GM Smart System

Описание решения

Содержание

1. Общие сведения

Данный документ описывает решение компании «Гетмобит» для построения платформы унифицированного рабочего пространства в концепции Smart Workspace (далее Система) для сотрудников федеральных органов исполнительной власти, ФГУП, МУП, предприятий ОПК и других организаций. Документ описывает концепцию и архитектуру Системы, а также её основные функционально-технические характеристики, средства интеграции как внутри Системы, так и со смежными информационными системами и сервисами.

Ключевой задачей является построение гибкой и адаптивной коммуникационной среды, обеспечивающей удобство работы конечных пользователей в различных контурах информационного обмена, операционную эффективность и экономию на владении. А учитывая усиливающееся влияние санкционных рисков, применение отечественного оборудования и поэтапное сокращение доли зарубежных технических и программных средств должны стать приоритетной задачей в части оптимизации затрат и обеспечения непрерывной поддержки вне зависимости от политической ситуации.

2. Назначение и цели создания Системы на базе платформы GM Smart System

Платформа GM Smart System предназначена для обеспечения доступа к информационным системам заказчика – к ресурсам прикладных информационных систем с выполнением всех необходимых требований по обеспечению мер информационной безопасности и требований по защите информации, в том числе, в государственных информационных системах.

Целями выполнения работ по внедрению Системы являются:

1. снижение операционных издержек при эксплуатации рабочих мест сотрудников;
2. повышение уровня защищенности информации, обрабатываемой на автоматизированных рабочих местах сотрудников организации.

Задачи, решаемые при выполнении работ по внедрению Системы:

1. обеспечение централизованного управления рабочими местами сотрудников организации;

2. обеспечение безопасности информации, циркулирующей в информационных системах организации;
3. снижение рисков потери данных из-за сбоев в работе сотрудников;
4. унификация пользовательской рабочей среды (единообразие ОС, ПО и настроек на рабочих местах сотрудников);
5. упрощение процессов развертывания и настройки рабочих мест сотрудников организации.

3. Функции, реализуемые Системой

GM Smart System обеспечивает реализацию следующих функций:

- предоставление пользователям доступа к сервисам виртуальных рабочих столов (VDI) основных отечественных и зарубежных производителей;
- предоставление пользователям доступа к веб-сервисам;
- предоставление пользователям доступа к сервисам VoIP-телефонии с использованием протокола SIP;
- предоставление пользователям доступа к сервисам видео-конференц-связи с использованием протокола SIP или штатными средствами в виртуальной машине пользователя;
- предоставление возможности использования различных способов и средств защиты информации, в том числе и криптографических, от различных вендоров;
- предоставление администраторам системы возможности централизованного управления пользовательским оборудованием;
- предоставление администраторам системы возможности централизованного управления учётными данными и профилями пользователей;
- предоставление администраторам системы возможности централизованного мониторинга состояния пользовательского оборудования;
- предоставление администраторам системы возможности централизованного обновления системного программного обеспечения пользовательского оборудования;
- предоставление пользователям возможности поочерёдного использования одного экземпляра оборудования разными сотрудниками.

4. Применимость Системы на объектах автоматизации

Система GM Smart System может применяться для создания автоматизированных рабочих мест (АРМ) сотрудников федеральных органов исполнительной власти, ФГУП, МУП, предприятий ОПК и других организаций, в т.ч. коммерческих.

Оптимальное использование возможностей Системы достигается на объектах автоматизации, оснащённых (оснащаемых) средами VDI, IP (SIP) телефонией, развитыми веб-сервисами и СКЗИ для организации удалённого доступа к рабочей среде.

Созданные с применением Системы АРМ могут применяться:

- на объектах автоматизации с обеспечением доступа к информационным системам, в том числе и защищенным информационным системам, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну;
- на ОКИИ первой категории;
- в ГИС первого класса защищённости;
- в АСУ (ТП) первого класса защищённости;
- в ИСПДн первого уровня защищённости;
- в ИС общего пользования второго класса.

5. Описание Системы

5.1. Структура GM Smart System

GM Smart System (GMSS) – это единая доверенная платформа для построения и централизованного управления инфраструктурой рабочих пространств на базе док-станции GM-Box G1 (далее GM-Box) со встроенным программным обеспечением GM Soft Kit и собственного серверного программного обеспечения GM Management Suite (GMMS). Кроме того, в платформу GMSS могут входить: сервис Global Discovery Service (GDS), обеспечивающий автоматизированную инициализацию GM-Box для подключения к инфраструктуре заказчика, и мобильное приложение GM Mobile Assistant, предназначенное для обеспечения возможности использования смартфона как средства аутентификации.

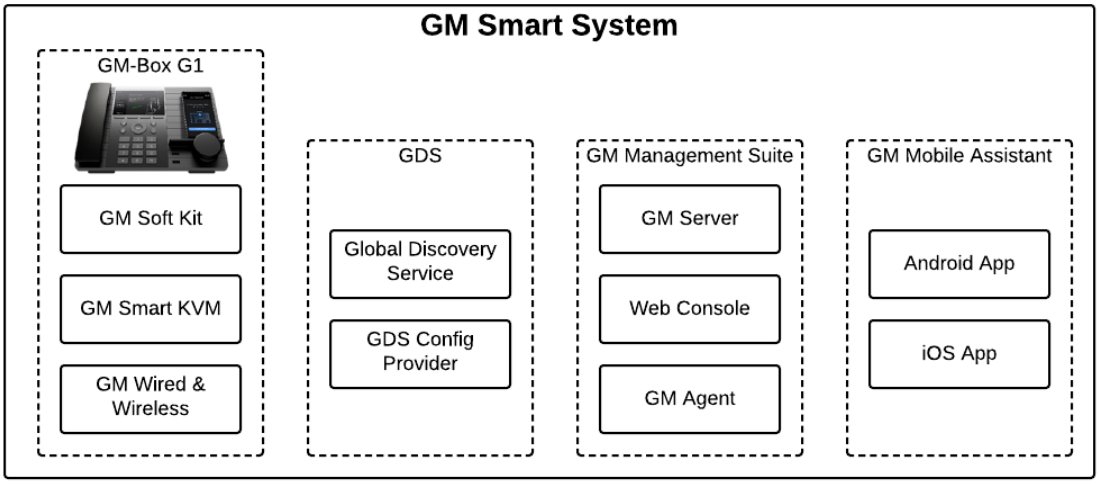

Рисунок 1 Компоненты платформы GM Smart System

Платформа GM Smart System позволяет обеспечить унифицированный доступ пользователей к корпоративным информационным ресурсам, в том числе в изолированных информационных контурах, и реализацию функций, перечисленных в разделе 4 настоящего документа.

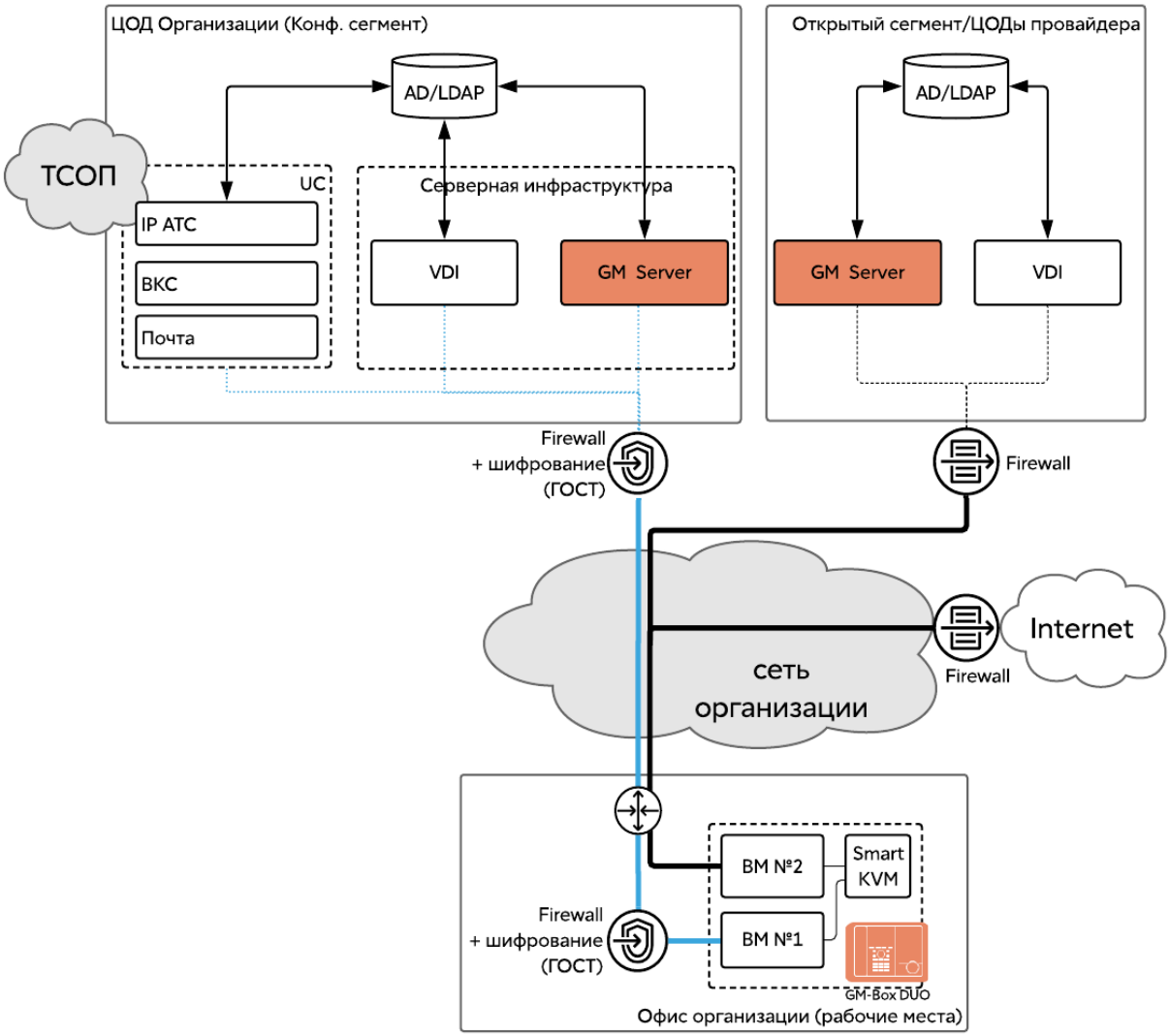

Рисунок 2 Структурная схема организации единой доверенной рабочей среды

Преимуществом платформы является интеграция и унификация доступа к инфраструктурным и пользовательским информационным системам и сервисам (ИСС) в едином, централизованно управляемом, пользовательском устройстве – док-станции GM-Box G1.

