ЦОД?
2. Какие принципы лежат в основе построения дата-центричной структуры?
3. Каково основное назначение программной платформы «СинтезМ»?
4. Какие компоненты в составе ЦПП «СинтезМ» обеспечивают выполнение всех функций, необходимых для построения, функционирования и эксплуатации АСЗИ?
5. Какие технологии, которые могут быть использованы как сквозные при построении защищённых ЦОД, реализованы в цифровой программной платформе «СинтезМ»?
6. С использованием каких основных средств создаются защищенные ЦОД?
7. Какие варианты информационного обмена существующих АИС с ЦОД ЕГССПУ имеются?
8. Какими свойствами обладают защищенные ЦОД, созданные на базе ЦПП «СинтезМ»?
9. Какова процедура переноса ПО, существующих АС в ЦОД в виде программных и информационных ресурсов централизованного доступа?
10. Какая технология лежит в основе построения территориально распределенных ЦОД и СЦ на базе платформы «СинтезМ»?
11. По какому принципу построена программная архитектура платформы «СинтезМ»?
12. Два каких основных компонента цифровой программной платформы «СинтезМ» используются при построении защищённых ЦОД?
13. Какова структура территориально распределенных защищенных ЦОД, созданных на базе цифровой платформы «СинтезМ»?
14. Что обеспечивает технологическая платформа «СинтезМ-Т»?
15. В чем отличие «СинтезМ» от других отечественных операционных систем с точки зрения обеспечения защиты информации?
16. Что обеспечивает информационная платформа «СинтезМ-И»?

17. Перечислите стадии информационной работы с использованием «СинтезМ-И».
18. Что обеспечивает применение отечественной программной платформы «СинтезМ» для создания защищенных ЦОД, ситуационных центров и автоматизированных систем в защищенном исполнении?

4. Квантовые вычисления – основа перспективных защищённых инфокоммуникационных технологий

С момента изобретения электронного калькулятора в 1960-х годах в мире вычислений произошел значительный прогресс. Последние несколько лет были особенно революционными для создания новых технологий обработки информации. Классические вычисления стали экспоненциально быстрее и мощнее, а наши вспомогательные устройства стали меньше и более адаптируемыми.

В последние годы начался процесс эволюции от классических вычислений (рисунок 20) к новой эре данных, называемой квантовыми вычислениями (рисунок 21). Предполагается, что квантовые вычисления ускорят развитие систем искусственного интеллекта (англ. AI - artificial intelligence), а также методов аналитики данных. Мощность и скорость квантовых вычислений помогут решить некоторые из самых больших и сложных проблем, с которыми сталкивается человечество. Исследователи надеются использовать квантовые принципы для создания сверхмощного компьютера, который решал бы проблемы, недоступные обычным компьютерам - от повышения кибербезопасности и моделирования химических реакций до разработки новых лекарств и повышения эффективности цепочек поставок.

Исследовательская фирма Gartner кратко описывает квантовые вычисления как: «использование атомных квантовых состояний для осуществления вычислений. Данные хранятся в кубитах (квантовых битах), которые могут одновременно хранить все возможные состояния. На данные, хранящиеся в кубитах, влияют данные, хранящиеся в других кубитах, даже когда они физически разделены. Этот эффект известен как запутанность». В упрощенном описании квантовые компьютеры используют квантовые биты, или кубиты, вместо традиционных двоичных разрядов единиц и нулей для цифровой связи. Классический бит имеет значение 0 или 1. Квантовые биты, напротив, могут иметь значение 0 или 1 одновременно, т.е. объект может существовать в двух или более состояниях одновременно. Это странное качество проистекает из квантовой концепции, называемой суперпозицией. Более подробное объяснение элементов, задействованных в квантовых вычислениях, было первоначально опубликовано в ежегодном исследовательском журнале Принстонского университета. Ниже приведём краткое описание концепций и терминов квантовых вычислений.

