ПРИМЕНЕНИЕ БАЗИС.WORKPLACE SECURITY ДЛЯ ЗАЩИЩЕННОГО ПОДКЛЮЧЕНИЯ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ

ВВЕДЕНИЕ

Базис.WorkPlace Security — программный продукт для защищенного терминального доступа с единого клиентского устройства в закрытые и открытые контуры безопасности, гарантирующий отсутствие передачи данных между ними.

Базис.WorkPlace Security решает такие задачи бизнеса, как:

- Улучшение информационной безопасности ИТ-инфраструктуры компании
- Упрощение построения комплексной системы безопасности всей архитектуры
- Значительное улучшение управляемости, масштабируемости и гибкости ИТ-инфраструктуры
- Возможность организации дистанционной работы мобильных или удаленных пользователей
- Снижение операционных затрат и стоимости владения техническим средствами

К основным преимуществам Базис.WorkPlace Security относят:

- Реализация требований по безопасности (приказы 17, 21, 239 ФСТЭК России)
- Сегментирование и фильтрация информационных потоков
- Идентификация и аутентификация пользователей и терминалов на собственном сервере безопасности
- Собственная терминальная операционная система, загружаемая на клиентское рабочее место
- Поддержка устройств на базе отечественных процессоров «Байкал» и «Эльбрус»
- Полный контроль доступа пользователей к данным, приложениям и устройствам
- Терминальное решение для доступа к удаленному ПК или VDI-машине с LIVE-USB

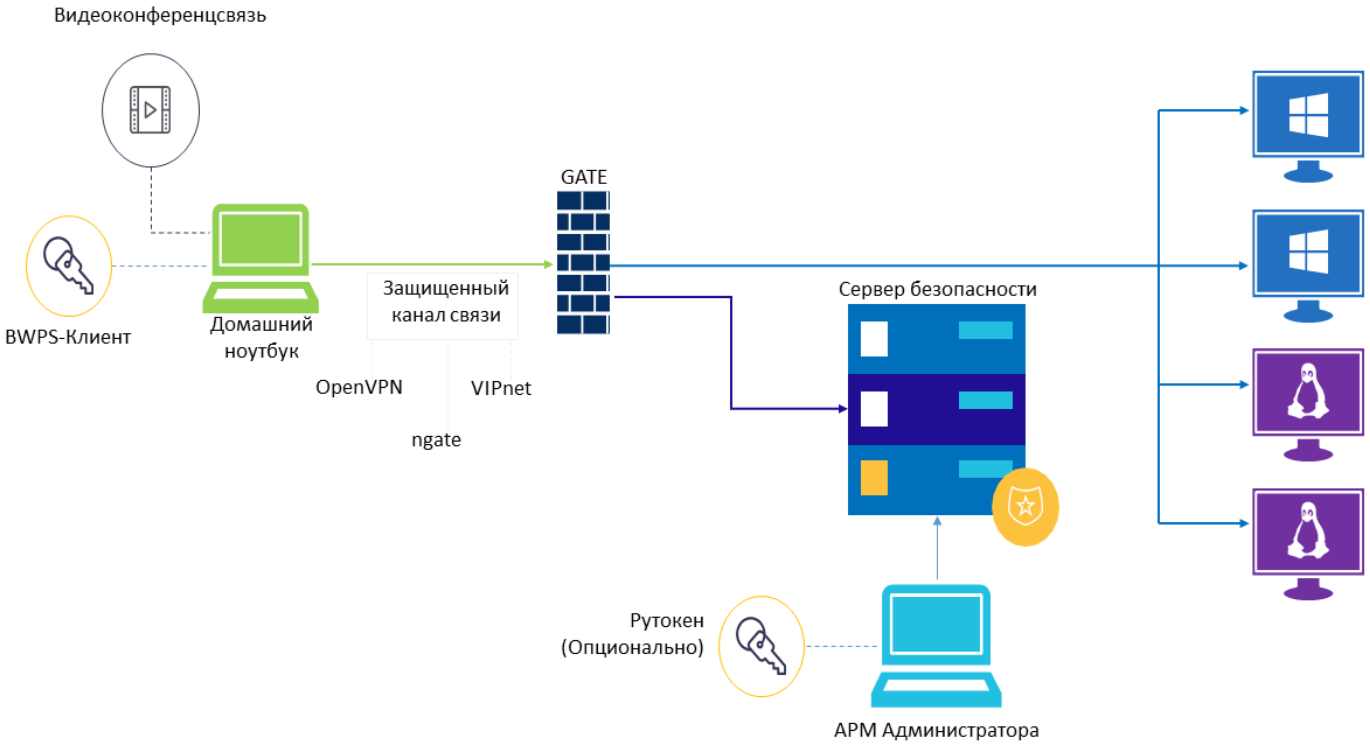
В данном документе рассматривается возможность использования сертифицированного программного обеспечения «Защита виртуальных рабочих столов ТИОНИКС» (далее – Базис.WorkPlace Security).