При внедрении GM Smart System на объекте автоматизации Заказчика, реализуются следующие возможности:

- а-персональность рабочего места;
- унификация рабочего места;
- сквозная интеграция рабочего места пользователя в ИСС заказчика;
- «следование» рабочего места за пользователем;
- повышение уровня информационной безопасности, в т.ч. благодаря возможности подключения одного устройства пользователя к изолированным сетевым сегментам («открытому» и «закрытому») информационной системы;
- упрощение миграции ИСС на новые аппаратно-программные решения (например, при замещении решений зарубежных производителей, решениями отечественных производителей).

5.2. Требования, необходимые для эксплуатации Системы

Для внедрения и эксплуатации Системы на объекте автоматизации должны быть выполнены следующие требования:

1. Настроены инфраструктурные сервисы DHCP, DNS, служба каталогов (MS Active Directory, LDAP), NTP согласно документации к Системе;
2. Запущена и настроена среда терминального доступа и/или VDI, совместимая с Системой;
3. Запущены и настроены веб-сервисы;
4. Запущена и настроена система унифицированных коммуникаций (IP телефония, видео-конференц-связь), совместимая с протоколом SIP;
5. Обеспечены необходимые, указанные в документации к Системе, вычислительные, сетевые и материально-технические ресурсы, определяемые в соответствии с конкретными архитектурно-техническими решениями;
6. Обеспечено межсетевое взаимодействие в соответствии с разделом 9 настоящего документа.

5.3. Описание компонентов GM Smart System

5.3.1. GM-Box

GM-Box – это универсальная док-станция, обеспечивающая доступ пользователя к информационным сервисам заказчика:

- VDI,
- терминальный доступ,
- веб-сервисы,
- IP телефония и видео-конференц-связь.

Устройство GM-Box состоит из корпуса, телефонной трубки, процессорного модуля, интерфейсов доступа к сетям связи (Ethernet, WiFi, GSM модем) и внешним периферийным устройствам, включая NFC-модуль и зарядное устройство.

Док-станция GM-Box доступна в 23 исполнениях, что позволяет обеспечить наиболее полное соответствие технико-экономическим требованиям заказчика.

В случае, когда на рабочем месте сотрудника необходимо организовать работу с изолированными сетевыми контурами, возможно применение двухконтурного исполнения док-станции - GM-Box DUO. Благодаря встроенному KVM переключателю, GM-Box DUO обеспечивает безопасную работу сотрудника с изолированными информационными сегментами с использованием одного комплекта периферийного оборудования. При этом основной монитор (подключаемый к выходу HDMI) переключается для использования между контурами встроенным KVM переключателем, а монитор, подключаемый к выходу Display Port фиксировано подключен к основному вычислительному модулю.

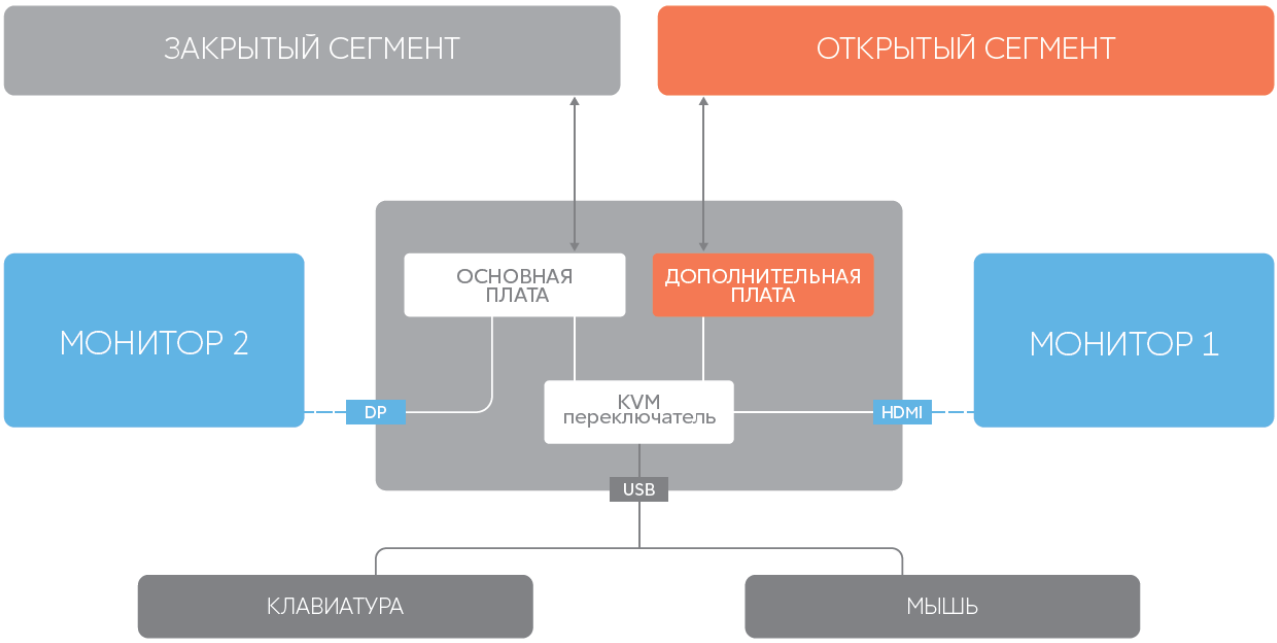

Рисунок 3 Схема подключений GM-Box G1 DUO

Для одноконтурного исполнения, подключение двух мониторов обеспечивает работу в режиме расширенного рабочего стола (при поддержке данного режима виртуальным рабочим столом пользователя).

GM-Box включает предустановленное встроенное системное ПО – GM Soft Kit: встроенную операционную систему собственной разработки (Linux-based ОС на основе Ubuntu 16.04 или сертифицированную ФСТЭК России ОС Альт 8 СП) и системное программное обеспечение для реализации основных функций док-станции.

Встроенное ПО поддерживает следующие VDI-клиенты:

- Citrix, протоколы: HDX, ICA;
- Microsoft, протоколы: RDP, RemoteFX;
- VMware, протоколы: PCoIP, Blast Extreme;
- Huawei, протокол: HDP;
- Тионикс, Скала-Р, протокол: RDP.
- Горизонт-ВС, протоколы: Spice, VNC

Дополнительно, по мере развития ПО Системы, в состав GM Soft Kit могут быть встроены дополнительные VDI-клиенты.

Встроенное ПО работает с АТС, совместимыми с SIP протоколом (RFC 3261), в частности: ПРОТЕЙ, ВАТС Ростелеком, ВАТС Манго, VideoMost, Communigate Pro, Cisco UCM, Avaya, Huawei, Asterisk, Siemens, Elastix, Eltex, Freeswitch и другими.

В GM Soft Kit встроены сертифицированные программные средства криптографической защиты информации: КриптоПро CSP, ViPNet Client 4U for Linux.

Подключение док-станции GM-Box к сетям передачи данных возможно посредством встроенных интерфейсов:

- Ethernet (доступно во всех исполнения),
- Wi-Fi (для отдельных исполнений),
- 3G/4G LTE (для отдельных исполнений, в перспективе с поддержкой 5G сетей).

В модификации GM-Box DUO реализовано физическое разграничение открытого и закрытого контура корпоративной сети путем использования двух независимых системных плат с возможностью переключения между ними одного комплекта устройств ввода/отображения информации (Keyboard-Video-Mouse) при помощи встроенного аппаратного KVM-переключателя.

GM-Box G1 обеспечивает следующие возможности:

- возможность одновременной работы в двух изолированных информационных контурах (для модификации DUO)
- возможность поочерёдного использования одного устройства разными сотрудниками;
- многовариативная идентификация и аутентификация;
- работу в сетевой среде Ethernet;
- работу в сети Wi-Fi (для исполнений с модулем Wi-Fi);
- подключение через сети 3G/4G LTE (для исполнений с модулем 3G/4G LTE);
- возможность вывода изображения на два монитора;
- поддержку протокола LDAP, включая Microsoft Active Directory;
- многовендорную поддержку сред VDI и терминального доступа без необходимости установки и конфигурирования отдельных клиентов;
- удалённое безопасное подключение к инфраструктуре заказчика с использованием программных СКЗИ VipNet Client 4U for Linux, КриптоПро CSP, а также OpenVPN.

5.3.2. GM Management Suite

Серверное программное обеспечение GM Management Suite обеспечивает интеграцию с инфраструктурой PKI, горизонтальное масштабирование, построение отказоустойчивых систем и решений высокой доступности и возможность интеграции с корпоративным сервисами, а также централизованное:

- управление учетными данными и профилями пользователей;
- управление клиентскими устройствами;
- контроль доступа к информационным ресурсам организации;
- обновление ПО док-станций GM-Box;

– мониторинг док-станций GM-Box,

Структура компонент, входящих в GM Management Suite приведена ниже.

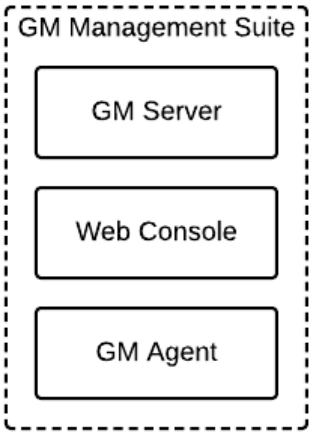

Рисунок 4 Компоненты GM Management Suite

GM Server – это сервер управления, устанавливаемый в инфраструктуре Заказчика. GM Server обеспечивает выполнение перечисленных выше функций GM Management Suite.