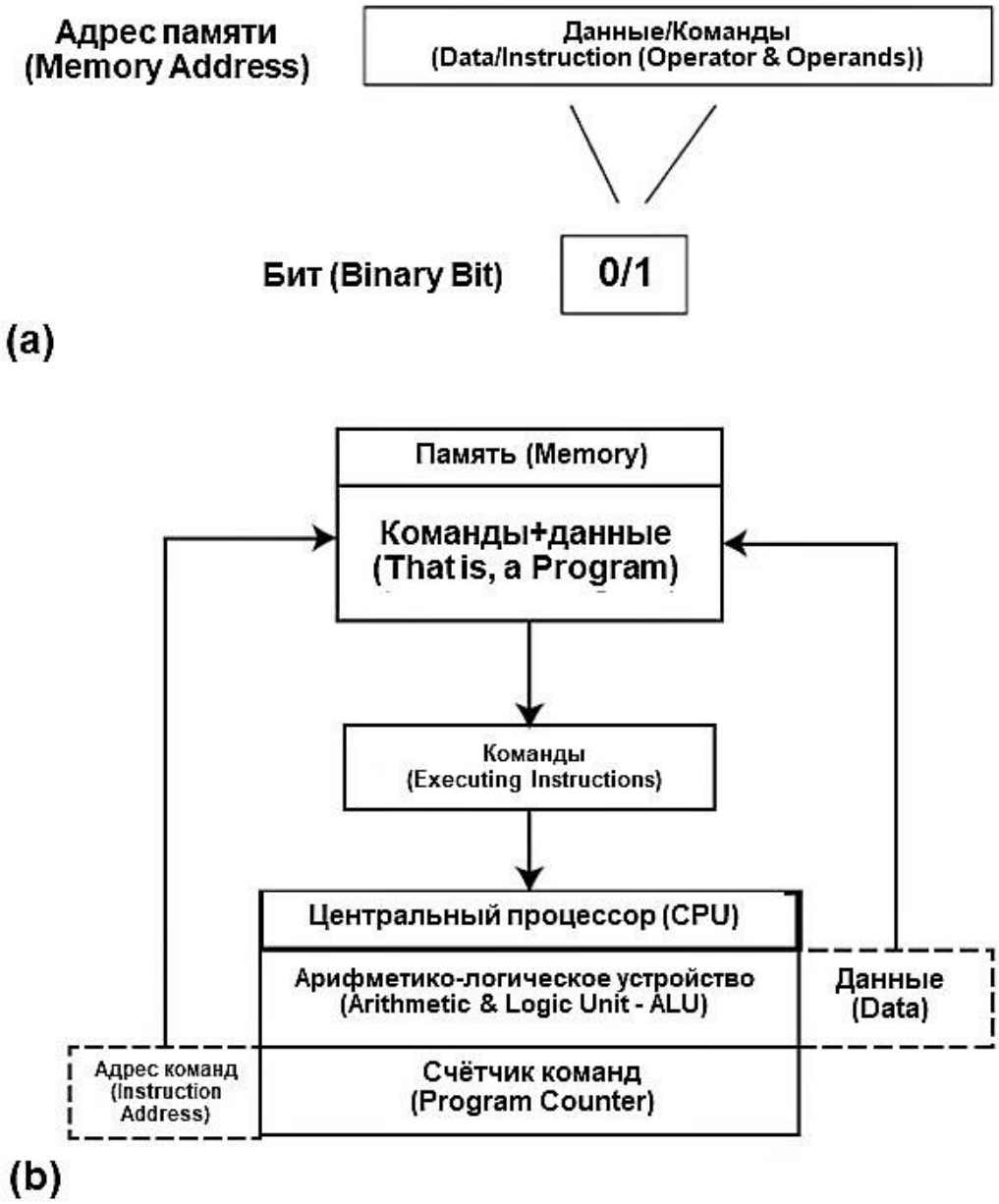

Рисунок 20 – Пример цифрового компьютера:
a) представление информации; b) компьютерная архитектура