АРХИТЕКТУРНЫЕ ОСОБЕННОСТИ БАЗИС.WORKPLACE SECURITY

Программное обеспечение Базис.WorkPlace Security является продуктом, который реализует современную концепцию виртуализации рабочих мест пользователей, терминального доступа к инфраструктуре центра обработки данных (ЦОД), и концепцию защищенных рабочих мест пользователей, управляемых и администрируемых централизованно.

Основным предназначением Базис.WorkPlace Security является построение защищенных, масштабируемых и высокопроизводительных информационных систем трехзвенной архитектуры (тонкий клиент – виртуальная машина – база данных, портал, другие информационные сервисы), для которых одним из ключевых условий является обеспечение высокого уровня информационной безопасности. Вместе с тем, наличие в составе Базис.WorkPlace Security клиентской компоненты (защищенной операционной системы, устанавливаемой на АРМ) позволяет создать эффективную территориально распределенную безопасную инфраструктуру рабочих мест пользователей АРМ, функционирующих как самостоятельно, так и в качестве терминальных станций, подключенных к ЦОД.

Одной из особенностей Базис.WorkPlace Security является возможность использования на АРМ пользователя т.н. контуров безопасности - изолированных друг от друга сред, в каждой из которой могут независимо выполняться процессы пользователя. Каждый контур безопасности может быть подключен к разным сегментам вычислительной сети, которые могут отличаться требованиями по безопасности, при этом гарантируется изоляция этих сегментов и невозможность передачи информации между ними. Обычное назначение контура – это подключение к удаленному рабочему столу назначенной для контура виртуальной (или физической) машины в заданном сегменте сети, но также существуют и локальные контуры – в них можно запускать локальные приложения пользователя, т.е. программное обеспечение, предназначенное для функционирования под управлением ОС Debian 11. Пользователь может в любое время переключаться между контурами с сохранением работающей сессии.



Типовой пример использования Базис.WorkPlace Security

Структурно Базис.WorkPlace Security состоит из следующих компонент:

1. Сервер безопасности – управляет подключением АРМ к инфраструктуре, доступом пользователей к АРМ и его ресурсам, и обеспечивает централизованное управление всей системой.

2. Терминал – специализированный тонкий клиент или обычный ПК, на котором функционирует операционная система собственной разработки, обеспечивающая работу локальных приложений пользователя и/или терминальный сервис при подключении АРМ к виртуальным машинам в ЦОД.

Основные компоненты Базис.WorkPlace Security – сервер безопасности и терминал – представляют собой операционную систему собственной разработки (на базе ядра Linux) и программное обеспечение, функционирующее в ОС. В следующих разделах эти компоненты рассмотрены более подробно.