GM Agent – агент сервера управления, обеспечивает взаимодействие GM Server и GM-Box (GM Agent также входит в состав GM Soft Kit и предустановлен на каждом GM-Box).

Web Console – веб-консоль управления GM-Server.

Управление GM Management Suite осуществляется администраторами системы посредством веб-консоли. В GM Management Suite предусмотрено три уровня доступа:

1. суперадминистратор
2. администратор
3. администратор ИБ

Уровни доступа позволяют определить возможность администраторов с указанным типом учётной записи выполнять команды (назначать задания) на устройствах пользователей. Определение доступных администраторам и администраторам ИБ команд осуществляется суперадминистратором.

Администраторы GM Management Suite могут определять, к каким информационным системам организации пользователь GM-Box получит доступ. Список информационных систем и параметры подключения к ним задаются профилем пользователя. Профиль пользователя может быть как индивидуальным, так и формироваться на основании шаблона (см. рис. 5). С целью автоматизации управления профилями пользователей, отдельные поля

профилей могут заполняться автоматическими значениями, в т.ч. на основании шаблонов с привязкой к группе пользователя в службе каталогов.

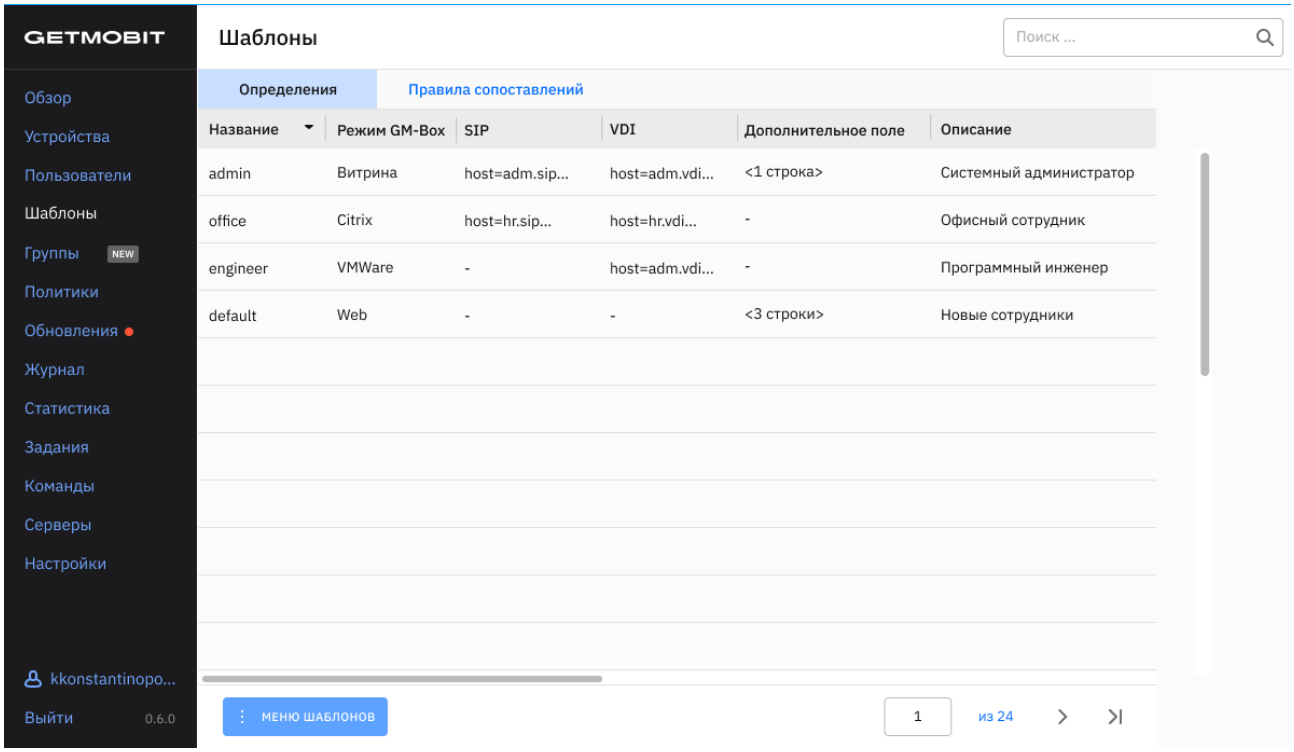

Рисунок 5 Шаблоны пользователей

5.3.3. Сервис Global Discovery Service

Global Discovery Service (GDS) обеспечивает автоматизированную инициализацию GM-Box для подключения к сети или облаку заказчика и реализуется с использованием следующих компонент:

1. Сервер Global Discovery Service
2. Провайдер конфигурации устройств (см. GDS Config Provider)
3. Сервер GM Server
4. Док-станция GM-Box

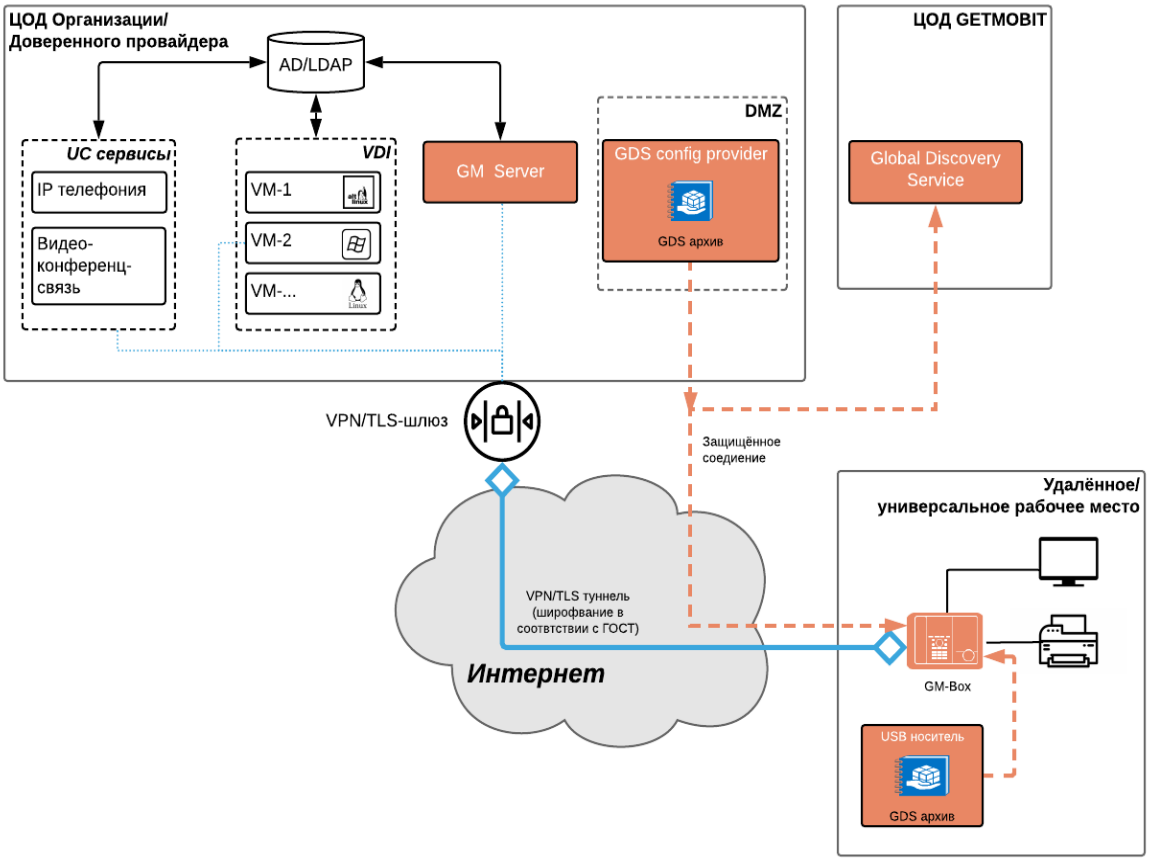

Рисунок 6 Компоненты сервиса Getmobit Discovery Service

Сервис Global Discovery Service существенно расширяет возможности платформы Getmobit Smart System, обеспечивая автоматизацию развёртывания GM-Box, разворачиваемых вне доверенного сетевого контура. Сервис GDS размещается в ЦОД Getmobit. Сервис хранит информацию по изготовленным и проданным устройствам, а также их связь с компаниями (организациями), которые приобрели устройства.

Сервис GDS выполняет следующие функции:

1. удостоверение идентичности GM-Box, обращающегося за базовой конфигурацией;
2. определение провайдера конфигураций, осуществляющего хранение конфигурации конкретного устройства;
3. установление безопасного соединения с Провайдером конфигурации устройств;
4. передачу запроса на поиск файла с настройками в Провайдер конфигурации устройств.

Провайдер конфигурации устройств (GDS Config Provider) – это репозиторий, содержащий:

1. архив с первичными настройками GM-Box (далее – GDS архив);
2. пароль на архив (опционально).

По умолчанию используется Провайдер конфигурации устройств, размещаемый в ЦОД Getmobit, но, в случае необходимости, предусмотрена возможность размещения Провайдера в ИТ инфраструктуре заказчика. GDS архив также может быть передан на GM-Box с использованием отчуждаемого USB носителя.

Выбор способа получения GDS архива определяется пользователем с использованием меню GM-Box.

GDS архив включает:

1. один или несколько конфигурационных файлов (сертификатов ViPNet) и Open-VPN;
2. сертификат для организации TLS соединения с GM Server.

На GDS архив может быть установлен пароль, который может быть передан сотруднику организации независимо от устройства (по другому каналу связи). Таким образом, обеспечивается дополнительный этап защиты.

5.3.4. Мобильное приложение GM Mobile Assistant

Основное назначение мобильного приложения GM Mobile Assistant – использование смартфона сотрудника как токена для идентификации/аутентификации пользователя. Для этой цели на смартфон пользователя устанавливается мобильное приложение GM Mobile Assistant. Приложение поддерживается ОС Android и iOS, доступно на Google Play и Apple Store.