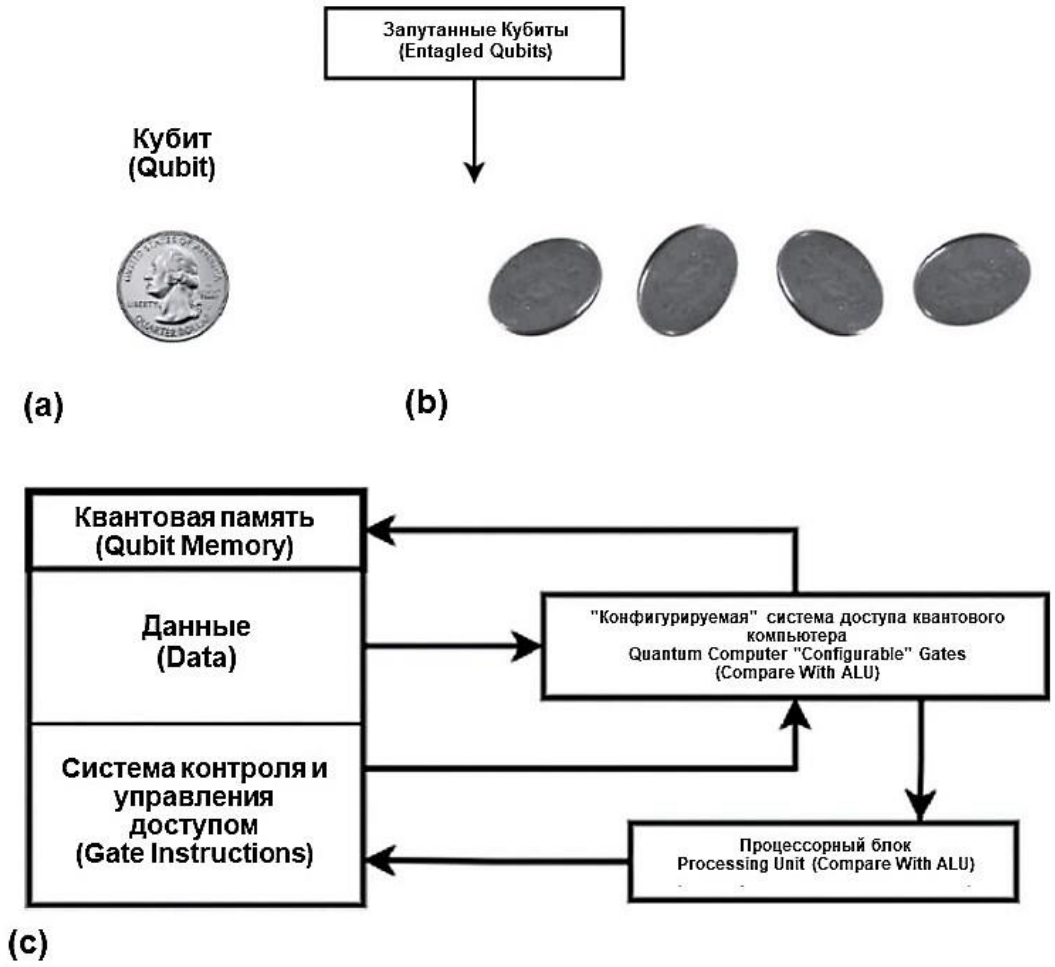

Рисунок 21 – Пример квантового компьютера: a) один кубит равен 0 и 1; b) четыре кубита представляют все 2^4 возможные перестановки; c) квантовый компьютер

Квантовая лексика и терминология

Кубиты не биты. Квантовые компьютеры выполняют вычисления с квантовыми битами, или кубитами, а не с цифровыми битами в традиционных компьютерах. Кубиты позволяют квантовым компьютерам рассматривать невообразимые ранее объемы информации.

Суперпозиция. Квантовые объекты могут находиться в более чем одном состоянии одновременно. Если применить эту концепцию к повседневной жизни, это приведет к парадоксу, известному как «кот Шредингера», в котором вымышленный кот одновременно жив и мертв. Например, кубит может одновременно представлять значения 0 и 1, тогда как классические биты могут быть только 0 или 1.

Запутанность. Чтобы квантовые вычисления полностью раскрыли свой потенциал, кубиты должны будут не только сохранять свои квантовые состояния, но и обмениваться информацией друг с другом. Они делают это с помощью квантового свойства, называемого запутанностью. Когда кубиты запутываются, они образуют связь друг с другом, которая сохраняется независимо от расстояния между ними. Если один кубит действует определенным образом, его запутанный близнец будет действовать таким же образом, независимо от расстояния, которое их разделяет. Они могут быть на расстоянии миллионов миль, но при этом действовать в идеальном согласии. Запутывая кубиты, исследователи могут создавать квантовые схемы, которые могут выполнять сложные вычисления. Это противоречащее интуиции представление, которое выдержало множество испытаний с момента его открытия в 1930-х годах, привело к тому, что Альберт Эйнштейн назвал запутанность «жутким действием на расстоянии».