СЕРВЕР БЕЗОПАСНОСТИ БАЗИС.WORKPLACE SECURITY

Сервер безопасности Базис.WorkPlace Security представляет собой операционную систему и набор функционирующих в ней сервисов, решающих следующие задачи:

- аутентификация и идентификация пользователей, АРМ и контуров безопасности;
- настройка и хранение учетных записей пользователей, АРМ и других ресурсов в единой базе учетных данных;
- организация связи с АРМ и управление их работой;
- управление доступом;
- сбор и обработка журналов регистрации событий безопасности.

Функциональная роль сервера безопасности Базис.WorkPlace Security заключается в том, что этот компонент выполняет функции ядра безопасности для подключаемых АРМ. Он обеспечивает идентификацию и аутентификацию пользователей и АРМ, организацию связи между компонентами инфраструктуры, авторизацию действий пользователя (в т.ч. разрешение доступа внешним устройствам), централизованное управление настройками безопасности инфраструктуры, регистрацию событий безопасности.

ТЕРМИНАЛЬНАЯ ОПЕРАЦИОННАЯ СИСТЕМА БАЗИС.WORKPLACE SECURITY

Терминальная операционная система Базис.WorkPlace Security предназначена для управления работой АРМ и реализует следующие функции:

- идентификация и аутентификация пользователей и АРМ на сервере безопасности Базис.WorkPlace Security;
- запуск локальных приложений в отдельных контейнерах и/или установление VDI-сессии с виртуальной инфраструктурой ЦОД (при ее наличии);
- формирование пользовательского окружения;
- поддержка работы независимых изолированных контуров безопасности, обмен информацией между которыми невозможен.

Функциональная роль терминальной операционной системы Базис.WorkPlace Security заключается в том, что этот компонент управляет работой АРМ пользователя, обеспечивает работу его локальных приложений и обеспечивает работу удаленных виртуальных рабочих столов ЦОД при их наличии.

ФУНКЦИИ БЕЗОПАСНОСТИ БАЗИС.WORKPLACE SECURITY

Основными функциями безопасности Базис.WorkPlace Security являются:

- Идентификация и аутентификация пользователей и терминалов. Для пользователей предусматривается двухфакторная аутентификация.
- Разграничение доступа к приложениям, виртуальным машинам и ресурсам виртуальных машин.
- Контроль целостности программного обеспечения.
- Регистрация событий безопасности.
- Возможность работы пользователя в нескольких изолированных друг от друга контурах безопасности.
- Обеспечение безопасности при работе с периферийными устройствами и съемными носителями.

ВОЗМОЖНЫЕ СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ БАЗИС.WORKPLACE SECURITY В АИС

УДАЛЕННАЯ РАБОТА ПОЛЬЗОВАТЕЛЕЙ АИС СО СВОИМИ РАБОЧИМИ МЕСТАМИ

ЦЕЛЬ РЕШЕНИЯ

Целью решения является предоставление некоторым категориям непривилегированных пользователей возможности безопасной удаленной работы с ресурсами АИС извне объектов информатизации (в т.ч. с домашних компьютеров).

Так же решение позволяет:

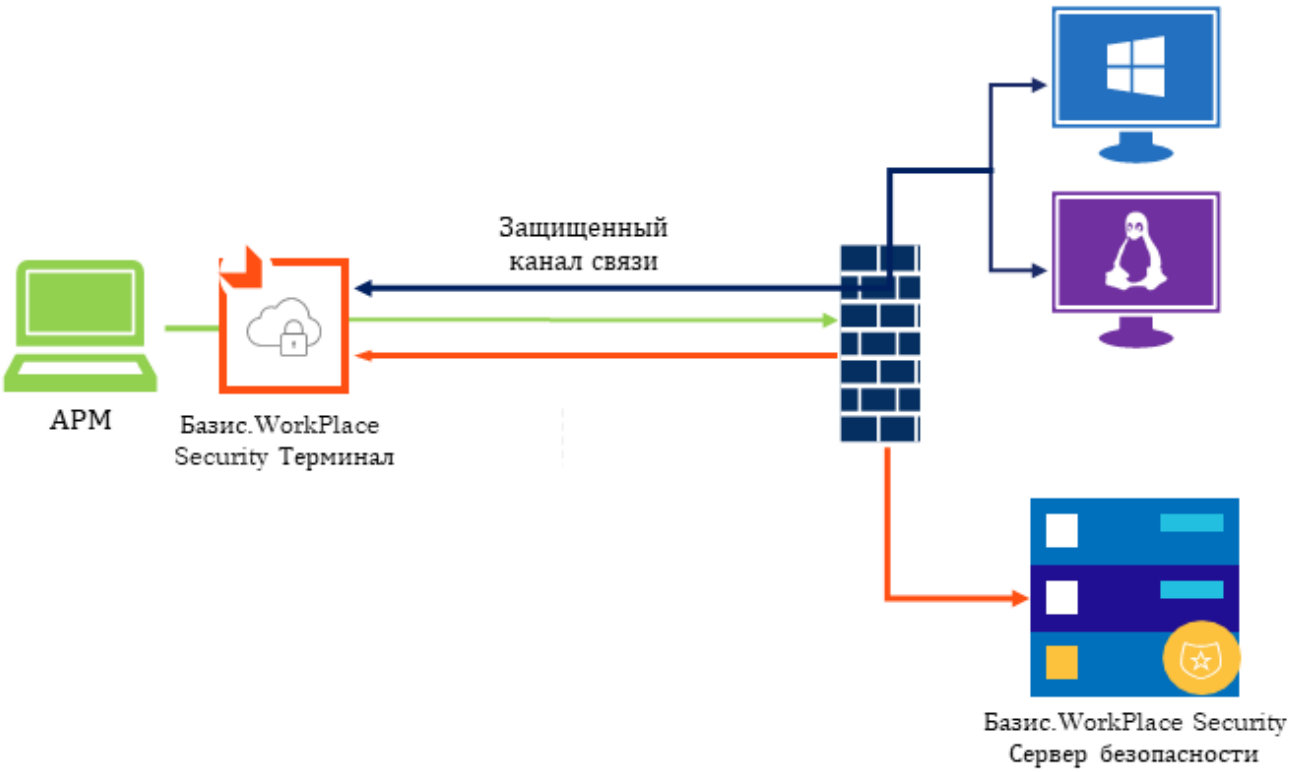
- Реализовать модель BYOD (возможность работы пользователя на своем частном оборудовании).
- Улучшить пользовательский опыт (UX) в части избавления от необходимости переключаться на разные наборы устройств при работе.
- Обеспечить централизованную (единую) точку доступа пользователя ко всем ресурсам АИС.

ПРИМЕР РЕШЕНИЯ

Базовыми принципами решения являются:

- Терминальный доступ к ресурсам АРМ (физического или виртуального), располагаемого внутри объекта информатизации АИС.
- Использование замкнутого неизменяемого клиентского ПО, работающего в составе Базис.WorkPlace Security, загружаемого с внешнего носителя информации.
- Использование сертифицированного СКЗИ (например, VipNet Client), встраиваемого в состав клиентской компоненты Базис.WorkPlace Security и обеспечивающего построение криптографически защищенного туннеля до инфраструктуры АИС. Ключи СКЗИ должны располагаться в защищенном токене.
- Отсутствие доступа к внешним каналам передачи данных во время работы клиентской компоненты Базис.WorkPlace Security, в том числе доступа к внешним портам, носителям информации, внутренним встроенным накопителям, сетевым интерфейсам, за исключением криптографически защищенного туннеля до криптошлюза, располагаемого внутри объекта информатизации АИС.