Для начала рабочей сессии пользователю необходимо ввести 4 цифры, выведенные на монитор устройства, - это его идентификатор. Это требуется, так как рядом могут стоять несколько устройств GM-Box. Если смартфон оснащен NFC-модулем, вводить цифры не потребуется, нужно только положить аппарат на специальную площадку док-станции, и телефон сам считает идентификатор. После этого смартфон передаст по Bluetooth логин и пароль, записанный в криптоконтейнер смартфона. Док-станция отправляет запрос на сервер управления, оттуда приходит профиль пользователя со всей необходимой ему функциональностью и открывается рабочая сессия.

У мобильного приложения GM Mobile Assistant есть еще одна функция: обеспечение автоматического завершения рабочей сессии в случае ухода пользователя с рабочего места. Для этого используются специальные алгоритмы, которые позволяют GM-Box отслеживать приближение или удаление пользователя от рабочего места как по уровню сигнала Bluetooth, так и путем использования сенсоров движения телефона.

6. Функциональная архитектура и связи Системы

На рисунке 6 ниже представлена общая функциональная архитектура предлагаемого решения, включая связь между компонентами GM Smart System и смежными системами:

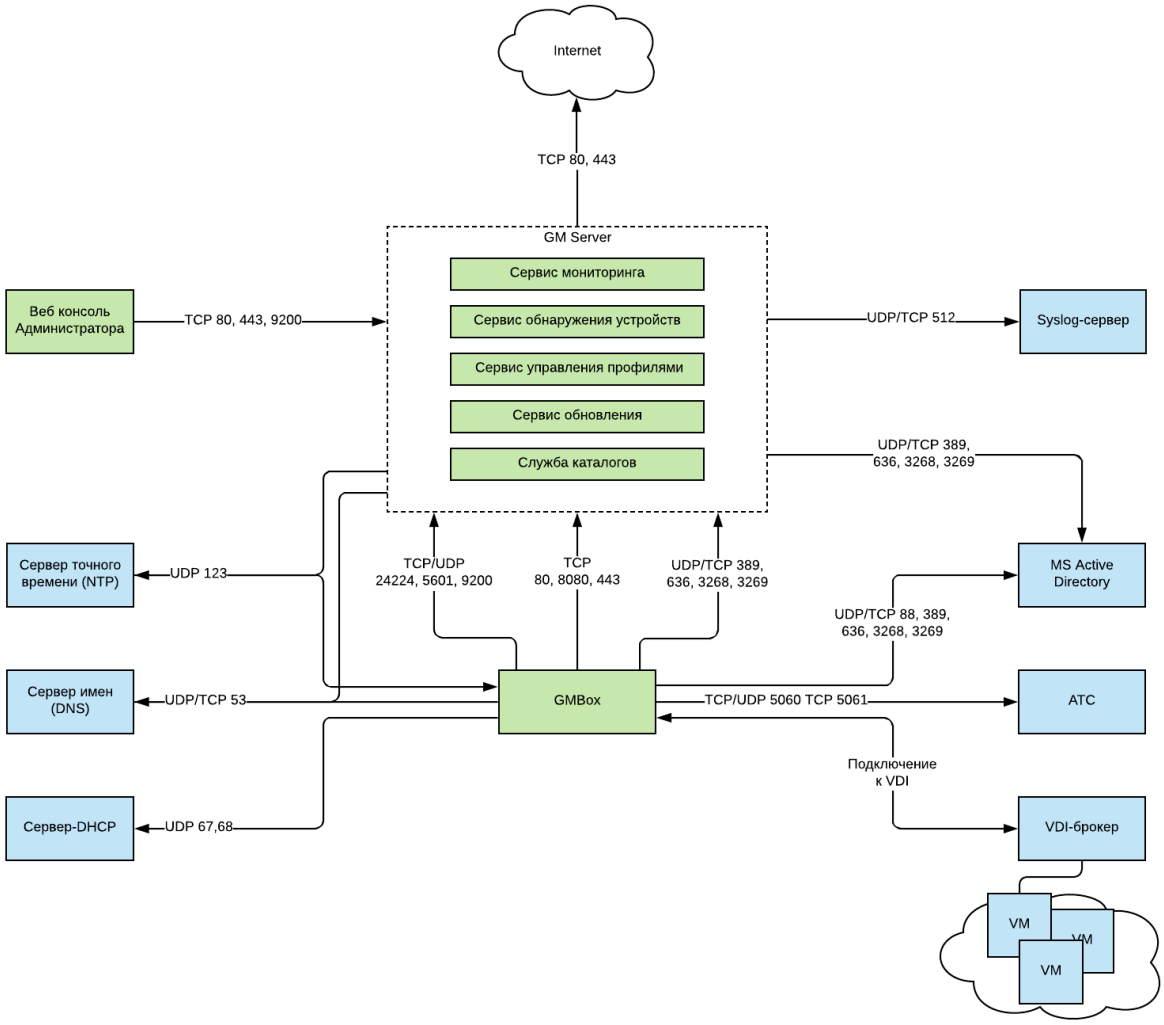

Рисунок 7 Структурная схема

Комплексное решение, формирующее автоматизированную (информационную) систему, можно условно разбить на следующие подсистемы:

1. Подсистема унифицированного рабочего места;
2. Подсистема управления идентификацией и аутентификацией;
3. Подсистема управления инфраструктурой;
4. Подсистема унифицированных коммуникаций (IP телефония и видео-конференц-связь);
5. Подсистема виртуализации;
6. Подсистема информационной безопасности.

Взаимодействие между подсистемами осуществляется посредством на прикладном уровне сети в стеке протоколов TCP/IP.

6.1. Подсистема унифицированного рабочего места сотрудника

Подсистема состоит из устройства (док-станции) GM-Box G1, устанавливаемого на рабочем столе сотрудника. В результате подключения к устройству GM-Box монитора, клавиатуры и мыши, принтера и сканирующего устройства (при необходимости), а также подключения его к сети Заказчика, сотрудник получает готовое к использованию рабочее место.

Режимы работы пользователя определяются профилем настроек. Профиль настроек задаётся администратором Системы на GM Server. При входе пользователя в сессию (после успешной авторизации), GM-Box получает от сервера управления GM Server профиль пользователя и запускает один из доступных, определённых администратором режимов:

1. Гостевой режим – используется для обеспечения возможности использования GM-Box в качестве IP телефона без входа в рабочую сессию пользователя. В текущей реализации, данный режим обеспечивает возможность использования запускаемого локально браузера (с элементами управления или в режиме «Киоск») и обезличенный номер телефона;
2. Веб-режим – пользователю доступен запускаемый локально браузер (с элементами управления или в режиме «Киоск», с индивидуальными или общими настройками) и индивидуальный номер телефона;
3. Терминальный режим – пользователю доступно подключение к определяемой администратором среде виртуальных рабочих столов (терминальному серверу) или выделенному терминальному серверу (в т.ч. и ПК) с использованием протоколов доступа к удалённым рабочим столам и индивидуальный номер телефона.
4. Режим «Витрина», предоставляющий авторизованному пользователю возможность выбора доступного ему VDI или web-подключения в рамках одной сессии (см. Рис. 7). Доступные пользователю подключения задаются администратором системы путем создания шаблонов настроек пользователей.

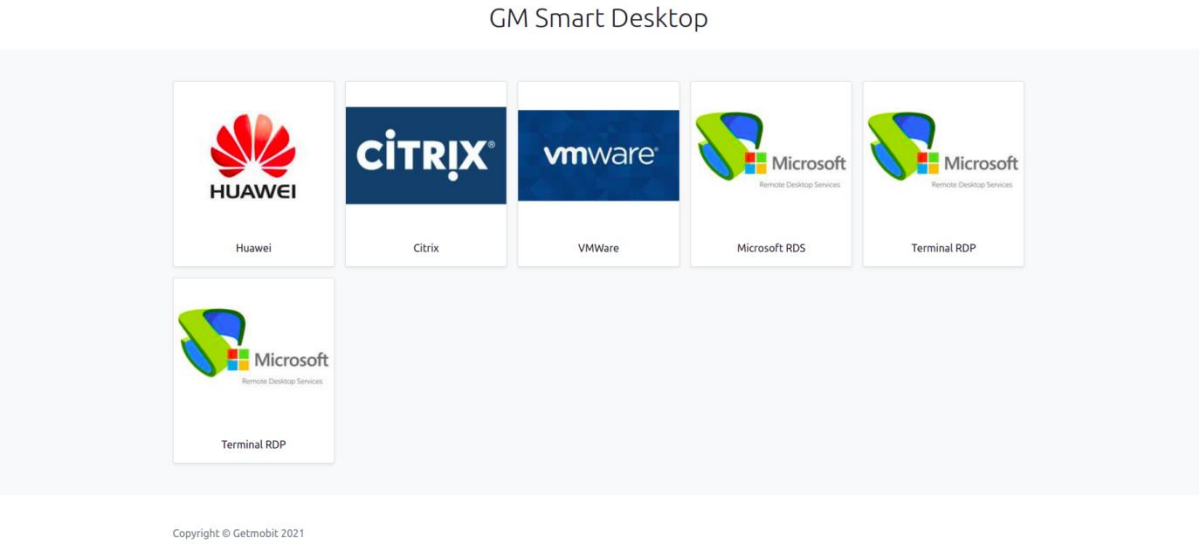

Рис.8 Вид экрана – «витрины»

6.2. Подсистема управления идентификацией и аутентификацией

Подсистема предназначена для управления механизмами идентификации и аутентификации пользователей на устройствах GM-Box и в VDI среде организации, а также администраторов GM Management Suite в веб-консоли. В состав подсистемы входит компонент сервера управления GM-Server (модуль поддержки аутентификации), предназначенный для настройки механизмов аутентификации пользователей и интеграции с корпоративным доменом организации (например, с MS AD или другим LDAP каталогом).