Типы кубитов. В основе квантового компьютера лежит кубит, квантовый бит информации, который обычно создается из частицы (атома, иона или электрона) настолько маленькой, что она проявляет квантовые свойства, а не подчиняется классическим законам физики, которые управляют нашей повседневной жизнью. В разработке находятся несколько типов кубитов.

Сверхпроводящие кубиты, или трансмоны (от англ. «transmon») - кубиты, которые уже используются в прототипах компьютеров, созданных Google, IBM и другими. Трансмон является своего рода искусственным атомом, построенным из таких материалов, как ниобий и алюминий, которые при низких температурах могут проводить электрический ток без сопротивления. Эти материалы образуют небольшую электрическую цепь, которая ведет себя как атом. Состояние кубита, квант 0 или 1, представлено количеством энергии, хранящейся в искусственном атоме.

Захваченные атомы - атомы, захваченные лазером, могут вести себя как кубиты. Захваченные ионы (заряженные атомы) также могут действовать как кубиты.

Кремниевые спиновые кубиты - перспективная технология включает захват электронов в кремниевые камеры для управления квантовым свойством, известным как спин. Спин описывает угловой момент

электрона и иногда сравнивается с вращением волчка. Однако он также аналогичен магнетизму, потому что, как и у магнита, спин электрона может указывать либо вниз, либо вверх, представляя значения 0 и 1.

Топологические кубиты - все еще находящиеся на ранней стадии развития, квазичастицы, называемые фермионами Майорана, которые существуют в определенных материалах, имеют потенциал для использования в качестве кубитов. Дополнительную информацию можно найти на сайте Принстонского университета.

Одной из основных проблем для трансмона и других типов кубитов является поддержание квантового состояния достаточно долго, чтобы быть полезным. Воздействия окружающей среды, такие как вибрации, тепло или свет, могут нарушить квантовые свойства. Эта «декогеренция» может затруднить поддержание частицы в квантовом состоянии даже в течение короткого промежутка времени. Чтобы решить эту проблему, исследователи изучают способы удержания и укрепления кубитов в течение относительно длительных периодов времени - в течение нескольких сотен микросекунд, что достаточно долго, чтобы выполнить множество вычислительных шагов.

Даже с этими определениями концептуализация понятий квантовых вычислений и запутанности является сложной задачей, поскольку они охватывают «загадочный» мир субатомной физики.

Как и в других областях науки, существуют конкурирующие теории о том, что является квантовым доказательством. Уже произошло несколько событий в этой эволюции, которые открыли путь в новую эру квантовых вычислений. В том числе квантовые прорывы за счет использования световых сигналов от сетей фотонов и квантового кодирования в кремниевых микрочипах.

Открытие, сделанное исследовательской группой из лаборатории квантовой фотоники в RMIT в г. Мельбурне (Австралия), впервые продемонстрировало идеальную передачу состояния запутанного квантового бита (кубита) на интегрированном фотонном устройстве. В 2019 году квантовый компьютер Google выполнил расчеты менее чем за четыре минуты, что примерно в 158 миллионов раз быстрее, чем аналогичные расчёты на самом быстром суперкомпьютере в мире, которому потребовалось бы примерно 10000 лет.

В США в рамках закона о «Национальной квантовой инициативе» создаётся государственно-частное партнёрство с объёмом

финансирования 1,2 миллиарда долларов США. Пять новых национальных исследовательских центров квантовой информации были созданы исследователями Министерства энергетики США из специалистов академических кругов, национальных лабораторий и промышленности США. Эти организации будут работать вместе, чтобы способствовать развитию исследований в области квантовой информатики и включают совместные проекты таких компаний, как IBM, Microsoft, Intel, Applied Materials и Lockheed Martin.

В гонке участвуют все глобальные ИТ-корпорации - Google, IBM, Alibaba, Intel, Microsoft, которые тестируют свои разработки на какой-либо из четырех существующих технологических платформ:

- на фотонных чипах;
- на сверхпроводниковых квантовых цепях;
- на основе нейтральных атомов;
- на ионах.

Коммерческие образцы с малым количеством кубитов предлагают отдельные стартапы. Например, во второй половине июля 2021 года пятикубитовый квантовый процессор Soprano всем желающим начала продавать нидерландская компания QuantWare. У российских ученых из МФТИ есть аналогичный прототип, но он пока не стал бизнес-продуктом.