Пример решения показана на рисунке ниже:



Для работы с ресурсами АИС удаленный пользователь осуществляет загрузку ПЭВМ со специального носителя, при этом происходит загрузка защищенной терминальной ОС, входящей в комплект Базис.WorkPlace Security, которая реализует замкнутую программную среду и:

- Подключается к серверу безопасности Базис.WorkPlace Security в ЦОД и устанавливает защищенное соединение.
- Выполняет идентификацию и аутентификацию пользователя.
- Запускает в контуре безопасности процесс терминального клиента, который получает удаленный доступ к удаленному рабочему столу виртуального или физического АРМ.

Настройками Базис.WorkPlace Security обеспечивается недоступность любых других USB и накопителей информации, подключенных к ПЭВМ.

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРА

Для полного соответствия требованиям регуляторов необходимо решить следующие вопросы:

- Корректность использования, выбранного СКЗИ в составе клиентской компоненты Базис.WorkPlace Security. Решение зависит от выбранного конкретного СКЗИ и его правил

пользования. В общем случае, необходимо проводить работы по подтверждению корректности встраивания и/или оценке влияния.

- Возможность исключения МЭ в составе клиентского ПО. Решением может быть использование СКЗИ со встроенными функциями МЭ или обоснование достаточности реализованных в Базис.WorkPlace Security подтвержденных мер защиты информации, реализующих изоляцию сегментов вычислительных сетей.
- Возможность исключения на ПЭВМ использования антивирусных средств. Решением может быть обоснование достаточности реализованных в Базис.WorkPlace Security подтвержденных мер защиты информации, реализующих замкнутую программную среду и контроль ее целостности.
- Возможность исключения на ПЭВМ использования средств доверенной загрузки. Решением может быть обоснование отсутствия в данном случае необходимости этих средств, т.к. Базис.WorkPlace Security загружается с доверенного носителя информации.

БЕЗОПАСНАЯ РАБОТА ПОЛЬЗОВАТЕЛЕЙ АИС В ЗАКРЫТОМ И ОТКРЫТОМ СЕГМЕНТАХ АИС С ОДНОГО АРМ

ЦЕЛЬ РЕШЕНИЯ

Целью решения является предоставление внутренним пользователям АИС возможности работать с одного АРМ в открытом и закрытом сегментах АИС.

Так же решение позволяет:

- Реализовать модель BYOD (возможность работы пользователя на своем частном оборудовании).
- Улучшить пользовательский опыт (UX) в части избавления от необходимости переключаться на разные наборы устройств при работе.
- Сократить затраты на оборудовании благодаря переходу на CAPEX модель и отказа от необходимости комплектовать рабочее пользователя место несколькими АРМ.