Для начала рабочей сессии, пользователь аутентифицируется на GM-Box доступным ему способом (ввод пары логин-пароль, с использованием токена, бесконтактной карты или смартфона). GM-Box передаёт аутентификационные данные пользователя на сервер управления, который, в свою очередь, передаёт их в службу каталогов для процесса аутентификации. Для аутентификации в службе каталогов используется механизм SASL. В случае успешной аутентификации, служба каталогов возвращает токен, используемый GM-Box для подключения к целевой среде.

6.3. Подсистема управления инфраструктурой

Подсистема предназначена для централизованного управления рабочими местами сотрудников организации и средствами защиты информации. В состав подсистемы входят следующие компоненты:

- компонент сервера управления GM-Server, предназначенный для управления рабочими местами сотрудников организации (устройствами GM-Box);
- компоненты управления подсистемой обеспечения безопасности информации третьих производителей, предназначенные для централизованной настройки и управления средствами защиты информации, устанавливаемыми в гостевых ОС внутри виртуальных машин и не только (например, аутентификация администраторов виртуальной инфраструктуры и разграничение доступа к средствам управления виртуальной инфраструктурой, контроль целостности конфигурации виртуальных машин и доверенная загрузка ОС).

6.4. Подсистема видео и голосовой связи

Подсистема предназначена для организации видео конференций и голосовой связи пользователей GM-Box между собой и с внешними абонентами. В состав подсистемы входят следующие компоненты:

- компонента сервера ВКС и IP-телефонии, предназначенная для обеспечения видеоконференцсвязи и маршрутизации звонков между абонентами;
- клиент ВКС и IP-телефонии, встроенный в GM-Box и предназначенный для обеспечения голосовой связи пользователей GM-Box между собой и внешними абонентами.

Встроенное ПО GM-Box обеспечивает совместную работу с АТС, совместимыми с SIP протоколом (RFC 3261), в частности: ПРОТЕЙ, ВАТС Ростелеком, ВАТС Манго, VideoMost, Cisco UCM, Avaya, Communigate Pro, Huawei, Asterisk, Siemens, Elastix, Eltex, Freeswitch.

Предоставляемые пользователю GM-Box сервисы видео и голосовой связи определяются возможностями соответствующих инфраструктурных компонент и могут включать:

1. голосовые и видеовызовы «точка-точка»;
2. постановку вызова на удержание, перевод вызова;
3. аудиоконференции на базе аппаратных ресурсов GM-Box до 10 участников;

4. видеоконференции на базе стороннего сервера ВКС, размещённого в инфраструктуре организации;
5. хранение журнала принятых, пропущенных во время рабочей сессии и сделанных пользователем GM-Box вызовов;
6. доступ к адресной книге предприятия;
7. индикацию занятости абонента;
8. возможность автоматической переадресации звонка на мобильный номер сотрудника при его отсутствии на рабочем месте (при поддержке такой возможности АТС организации).

6.5. Подсистема виртуализации

Подсистема предназначена для оптимизации аппаратных ресурсов организации путем развертывания и управления множеством виртуальных машин на ограниченном количестве физических серверов. В состав входят следующие компоненты:

- ПО гипервизора, предназначенное для управления виртуальными машинами;
- Шлюз клиентских подключений, предназначенный для обеспечения подключения рабочих мест сотрудников организации к виртуальным машинам VDI среды организации.

Платформа GM Smart System поддерживает большинство присутствующих на рынке сред VDI, в том числе:

- Citrix, протоколы: HDX, ICA;
- Microsoft, протоколы: RDP, RemoteFX;
- VMware, протоколы: PCoIP, Blast Extreme;
- Huawei, протокол: HDP;
- Тионикс, Скала-Р, протокол: RDP;
- Горизонт-ВС, протоколы: Spice, VNC.

Дополнительно, по мере развития ПО Системы, в состав GM Soft Kit могут быть встроены дополнительные VDI-клиенты.

6.6. Подсистема информационной безопасности

Подсистема предназначена для идентификации и проверки подлинности пользователей, неизменности компонентов общесистемного ПО и средств защиты информации, антивирусной защиты информации и контроля доступа к внешним (съемным)

носителям информации и периферийным устройствам, а также регистрации событий информационной безопасности (далее – ИБ) при работе пользователей в VDI среде организации. Подсистема использует как компоненты третьих производителей с учётом нормативных требований, так и возможности платформы GM Smart System.

В состав подсистемы входят следующие компоненты:

а) Средства от несанкционированного доступа к информации;
б) Средства, предназначенные для обеспечения контроля целостности общесистемного программного обеспечения виртуальных машин;
в) Средства антивирусной защиты виртуальных машин;
г) Встроенные в GM-Box механизмы защиты информации, предназначенные для обеспечения контроля целостности общесистемного ПО GM-Box.

7. Общий план внедрения Системы

Типовой план внедрения Системы:

Исходное состояние

В инфраструктуре заказчика развёрнуты или запланированы к развёртыванию сервисы VDI, IP телефонии, ВКС, а также сопутствующие инфраструктурные сервисы (см. раздел 4).

Этап №1. Планирование и сбор исходных данных

Результат выполнения этапа №1: осуществлён сбор исходных данных с учётом «Требований к инфраструктуре» для GM Smart System, необходимых для проведения работ по интеграции. Запланированы работы по донастройке сетевой инфраструктуры и смежных информационных систем в соответствии с «Требованиями к инфраструктуре»

Этап №2. Развёртывание сервера управления GM Server

Результат выполнения этапа №2: в сети Заказчика развёрнут сервер управления GM Server.

Этап №3. Интеграция GM Smart System с инфраструктурой Заказчика

Результат выполнения этапа №3: GM Server настроен для интеграции Системы с инфраструктурой Заказчика: проверен доступ к VDI среде, IP телефонии, ВКС.

Этап №4. Ввод GM Smart System в эксплуатацию

Результат выполнения этапа №4: рабочее место сотрудника с использованием GM-Box установлено и настроено. Работают различные виды аутентификаций (токен и смартфон) в сети Заказчика, проводятся телефонные звонки и видео конференции по VoIP, работает беспроводная зарядка смартфона, есть подключение к периферийному оборудованию (монитор, клавиатура, мышь, принтер, сканер, факс).

8. Приложение 1. Основные технические характеристики док-станции GM-Box

(модификации BASE и DUO)

Таблица 1 – Основные технические характеристики исполнений модификации BASE

Характеристика	**Исполнения GM-Box G1 модификации Base**									
	B1	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**B8**	**B9**	**B10**
Количество вычислительных модулей	1									
KVM-переключатель	Нет									
Процессор	Intel® Celeron® N3450									
Оперативная память	4 ГБ									
Энергонезависимая память	16 ГБ									
Графические интерфейсы и максимальное разрешение	HDMI 1.4b (1920x1080), DisplayPort 1.2 (1920x1080)									
Стандартные USB-порты	USB 2.0 (500 мА) – 5 шт. USB 3.0 (900 мА) – 3 шт.									
USB-порты для подключения смартфона	Micro-USB Type B – 2 шт. USB Type C – 1 шт.									
Звуковые устройства	Аудиотрубка со встроенным динамиком и микрофоном. Встроенные в корпус стереодинамики и микрофон с шумоподавлением. Разъем 3,5 мм для подключения аудиогарнитуры с поддержкой микрофонного входа, кнопок регулировки громкости и приема/завершения вызова.									
Веб-камера	Встроенная, цветная, максимальное разрешение - 1280x720 пикселей									
Встроенный графический дисплей	Цветной, 1280x720 пикселей, 110x62 мм, Класс по ISO 13406-2 – II									
Клавиатура	Встроенная, 21 функциональная клавиша, 4 контекстные клавиши									
Сетевой интерфейс	LAN 10/100/1000 Мбит/с									
Программное обеспечение	Встроенное									

Характеристика	Исполнения GM-Box G1 модификации Base									
	B1	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**B8**	**B9**	**B10**
Модуль Wi-Fi 802.11 n/ac 2,4 и 5 ГГц / Bluetooth 4.2 (BLE)			•	•	•		•	•	•	•
RFI 13,56 МГц			•	•	•	•	•	•	•	•
RFID 125 кГц						•	•	•	•	•
Встроенный 3G/LTE-модем				•				•		•
АПМДЗ		•			•				•	•
Модуль беспроводной зарядки для смартфона Qi 1.2			•	•	•	•	•	•	•	•
Охлаждение	Активное воздушное									
Слот для замка Kensington lock	Есть									
Электропитание	Адаптер питания: внешний Параметры напряжения сети: от 90 до 264 В, частотой 50 Гц Выходное напряжение: от 11,4 до 12,6 В Номинальная потребляемая мощность: не более 25 Вт Максимальная потребляемая мощность: не более 40 Вт Тип батареи питания встроенных часов: CR2032									
Габаритные размеры	При разложенной опоре: Ширина: 280 мм, Высота: 175 мм, Глубина: 170 мм В сложенном состоянии: Ширина: 280 мм, Высота: 175 мм, Глубина: 70 мм									
Вес НЕТТО	Не более 2 кг									