Большинство компаний в мире сегодня предоставляет заказчикам квантовые симуляторы из лабораторий – облачные платформы. Например, компания Google, с мая 2021 года предлагает доступ к 100-кубитному прототипу компьютера. Ученые из Российского квантового центра (РКЦ) также разработали подобный сервис.

Эксперты предполагают, что уже в 2023 году устройства нового типа появятся на основе 1 тыс. кубитов, а к 2030 году мощность квантовых установок достигнет миллиона единиц. Компания Google обещает выпустить первый коммерческий образец процессора на 1 млн. квантовых битов к 2029 году.

Лидером по внедрению может остаться Китай, который сегодня осуществляет максимальные инвестиции в квантовые технологии. КНР уже вложила 10 млрд. долларов США в создание открывшейся осенью 2020 года лаборатории в провинции Хэфэй.

Евросоюз в 2018 году объявил о программе Quantum Flagship. Суммарный бюджет ЕС на данные проекты составил 7 млрд. долларов США. Национальная квантовая инициатива в США предусматривает выделение на аналогичные исследования 1,2 млрд. долларов США до 2024 года.

Российская дорожная карта развития квантовых технологий, утвержденная в июле 2020 года, предполагает расходы порядка 50 млрд. рублей до 2024 года по нескольким направлениям исследований.

В России новыми вычислительными технологиями занимаются несколько госкомпаний.

Исследования в области «квантовых коммуникаций» находятся в ведении ОАО «РЖД», и проводимые компанией исследования направлены в первую очередь на борьбу с утечками конфиденциальной информации путём создания волоконно-оптических линий связи (ВОЛС) с квантовой криптографией. В таких ВОЛС распределенный между двумя абонентами квантовый ключ используется для симметричного шифрования информации, отправленной по любым открытым каналам связи. В июне 2021 года ОАО «РЖД» ввела в эксплуатацию первую ВОЛС защищенной связи протяжённостью 700 км между Москвой и Санкт-Петербургом. Это вторая в мире по протяжённости защищённая ВОЛС после китайской линии между Шанхаем и Пекином, протяженность которой достигает 4,6 тыс. километров. Российский проект создан на базе оригинальных отечественных решений. Реализация первых пилотных сервисов на новой инфраструктуре запланирована на 2023-24 годы. Планируется, что к 2024 году в России появится более 7 тыс. км «квантовых сетей» – ВОЛС защищаемых с помощью квантовой криптографии.

Дорожная карта также предполагает создание рынка отечественного оборудования для обслуживания таких линий связи. Одним из таких проектов занимается госкорпорация «Ростех», ответственна за разработку и внедрение квантовых сенсоров. Датчики можно будет использовать в системах спутниковой, наземной и сотовой связи для сверхточного измерения положения космических аппаратов и беспилотников, а также в сфере Интернета вещей.

Третьим направлением исследований, а именно «кантовыми вычислениями» занимается госкорпорация «Росатом». В настоящее время проводится координация работы научных коллективов, создание

инфраструктуры, закупка оборудования, комплектование лабораторий, которые планируется разместить в том числе в центре нанофабрикации на территории «Сколково» (строительство должно начаться в 2021 году). Компания «Росатом» в партнёрстве с компанией «Сбер» планирует создать в 2021 году прототип квантового компьютера на 5 кубитах.

Можно ожидать, что квантовые вычисления найдут широкое применение в защищённых ЦОД (СЦ). Установленные в них квантовые компьютеры могут быть использованы для решения сложных оптимизационных задач. Квантовая криптография может быть использована для защиты критически важной конфиденциальной информации как передаваемой по телекоммуникационной подсистеме внутри защищённого ЦОД (СЦ), так и по внешним линиям связи между ЦОД (СЦ) и терминальным оборудованием пользователей.

Квантовые компьютеры представляют собой смену парадигмы вычислений. Квантовые системы увеличиваются как в размере, так и в надежности и приближаются к тому, чтобы продемонстрировать реальное преимущество перед классическими компьютерами. Квантовые компьютеры используют возможность существования кубитов в разных состояниях одновременно. Это означает, что квантовые компьютеры могут рассматривать намного больше информации одновременно, оценивая множество результатов одновременно, тем самым увеличивая свою вычислительную мощность в геометрической прогрессии. Поскольку эта технология все еще находится на такой ранней стадии, возможно, ее истинное влияние еще полностью не понято. Это открывает широкие возможности для исследователей.