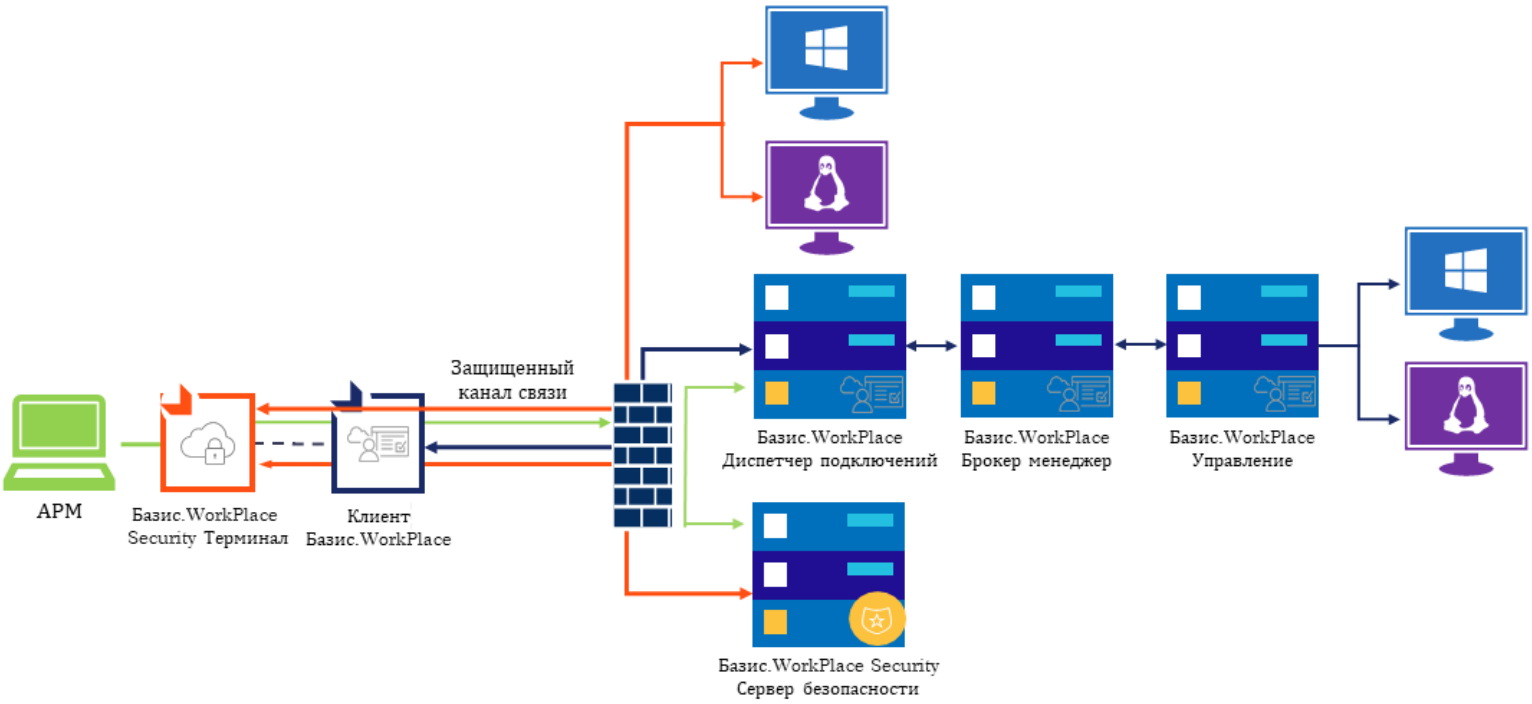
ПРИМЕР РЕШЕНИЯ

Основой решения является единый защищенный АРМ с установленной клиентской компонентой Базис.WorkPlace Security. АРМ расположен в закрытом сегменте АИС и имеет два физических сетевых интерфейса. Один сетевой интерфейс подключен к маршрутизатору/коммутатору закрытого сегмента, другой – открытого. Каждый сетевой интерфейс ассоциируется только со своим контуром безопасности Базис.WorkPlace Security, отсутствие возможности влияния и передачи информации между контурами и различными сегментами сети обеспечивается мерами защиты информации, встроенными в Базис.WorkPlace Security.

Пример кейса использования:

У Организации есть потребность обеспечить 100 пользователей рабочими местами с доступом в открытый сегмент сети с интернетом и в закрытый с конфиденциальными документами. В классическом устаревшем исполнении, Организации пришлось бы обеспечивать каждого пользователя одновременно двумя рабочими местами, потратив значительные средства на комплектацию 200 рабочих АРМ. При использовании же решения Базис.Workplace Security необходимость в АРМ уменьшается вдвое, так как 1 АРМ позволяет работать сразу в нескольких сегментах сети.

Пример решения показана на рисунке ниже:



Настройками Базис.WorkPlace Security обеспечивается независимость сетевых интерфейсов и отсутствие сетевой связности между сегментами сети, а также невозможность передачи информации между контурами безопасности.