Таблица 2 – Основные технические характеристики исполнений модификации DUO

Характеристика	**Исполнения GM-Box G1 модификации DUO**												
	D1	**D2**	**D3**	**D4**	**D5**	**D6**	**D7**	**D8**	**D9**	**D10**	**D11**	**D12**	**D13**
Количество вычислительных модулей	2 (основной и дополнительный)												
KVM-переключатель	Встроенный												
Процессор	Основной ВМ: Intel® Celeron® N3450; Дополнительный ВМ: Intel® Celeron® N3350 / Intel® Celeron® N3450												
Оперативная память	Основной ВМ: 4 ГБ; Дополнительный ВМ: 4 ГБ												
Энергонезависимая память	Основной ВМ: 32 ГБ; Дополнительный ВМ:32 ГБ												
Графические интерфейсы и максимальное разрешение	Основной ВМ: DisplayPort 1.2, 1920x1080; Совмещенный через KVM: HDMI 1.4b, 1920x1080												
Стандартные USB-порты	Основной ВМ: USB 2.0 (500 мА) – 2 шт., USB 3.0 (900 мА) – 2 шт. Дополнительный ВМ: USB 3.0 (900 мА) – 2 шт.; Совмещенный через KVM: USB 2.0 (500 мА) – 2 шт.												
USB-порты для подключения смартфона	Основной ВМ: Micro-USB Type B – 2 шт. USB Type C – 1 шт.												
Звуковые устройства	Основной ВМ: аудиотрубка со встроенным динамиком и микрофоном, встроенные в корпус изделия стереодинамики и микрофон с шумоподавлением; Совмещенный через KVM: разъем 3,5 мм для подключения аудиогарнитуры с поддержкой микрофонного входа, кнопок регулировки громкости и приема/завершения вызова												
Веб-камера	Основной ВМ: встроенная, цветная, максимальное разрешение - 1280x720 пикселей												
Встроенный графический дисплей	Основной ВМ: цветной, 1280x720 пикселей, 110x62 мм, Класс по ISO 13406-2 – II												
Клавиатура	Встроенная, 21 функциональная клавиша, 4 контекстные клавиши												
Сетевые интерфейсы	Основной ВМ: LAN 10/100/1000 Мбит/с; Дополнительный ВМ: LAN 10/100/1000 Мбит/с												
Программное обеспечение	Встроенное												
Охлаждение	Активное воздушное												
Слот для замка Kensington lock	Есть												

Характеристика	Исполнения GM-Box G1 модификации DUO												
	D1	**D2**	**D3**	**D4**	**D5**	**D6**	**D7**	**D8**	**D9**	**D10**	**D11**	**D12**	**D13**
Модуль Wi-Fi 802.11 n/ac 2,4 и 5 ГГц на основном ВМ / Bluetooth 4.2 (BLE) на основном ВМ				•	•	•	•	•	•	•	•	•	•
RFI 13,56 МГц на основном ВМ				•	•	•	•	•	•	•	•	•	•
RFID 125 кГц на основном ВМ								•	•	•	•	•	•
Встроенный 3G/LTE-модем на основном ВМ				•							•	•	•
АПМДЗ на основном ВМ		•			•			•				•	•
АПМДЗ на дополнительном ВМ			•			•			•				•
Модуль беспроводной зарядки для смартфона Qi 1.2				•	•	•	•	•	•	•	•	•	•
Электропитание	Адаптер питания: внешний Параметры напряжения сети: от 90 до 264 В, частотой 50 Гц Выходное напряжение: от 11,4 до 12,6 В Номинальная потребляемая мощность: не более 25 Вт Максимальная потребляемая мощность: не более 40 Вт Тип батареи питания встроенных часов: CR2032 - одна												
Габаритные размеры	При разложенной опоре: Ширина: 280 мм, Высота: 175 мм, Глубина: 170 мм В сложенном состоянии: Ширина: 280 мм, Высота: 175 мм, Глубина: 70 мм												
Вес НЕТТО	Не более 2 кг												

9. Приложение 2. Правила сетевого взаимодействия

Протокол (TCP,UDP,IP)	Источник		Приемник		Описание правила
	IP-адрес	Порт	IP-адрес	Порт	
HTTP (TCP)	--	*	GM-Server	80, 8080	Доступ в веб консоль администрирования
HTTPS (TCP)	--	*	GM-Server	443	Доступ в веб консоль администрирования
LDAP (TCP, UDP)	GM-Server	*	Корпоративная служба каталогов	389	Синхронизация пользователей из корпоративной службы каталогов (read only account)
LDAPS (TCP, UDP)	GM-Server	*	Корпоративная служба каталогов	636	Синхронизация пользователей из корпоративной службы каталогов (read only account)
SYSLOG (TCP, UDP)	GM-Server	*	SYSLOG	514	SIEM, синхронизация логов с внешними системами заказчика (опционально)
NTP (UDP)	GM-Server	*	NTP	123	Синхронизация времени
Websocket (TCP)	GM-Box	*	GM-Server	80, 8080	Постоянное соединение GM-Box → GM-Server
(TCP, UDP)	GM-Box	*	GM-Server	24224, 5601, 9200	Мониторинг
LDAP (TCP, UDP)	GM-Box	*	GM-Server	389	Соединение с LDAP
LDAPS (TCP, UDP)	GM-Box	*	GM-Server	636	Соединение с LDAP
Kerberos LDAP (TCP, UDP)	GM-Box	*	Корпоративная служба каталогов	88, 389	SSO Citrix Domain Pass-thought Authentication Синхронизация корпоративной адресной книги (read

Протокол (TCP,UDP,IP)	Источник		Приемник		Описание правила
	IP-адрес	Порт	IP-адрес	Порт	
					only account)
LDAPS (TCP, UDP)	GM-Box	*	Корпоративная служба каталогов	636	Синхронизация корпоративной адресной книги (read only account)
HTTP (TCP, UDP)	GM-Box	*	Web servers/services	80	Корпоративные веб-приложения
HTTPS (TCP, UDP)	GM-Box	*	Web servers/services	443	Корпоративные веб-приложения
TLS (TCP)	GM-Box	*	TLS gateway	443	Transport Layer Security — Протокол защиты транспортного уровня для удаленного подключения
DNS (TCP, UDP)	GM-Box	*	DNS Server	53	DNS name resolution
DHCP (TCP, UDP)	GM-Box	*	DHCP Server	67, 68	Динамическое получение IP-адреса
NTP (UDP)	GM-Box	*	NTP	123	Синхронизация времени
SIP (UDP)	GM-Box	5060	SIP gateway/agent	5060	Сигнальный протокол VoIP
RTP (UDP)	GM-Box	*	SIP agent	16384–32767	Медиатрафик VoIP
TLS SIP (TCP)	GM-Box	5061	SIP gateway	5061	Сигнальный протокол VoIP защищённый TLS
RDP (TCP, UDP)	GM-Box	*	RDS server	3389	Remote Desktop Protocol — протокол удалённого рабочего стола
MMR (TCP)	GM-Box	*	View Agent/Horizon Agent	9427	Windows Media MMR VMware

Протокол (TCP,UDP,IP)	Источник		Приемник		Описание правила
	IP-адрес	Порт	IP-адрес	Порт	
USB Redirect (TCP)	GM-Box	*	View Agent/Horizon Agent	32111	USB redirection VMware
PCoIP (TCP, UDP)	GM-Box	*	View Agent/Horizon Agent	4172	PC-over-IP - Personal Computer over Internet Protocol
BLAST (TCP, UDP)	GM-Box	*	View Agent/Horizon Agent	8443, 22443	Blast – протокол VDI VMware
ICA/HDX (TCP, UDP)	GM-Box	2598, 1494	XenDesktop/XenApp VDA	2598, 1494	ICA/HDX Citrix protocol
SSH (TCP)	--	*	GM-Box, GM-Server	22	Настройка и отладки устройства и сервера
ICMP	--	*	--	--	Отправка и прием диагностических пакетов ICMP следующих типов: ECHO_REQUEST, ECHO_REP

10. Приложение 3. Обеспечение защиты информации

1) Общие сведения

Обеспечение мер безопасности информации при использовании клиентских устройств осуществляется с использованием следующих мер.

1. Наличием механизмов контроля целостности системного ПО.
2. Невозможностью загрузки стороннего ПО на устройство или загрузки с использованием съёмных носителей информации.
3. Наличием механизма идентификации и аутентификации пользователей.
4. Подключение устройства к серверу управления осуществляется по протоколу HTTPS, все соединения с сервером управления недоступны в открытом виде, зашифрованы с помощью TLS.
5. Устройство поддерживает возможность соединения с VDI-брокерами по протоколу HTTPS (для сред виртуализации, реализующих указанный механизм).
6. Устройство поддерживает возможность передачи голосового трафика в отдельном VLAN.
7. Централизованное управление профилями пользователей, в том числе правами доступа.
8. Управление доступностью USB-портов для пользователя на устройстве через централизованную систему управления.
9. Управление отключением/включением беспроводных интерфейсов (Wi-Fi / Bluetooth) через централизованную систему управления.
10. Блокирование локальных изменений сетевых настроек на устройстве через централизованную систему управления.
11. Наличие нескольких ролей (администратор, администратор безопасности, супер-администратор), обеспечивающих разграничения прав доступа к серверу управления, с возможностью настройки политик политики разграничения.
12. Возможность управления перезагрузкой, выключением устройств, принудительным завершением сессии пользователя.
13. Поддержка создания электронной подписи документов в корпоративных информационных системах
14. Возможность просмотра на сервере управления журнала событий с устройства (в том числе системного журнала syslog).

15. Возможность экспорта логов в сторонние SIEM системы по протоколу syslog (возможность определения формата).

Технические меры по защите информации могут быть обеспечены наложенными средствами: например, туннелированием трафика между клиентским устройством и вычислительной инфраструктурой, а также средствами защиты среды виртуализации, в частности:

а) идентификации/аутентификации пользователей (реализуются средствами службы каталогов и гипервизора и виртуальной машины);

б) сегментации, фильтрации и анализа трафика средствами межсетевых экранов, эксплуатируемых в инфраструктуре заказчика;

в) сбора, записи, хранения и просмотра событий безопасности средствами гипервизора.

Примечание: события безопасности могут быть использованы каталогизаторами событий для последующего анализа;

г) резервного копирования данных, резервирования технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры средствами гипервизора.

2) Защита информации в информационной системе заказчика

Док-станция GM-Box, используемая в качестве АРМ пользователя ИС по технологии «клиент-сервер», является средством доступа пользователя к информационным ресурсам и выполняет функции ввода и отображения информации. Док-станция не участвует в обработке информации, информация сессии после ее завершения в док-станции не сохраняется.

В зависимости от архитектуры построения информационной системы, заказчик (разработчик) определяет входят ли технические средства АРМ пользователя в состав защищенной информационной системы. Необходимо отметить, что технические средства АРМ пользователя защищенной ИС могут как входить в её состав, так и не входить. В случае включения технических средств АРМ пользователя в состав защищенной информационной системы, указанные АРМ должны быть оснащены средствами защиты информации, прошедшими оценку соответствия предъявляемым требованиям по безопасности информации.