Приведём основные потенциальные преимущества квантовых вычислений для общества на основе исследований, проведённых Quantum Computing: Benefits And Applications (autome.me).

Квантовые компьютеры обеспечивают **огромную скорость** для решения конкретных задач. Исследователи работают над созданием алгоритмов для поиска и решения проблем, подходящих для квантового ускорения.

Скорость квантовых компьютеров улучшит многие из наших технологий, которые требуют **огромной вычислительной мощности,** такие как машинное обучение, устройства и системы подвижной связи 6G, сверхскоростные поезда (и многие другие методы транспортировки) и т.п.

Квантовые вычисления важны для анализа **больших данных** (англ. Big Data), поскольку при их обработке нужны эффективные компьютеры для обработки того огромного количества данных, которые производятся ежедневно людьми и устройствами Интернета вещей (англ. IoT – Internet of Things).

Квантовая информационно-телекоммуникационная сеть – «квантовый Интернет» - должна стать более безопасной, чем существующая информационно-телекоммуникационная сеть Интернет. Квантовая запутанность гарантирует, что этот новый вид Интернета будет значительно лучше защищен от хакеров. Любая попытка перехватить передачу данных нарушит их целостность. Сравнивая переданный фотон с его запутанным двойником, приемник может определить, нарушил ли злоумышленник передачу. Однако следует отметить, что квантовые вычисления дадут новые возможности и злоумышленникам для несанкционированного доступа к конфиденциальной информации путём использования их вычислительной мощности для взлома криптоалгоритмов.

Несмотря на вычислительную **мощность**, квантовые компьютеры помогут **снизить энергопотребление** от 100 до 1000 раз, если они используют квантовое туннелирование.

К научным категориям, на которые квантовая физика напрямую повлияет, относятся физика, химия, математика и биология. Приложения для промышленности повлияют на отраслевые вертикали, такие как здравоохранение, финансы, коммерция, связь, безопасность, кибербезопасность и криптография, энергетика, освоение космоса и многие другие дисциплины (рисунок 22).

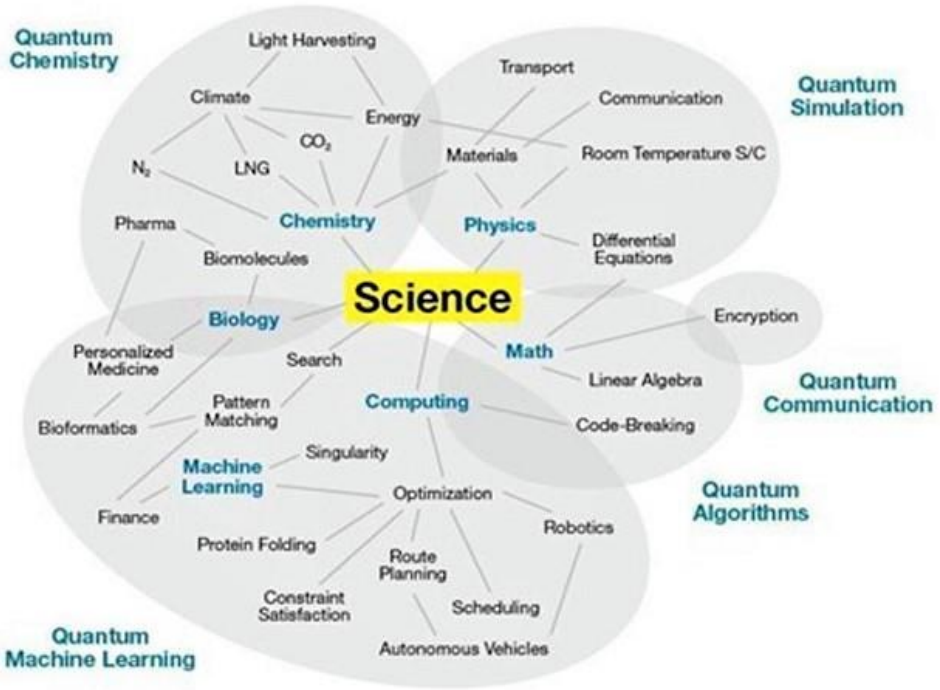

Рисунок 22 - Примеры использования квантовых вычислений

Источник: GARTNER

Перечисленные примеры лишь малая часть сфер применения квантовых технологий, поскольку в этой области есть еще десятки других заметных разработок. Еще предстоит проделать большой объем исследований и разработок прототипов. Многие эксперты по-прежнему считают, что квантовые вычисления все еще являются теоретическими, но некоторые говорят, что мы, похоже, приближаемся к трансформационным квантовым воротам, которые позволят нам войти в новую вычислительную эру.