Данное решение предполагает различные способы обеспечения замкнутости ПО на АРМ – например, выход в закрытый сегмент может обеспечивать локальный контур безопасности, в котором может быть установлено прикладное ПО, функционирующее под ОС типа Debian (LibreOffice, Mozilla и др.) и имеющее возможность сохранять свои данные на локальном диске. Контур, имеющий выход в открытый сегмент, может иметь запрет на установку любого ПО, кроме браузера, и не иметь возможности записи данных на локальный диск или на съемных носителях информации.

Другим вариантом данного решения является использование двух терминальных контуров безопасности, полностью закрытых от изменения ПО и обеспечивающих лишь терминальный доступ к рабочим столам виртуальных машин, функционирующих в виртуальной инфраструктуре открытого и закрытого сегмента.

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРА

Данное решение полностью соответствует требованиям регулятора и условиям применения сертифицированного СЗИ Базис.WorkPlace Security. Дополнительными сертифицированными СЗИ, уже использующимися в инфраструктуре АИС, в зависимости от условий применения такого типа АРМ, могут быть антивирусное ПО «Kaspersky Endpoint Security 10 для Linux» и сертифицированный АПМДЗ «Соболь».

ЦЕЛЬ РЕШЕНИЯ

Целью решения является существенное повышение безопасности АИС при доступе к ее ресурсам, предоставляемым работникам подрядных организаций при выполнении работ по обслуживанию АИС в соответствии с договором подряда.

Так же решение позволяет:

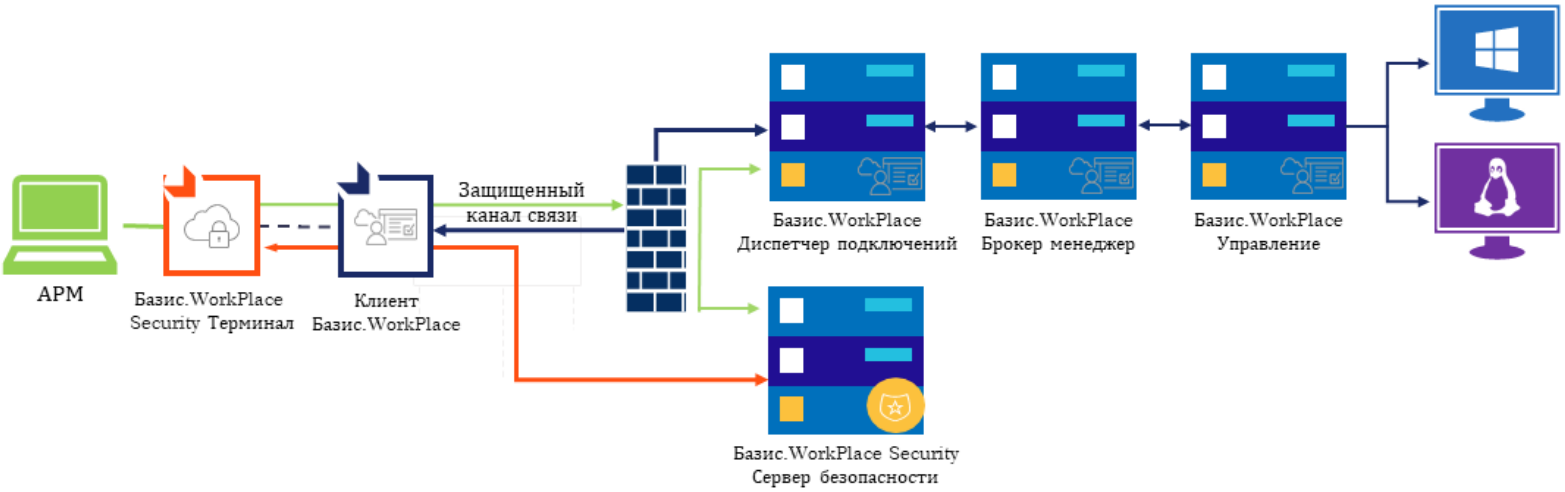
- Обеспечить централизованную (единую) точку доступа пользователя ко всем ресурсам АИС.
- Обеспечить контроль за действиями пользователей.
- Обеспечить гибкое централизованное управление временными учетными записями и доступом к ресурсам АСИ.