Док-станция GM-Box может устанавливаться в выделенные помещения (ВП) различных категорий.

3) Средства и методы защиты информации в GMSS

Непосредственно в GMSS предусмотрены следующие средства и методы защиты информации.

1. Собственные (встроенные) средства защиты информации док-станции GM-Box (в привязке к группам требований ФСТЭК России к мерам защиты информации):
   1.1. Доверенный BIOS с парольной защитой от изменения (группы мер: ИАФ – идентификация и аутентификация пользователей, УПД – управление доступом, ОЦЛ – обеспечение целостности ИС (далее будут указываться только условные наименования группы мер))
   1.2. Встроенное ПО GM SOFT KIT, размещаемое на микросхеме памяти в режиме «только для чтения». Пользователь не имеет возможности локально перезаписать встроенное ПО или установить стороннее ПО. (ОЦЛ, УПД, ОПС – ограничение программной среды)
   1.3. Контроль целостности ПО GM SOFT KIT путем проверки электронной подписи встроенного ПО GM SOFT KIT на базе PKI-инфраструктуры ООО «ГЕТМОБИТ» (ОЦЛ)
   1.4. Встроенная ОС на базе Linux Ubuntu 16.04 совместно с Сервером управления (ПО GM MANAGEMENT SUITE, включающая сервис мониторинга):
      1.4.1. Многовариативная идентификация (логин, USB-токен, бесконтактная карта, смартфон) и аутентификация (пароль) (ИАФ)
      1.4.2. управление доступом, в том числе доступом пользователя к внешним устройствам (USB-носителям, локальным принтерам) (УПД);
      1.4.3. логирование и мониторинг основных данных функционирования системы (аудит безопасности) (АУД)
   1.5. Централизованная система доверенного обновления ПО GM SOFT KIT, ПО GM MANAGEMENT SUITE, ПО GM MOBILE ASSISTANT
   1.6. Сертифицированное средство защиты информации ПАК «GM SMART KVM» (KBM-переключатель в составе GM-Box DUO) с функцией контроля целостности собственного ПО (УПД, ОЦЛ)
2. **Наложенные (встраиваемые) средства защиты информации других вендоров:**
   2.1. Средство доверенной загрузки ПАК «Соболь»
   2.2. Средства криптографической защиты информации (СКЗИ) для построения защищенных туннелей, в том числе с применение алгоритмов согласно ГОСТ:

КриптоПро CSP (компонента stunnel), VipNet Client 4U for Linux. Данные программные СКЗИ встроены в ПО GM Soft Kit.

2.3. Обеспечение возможности создания пользователем электронной подписи документа в основной информационной системе. С этой целью обеспечивается возможность «проброса» информации закрытого ключа электронной подписи пользователя по защищенному каналу в основную информационную систему.

3. Спецпроверка и специсследования док-станции GM-Box

Для подтверждения оценки возможности использования док-станции GM-Box в выделенных помещениях как объекта ВТСС проводятся спецпровека и специсследования поставляемой партии GM-Box. Заключения по результатам спецпроверки и специсследований, имеющие гриф секретности, направляются в режимно-секретное подразделение организации-заказчика.

4. В случае включения технических средств АРМ пользователя в состав защищенной информационной системы, указанные АРМ должны быть оснащены средствами защиты информации, прошедшими сертификацию на соответствие предъявляемым требованиям по безопасности информации.

4.1. Сертифицированное средство доверенной загрузки ПАК «Соболь» вер.4.

В средстве реализованы следующие функции безопасности:

- защита от несанкционированной загрузки операционной системы со съемных носителей информации;
- контроль целостности (КЦ) программного обеспечения GM-Box;
- идентификация и аутентификация пользователей при их входе в систему с помощью персональных идентификаторов.

ПАК «Соболь» вер.4 имеет сертификат соответствия ФСТЭК России № 4043, действителен до 05.12.2023.

4.2. Сертифицированная операционная система Альт 8 СП.

ОС Альт 8 СП является операционной системой общего назначения, сертифицированной ФСТЭК России (сертификат № 3866, действителен до 10.08.2023) как средство защиты информации 4 класса защиты на соответствие требованиям к операционным системам, профилю защиты ОС ИТ.ОС.А4.ПЗ, Требованиям доверия по

4 уровню доверия, и может быть использована в государственных информационных системах до 1 класса защищенности включительно и аналогичным им.

Примечание: ООО «ГЕТМОБИТ» в настоящий момент проводит работы по портированию ОС Альт 8 СП на средства платформы GM Smart System.

4.3. ПАК «GM SMART KVM»

Средство защиты информации «Программно-аппаратный комплекс «GM SMART KVM» (ПАК «GM SMART KVM») является программно-аппаратным средством управления однонаправленной передачи информации, устанавливаемым в двухплатную модификацию док-станции GM-Box DUO, и представляет собой KBM-переключатель, обеспечивающий организацию с одного устройства раздельного физически независимого доступа к разным информационным контурам, а также использование одного комплекта устройств ввода/отображения информации (монитор, клавиатура, манипулятор «мышь», аудио-гарнитура) для работы с двумя независимыми системными платами.

В ПАК «GM SMART KVM» реализованы:

– функция управления однонаправленной передачи данных (мера защиты УПД.3 – согласно приказов ФСТЭК России № 17-2013 и 21-2013);

– функция контроля целостности программного обеспечения (мера защиты ОЦЛ.1).

Примечание: В настоящее время на основании решения ФСТЭК России № 6267 от 12.11.2019 г. проводятся сертификационные испытания ПАК «GM SMART KVM».

5. Криптографическая защита информации, реализованная в системе GMSS

Криптографическая защиты информации, передаваемой по каналам связи между док-станциями GM-Box и серверами информационной системы, может быть организована с помощью одного из типов сертифицированных СКЗИ: КриптоПро CSP или VipNet Client.

5.1. Криптографическая защита информации в GMSS с использованием СКЗИ ViPNet Client 4U for Linux

5.1.1. Общая информация

Для обеспечения возможности безопасного удалённого подключения GM-Box к инфраструктуре заказчика с установленными шлюзами ViPNet Coordinator, в том числе, в соответствии с требованиями ГОСТ, используется сертифицированное программное средство криптографической защиты информации (СКЗИ) ViPNet Client 4U for Linux),

встраиваемое в ПО док-станции GM-Box (сертификат ФСБ России № СФ/124-3864, действителен до 23.07.2023г.).

5.1.2. Информация об используемых версиях ПО

GM-Box: встроенное ПО GM Soft Kit вер.1.12.0 (предустановлен клиент ViPNet Client 4U for Linux (релиз 4.10.0-65214.5)

ViPNet Coordinator HW 4.2+ (протестировано с HW 4.2.1-2081)

5.1.3. Сравнение возможностей предустановленных в GM Soft Kit криптопровайдеров

В GM Soft Kit встроены программные СКЗИ: КриптоПро CSP вер.4 и ViPNet Client 4U for Linux

Криптоптровайдер	**OpenVPN**	**ViPNet Client 4U for Linux**	**КриптоПро CSP вер. 4**
Тип ПО	Open Source	Отечественное ПО	Отечественное ПО
Шифрование в соответствии с ГОСТ	нет	да	да
Протокол туннелирования	OpenVPN	ViPNet	TLS 1.2
Транспортные IP протоколы	UDP, TCP	UDP, TCP	TCP
Необходимость дополнительной инкапсуляции для передачи различных видов данных	нет	нет	да (например, OpenVPN внутри TLS туннеля)
Индивидуальная настройка для каждого устройства	Опционально	Обязательно	Опционально

5.1.4. Структурная схема организации удалённого подключения

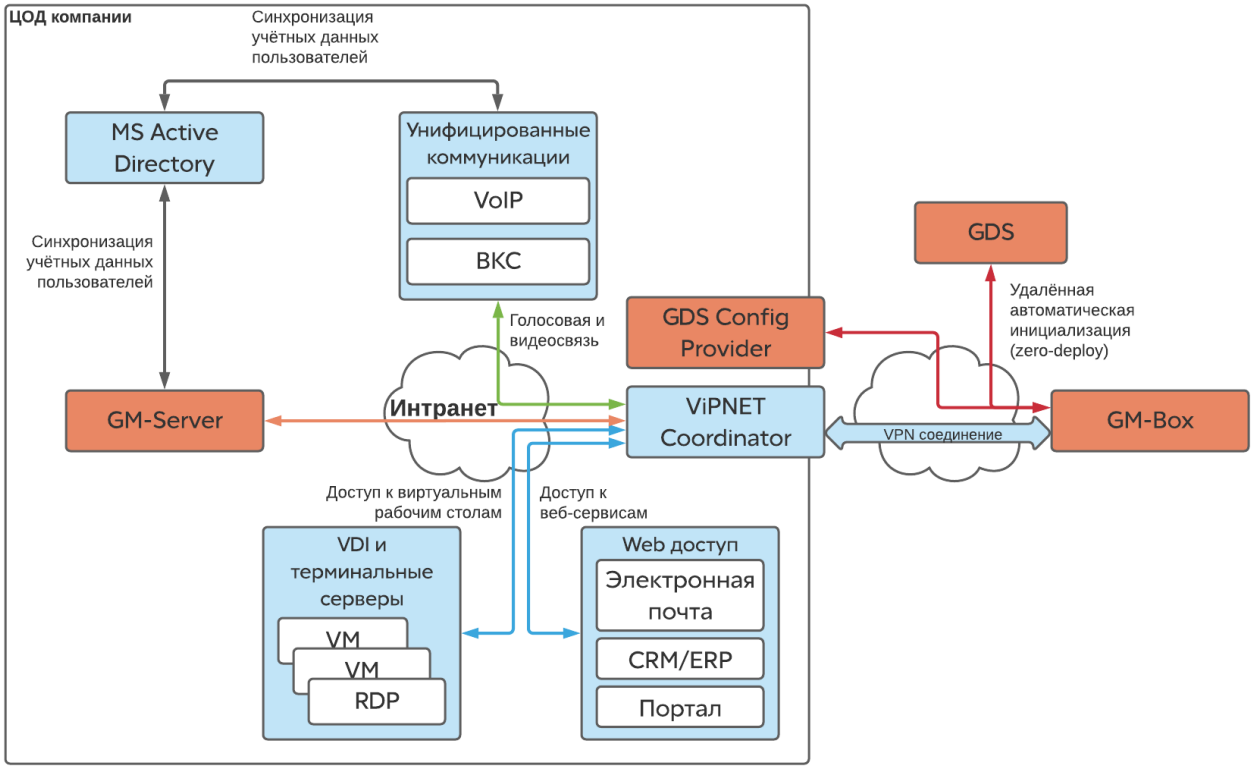

Рисунок 8 Структурная схема организация удалённого подключения

Для организации удалённого подключения GM-Box к сети заказчика через шлюз ViPNet Coordinator используется предустановленный в GM Soft Kit ViPNet Client 4U for Linux.

Система криптографической защиты ViPNet построена на принципах симметричной криптографии. В этой связи для каждого пользователя сети администратор безопасности создает свой набор ключевой информации, который входит в состав файла *.dst. Данный файл должен быть предварительно информационно безопасно распределен (доставлен) конкретному пользователю.

С точки зрения сетевого взаимодействия, организация подключения через шлюз ViPNet Coordinator является классическим VPN туннелем. Управление трафиком, проходящим через туннель, осуществляется в ViPNet координаторе и задаётся при помощи специально генерируемого администратором ViPNet Coordinator DST файла.

5.1.5. Типовой процесс организации удалённого подключения с использованием ViPNet Coordinator

Оптимальным способом организации и настройки удалённого подключения GM-Box с использованием ViPNet Coordinator является использование сервиса GDS и формирование специально подготовленного GDS архива по следующим правилам:

1. ***ОБЯЗАТЕЛЬНО*** Файл с расширением *.dst
    a. Расположение: в корне архива
    b. Содержимое: конфигурация сети ViPNet (включая ключевую информацию), защищённая паролем
    c. Назначение: определяет параметры VPN подключения с использованием ViPNet
2. ***ОБЯЗАТЕЛЬНО*** Файл с URL сервера управления GM-Server:
    a. Наименование: gmserver.url
    b. Расположение: в корне архива
    c. Содержимое: [http[s]://]<Доменное имя или IP-адрес>[:<Порт>][/]

Примечание: если URL записан без указания протокола (например, "https://"), то по умолчанию используется протокол HTTP.

Пример содержимого файла gmserver.url:
http://10.0.0.1

3. ***ОПЦИОНАЛЬНО*** Файл с учётными данными VPN ViPNet конфигурации
    a. Наименование: vipnet_secret.txt
    b. Расположение: в корне архива
    c. Содержимое: Файл состоит из одной строки, которой указан пароль от учётной записи VPN ViPNet
    d. Назначение: используется для исключения необходимости ввода пользователем пароля к файлу ViPNet. При отсутствии данного файла, при первом подключении с данной конфигурацией, пользователь вводит пароль. Повторный ввод пароля не требуется.

Подготовленные файлы должны быть заархивированы с использованием архиватора 7-zip с учётом следующих требований:

Формат контейнера:

Архив в формате 7z, с методом сжатия LZMA2 без использования технологии SFX.

Шифрование данных, при необходимости, осуществляется средствами 7z (AES 256), но с ограничением на "шифрование имён файлов" (т.е. заголовка 7z-архива).

Схема процесса отражена на рисунке 9 ниже:

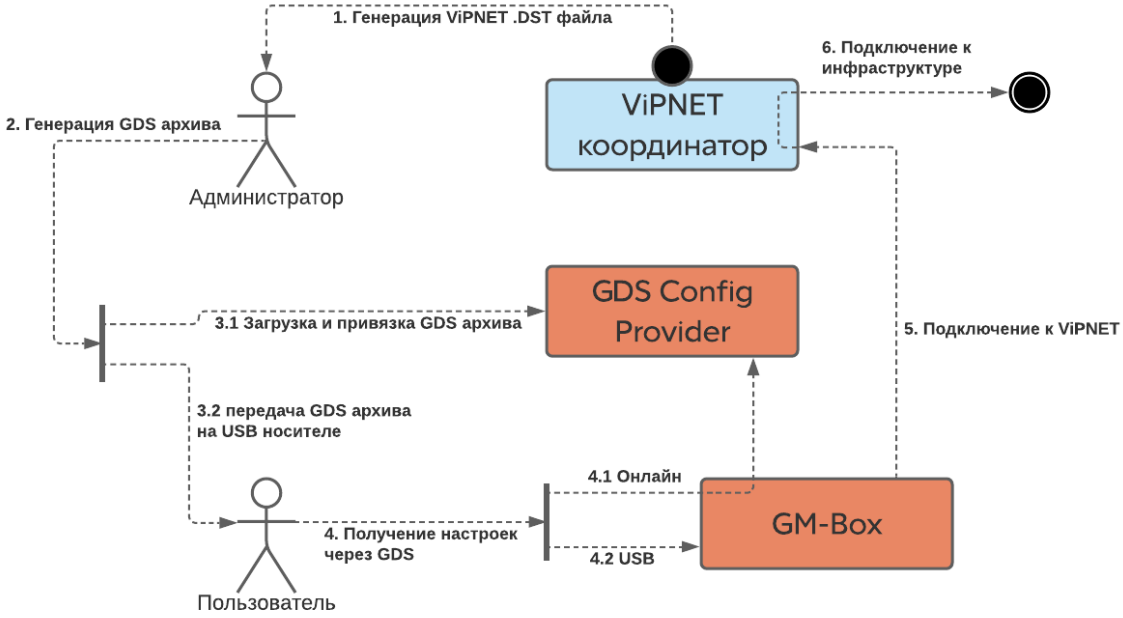

Рисунок 9 Процесс подключения к сети заказчика через шлюз ViPNet координатор

1. Администратор генерирует DST файл для устройства пользователя
2. Сгенерированный DST файл используется для подготовки GDS архива для пользователя
3. Доставка GDS архива, осуществляемая одним из двух способов:
   3.1. путем доверенной доставки пользователю USB носителя с GDS архивом - для оффлайн настройки GM-Box;
   3.2. путем загрузки GDS архива в GDS Config Provider для последующей его передачи по доверенному (защищенному) каналу связи - для онлайн настройки GM-Box.

4. Пользователь запускает процесс получения настроек ViPNet Client 4U for Linux подключения на GM-Box выбранным способом: оффлайн (с использованием USB носителя) или онлайн.
5. GM-Box получает и применяет настройки, подключается к ViPNet Coordinator заказчика
6. В случае успешного построения VPN туннеля, GM-Box подключается к сети заказчика и пользователь может приступить к работе.

5.2. Криптографическая защита информации в GMSS с использованием СКЗИ КриптоПро CSP

Для организации криптографической защиты канала связи с использованием СКЗИ КриптоПро CSP, имеющего сертификат ФСБ России № СФ/124-3570 от 14.12.2018, действителен до 15.01.2024, применяются:

- на док-станции GM-Box – клиентская версия СКЗИ КриптоПро CSP,
- на сервере информационной системы – серверная версия СКЗИ КриптоПро CSP.

Ключевая система СКЗИ КриптоПро CSP основана на принципах ассиметричной криптографии (PKI-инфраструктуры).

Формирование ключа связи док-станции GM-Box с сервером может осуществляться с использованием как односторонней аутентификации (только сервера), так и двусторонней аутентификации (сервера и GM-Box). Для реализации двусторонней аутентификации (т.е. аутентификации GM-Box) пользователь должен получить персональный закрытый ключ электронной подписи (ЭП). Данный ключ пользователь может получить традиционным способом – на отдельном флеш-носителе, или в составе GDS архива, распределяемого офлайн способом на флеш-носителе (аналогично распространению dst-файла для СКЗИ ViPNet Client 4U for Linu).

6. Эксплуатация док-станции GM-Box в выделенных помещениях

Док-станция GM-Box может устанавливаться в выделенные помещения (ВП) различных категорий. При установке в ВП док-станция GM-Box может использоваться:

- в качестве «тонкого» клиента, на базе которого построено рабочее место пользователя;
- в качестве оконечного оборудования открытой телефонной связи, основанной на применении IP-протоколов;
- в качестве абонентского пункта доступа в сеть «Интернет».

6.1. Оценка возможности использования док-станции GM-Box в выделенных помещениях

Оценка возможности использования док-станции GM-Box в выделенных помещениях различных категорий осуществляется в рамках проводимых работ по разработке и внедрению системы в интересах отдельных спецпотребителей. В рамках этих работ будут проведены оценка соответствия GM-Box требованиям ФСБ России (или ФСТЭК России), предъявляемым к:

- объектам ВТСС, размещаемым в выделенных помещениях требуемой категории (например, до 1 категории включительно - см. «Спецпроверка и специсследования док-станции GM-Box»);
- оконечным абонентским устройствам сети открытой проводной телефонной связи, размещаемым в выделенных помещениях;
- абонентским пунктам доступа в сеть «Интернет», размещаемым в выделенных помещениях.

6.2. Защита акустической информации от утечки по «телефонным» каналам открытой связи

В случае установки док-станции GM-Box в выделенные помещения необходимо обеспечить защиту циркулирующей в данных помещениях голосовой информации от утечки по открытым каналам связи в результате акустоэлектрических преобразований. В настоящее время проводятся работы по встраиванию в док-станцию сертифицированного ФСТЭК России СЗИ, предназначенного для защиты цифрового телефонного аппарата, находящегося в режиме ожидания вызова, от утечки через него сигналов помещения в звуковом диапазоне частот (акустоэлектрические преобразования) через телефонный и микрофонный капсюли трубки, динамик и микрофон громкоговорящей связи, а также отключения режима прослушивания помещения.