Как отмечалось выше, несколько квантовых компьютеров в настоящее время запущены в эксплуатацию. Некоторые из них доступны пользователям для экспериментов через облачные сервисы, но они по-прежнему работают в экспериментальном режиме. Во-первых, в этих компьютерах есть сотни кубитов, тогда как для решения сложных задач необходимо несколько тысяч или даже миллионов кубитов. Другая проблема заключается в том, что кубиты сложно изготовить, и некоторые из кубитов не будут вести себя так, как ожидалось, что потребует от исследователей добавления дополнительных кубитов для квантовой коррекции ошибок. Для управления работой миллионов квантовых битов в настоящее время используется трехмерный

диэлектрический резонатор, который может вырабатывать магнитные поля из импульсов микроволнового излучения. Австралийские физики разработали новую систему контроля состояния кубитов, с помощью которой можно одновременно считывать и записывать данные в миллионы ячеек памяти квантового компьютера. Результаты исследования опубликовал научный журнал Science Advances.

К 2021 году полноценных квантовых компьютеров ученые пока не создали. Сейчас существуют только их прототипы – например, в 2017 году физик из Гарвардского университета Михаил Лукин рассказал о создании 51-кубитного прототипа, а компания Google в 2019-м году – о 53-кубитном прототипе под названием Sycamore, в начале декабря 2020 года китайские ученые создали фотонный квантовый компьютер "Цзю Чжан".

В ноябре 2021 года появилась информация о создании компанией IBM 127-кубитного квантового процессора Eagle (Орёл). Это третий квантовый процессор IBM. В 2019 году компания представила 27-кубитный Falcon ("Сокол"), а годом позже - 65-кубитный Hummingbird ("Колибри").

В настоящее время проводятся большие работы по превращению квантовых компьютеров из лабораторных прототипов в практичные, работающие устройства. Эта область исследований включает в себя исследования от того, как квантовый компьютер будет взаимодействовать с существующими технологиями, до того, какие типы программного обеспечения будут совместимы с квантовыми системами. В современных компьютерах программное обеспечение играет роль координации и преобразования битов в вычисления и результаты. То же самое и с квантовыми вычислениями - разрабатываются программы, называемые компиляторами, которые читают и переводят языки программирования высокого уровня до уровня кубитов компьютера. Кроме того, разрабатывается программное обеспечение, чтобы изучить, какие алгоритмы лучше всего работают с различными типами кубитов.

Ожидается, что квантовые компьютеры будут способны решать проблемы, которые в настоящее время нельзя решить, но они, скорее всего, не заменят классические компьютеры для решения повседневных задач. Экспертное сообщество едино в мнении, что квантовые компьютеры уже работают. Нет никаких сомнений в том, что в будущем круг решаемых ими задач будет только расширяться. Но следует

отметить, что в силу своих технических особенностей вряд ли в обозримом будущем квантовые компьютеры будут столь же универсальны, как и обычные компьютеры. Квантовые компьютеры будут использоваться в первую очередь для решения сложных задач – NP-задач (англ. non-deterministic polynomial – «недетерминированные с полиномиальным временем»), возникающих при исследовании Больших систем и для которых не существует эффективных алгоритмов решения.

Хотя до действительно мощных квантовых компьютеров с миллионами кубитов еще далеко, технологии для создания этого преимущества приближаются.

Отметим, что в экспертном сообществе нет единого мнения – может ли быть создан квантовый компьютер в 1 000 000 кубитов в следующие 50 лет. Квантовые компьютеры в настоящее время проходят стадию «завышенных ожиданий» жизненного цикла любой технической системы. Это во многом напоминает стадии развития технологии управляемого термоядерного синтеза, который сегодня находится на «плато осознания» - реально перспективная технология, но довести её до уровня промышленного производства чрезвычайно сложно.

Контрольные вопросы к разделу 4

1. В чём заключается основное отличие квантовых вычислений от обычных?
2. Какие принципы лежат в основе квантовых вычислений?
3. Что такое квантовая линия связи?
4. Какие направления работ по квантовым коммуникациям проводятся в России?
5. В каких видах экономической деятельности могут использоваться квантовые вычисления?
6. В чём заключаются потенциальные преимущества квантовых вычислений?
7. Для решения каких задач могут использоваться квантовые компьютеры?
8. Как квантовые вычисления могут использоваться в защищённых ЦОД?

Рекомендуемая литература

1. Докучаев В.А., Кальфа А.А., Маклачкова В.В. Архитектура центров обработки данных / Под ред. проф. В.А. Докучаева. - М.: «Горячая линия-телеком», 2020.
2. Докучаев В.А., Кальфа А.А., Мытенков С.С., Шведов А.В. Анализ технических решений по организации современных центров обработки данных / В.А. Докучаев, А.А. Кальфа, С.С. Мытенков, А.В. Шведов // T-Comm: Телекоммуникации и транспорт. – 2017. – Том 11. – № 6. – С. 16-24.
3. Докучаев В.А., Шведов А.В. Защита информации на корпоративных сетях VoIP // «Электросвязь». - 2012. - № 4. - С. 32-35.
4. Крупин А. «Made in Russia: обзор 20 российских операционных систем»: сайт. – URL: https://3dnews.ru/958857 (дата обращения: 02.07.2021). – Текст: электронный.
5. Горшков Сергей. Единая точка доступа к данным предприятия // Открытые системы. СУБД. — 2018. — № 4. — С. 33–35: сайт. - URL: http://www.osp.ru/os/2018/04/13054596 (дата обращения: 02.07.2021) - Текст: электронный.
6. Горшков С. Три шага к дата-центричной архитектуре: сайт. – URL: https://www.osp.ru/os/2019/04/13055224 (дата обращения: 02.07.2021) - Текст: электронный.
7. Dokuchaev V.A. "Digital Transformation: New Drivers and New Risks," 2020 International Conference on Engineering Management of Communication and Technology (EMCTECH), Vienna, Austria, 2020, pp. 1-7, doi: 10.1109/EMCTECH49634.2020.9261544.
8. Data-Centric Manifesto. URL: http://datacentricmanifesto.org/principles/ (дата обращения: 02.07.2021) - Текст: электронный.
9. Dave McComb. The Data-Centric Revolution: Restoring Sanity to Enterprise Information Systems. O'Reilly, 2019.
10. Определение квантовых вычислений - Глоссарий по информационным технологиям Gartner, URL: https://www.gartner.com/en/information-technology/glossary/quantum-computing (дата обращения: 21.11.2021) -Текст: электронный.
11. Discovery: Research at Princeton : Quantum computing открывает новые области возможностей - Discovery: Research at Princeton, URL: https://discovery.princeton.edu/2019/12/09/quantum-computing-opens-new-realms-of-possibilities/ (дата обращения: 21.11.2021) - Текст: электронный.

12. Quantum computing: Opening new realms of possibilities, URL: https://www.princeton.edu/news/2020/01/21/quantum-computing-opening-new-realms-possibilities (дата обращения: 21.11.2021) - Текст: электронный.
13. Argonne and UChicago scientists take important step in developing national quantum internet, URL: https://www.anl.gov/article/argonne-and-uchicago-scientists-take-important-step-in-developing-national-quantum-internet (дата обращения: 21.11.2021) - Текст: электронный.

Содержание

План УМД на 2021/22 уч.г.
С. 4, п. 15

Владимир Анатольевич Докучаев
Сергей Владимирович Запольских
Виктория Валентиновна Маклачкова
Вячеслав Михайлович Матросов
Андрей Вячеславович Шведов
Олег Владимирович Щербина

АРХИТЕКТУРА ЦИФРОВЫХ ПЛАТФОРМ ДЛЯ ЗАЩИЩЁННЫХ ЦОД

Часть 1

ОБЩИЕ ПОДХОДЫ И ИСПОЛЬЗУЕМЫЕ ТЕХНОЛОГИИ

Учебное пособие

Подписано в печать 14.12.2021г. Формат 60x90 1/16.
Объём 5,6 усл.п.л. Изд. № 66.