АРХИТЕКТУРА РЕШЕНИЯ

Базовыми принципами решения являются:

- Организация доступа подрядных организаций осуществляется исключительно через виртуальные машины подрядчиков (ВМП), располагаемые внутри виртуальной инфраструктуры АИС и управляемую штатными администраторами АИС.
- Доступ к ВМП осуществляется в терминальном режиме с АРМ подрядчика, на котором установлено сертифицированное клиентское ПО, в котором реализованы меры защиты информации по ограничению программной среды и управлению доступом.
- При работе АРМ в режиме терминального доступа к ВМП должны быть ограничены возможности по взаимодействию с другими системами, в т.ч. Интернет. Доступ к внешним носителям АРМ должен быть разрешен только в тех случаях, когда это требуют задачи по сопровождению АИС.
- Использование отдельного сертифицированного СКЗИ (например, VipNet Coordinator), реализованного в виде программно-аппаратного комплекса, который устанавливается в вычислительной сети подрядчика для организации криптографически защищенного туннеля до инфраструктуры АИС.

Пример решения показана на рисунке ниже:



Настройками Базис.WorkPlace Security обеспечивается отсутствие сетевой связности между открытым и закрытым (зашифрованный туннель) сегментами сети подрядчика, невозможность влияния со стороны ЛВС подрядчика на контур безопасности, предоставляющий терминальный доступ к ВМП, при этом сохраняется возможность одновременной работы обслуживающего персонала как с ВМП, так и со сторонними ресурсами, необходимыми для выполнения работ по обслуживанию АИС.

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРА

Данное решение полностью соответствует требованиям регулятора и условиям применения сертифицированного СЗИ Базис.WorkPlace Security. Дополнительными сертифицированными СЗИ, в случае инсталляции Базис.WorkPlace Security на внутренний диск АРМ и/или использования дополнительного локального контура, имеющего связь с открытым сегментом сети, должны быть антивирусное ПО «Kaspersky Endpoint Security 10 для Linux» и сертифицированный АПМДЗ «Соболь».

СВЕДЕНИЯ О СЕРТИФИКАТАХ И РЕАЛИЗОВАННЫХ В БАЗИС.WORKPLACE SECURITY МЕРАХ ЗАЩИТЫ ИНФОРМАЦИИ

Базис.WorkPlace Security сертифицирован ФСТЭК России - сертификат соответствия Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 № 4489 выдан ФСТЭК России 21.12.2021, действителен до 21.12.2026.

Согласно сертификату, Базис.WorkPlace Security является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции идентификации и аутентификации, управления доступом, регистрации событий безопасности, обеспечения целостности и ограничения программной среды, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) – по 4 уровню доверия и технических условиях RU.НРФЛ.00003-01 90 01.

Базис.WorkPlace Security может применяться для защиты информации от несанкционированного доступа в государственных информационных системах 1-го класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1-го класса защищенности, на объектах критической информационной инфраструктуры первой категории значимости, в информационных системах персональных данных при необходимости обеспечения 1-го уровня защищенности персональных данных.

Согласно Формуляру и Техническим условиям RU.НРФЛ.00003-01 90 01 в Базис.WorkPlace Security реализованы следующие меры защиты информации:

Условное обозначение меры защиты	**Название меры защиты**
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора

Условное обозначение меры защиты	Название меры защиты
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов управления доступом (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)

Условное обозначение меры защиты	Название меры защиты
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
ЗНИ.5	Контроль использования интерфейсов ввода (вывода)
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти

Условное обозначение меры защиты	Название меры защиты
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности
РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
ЗИС.14	Использование устройств терминального доступа для обработки информации

Условное обозначение меры защиты	Название меры защиты
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы
ЗИС.21	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения