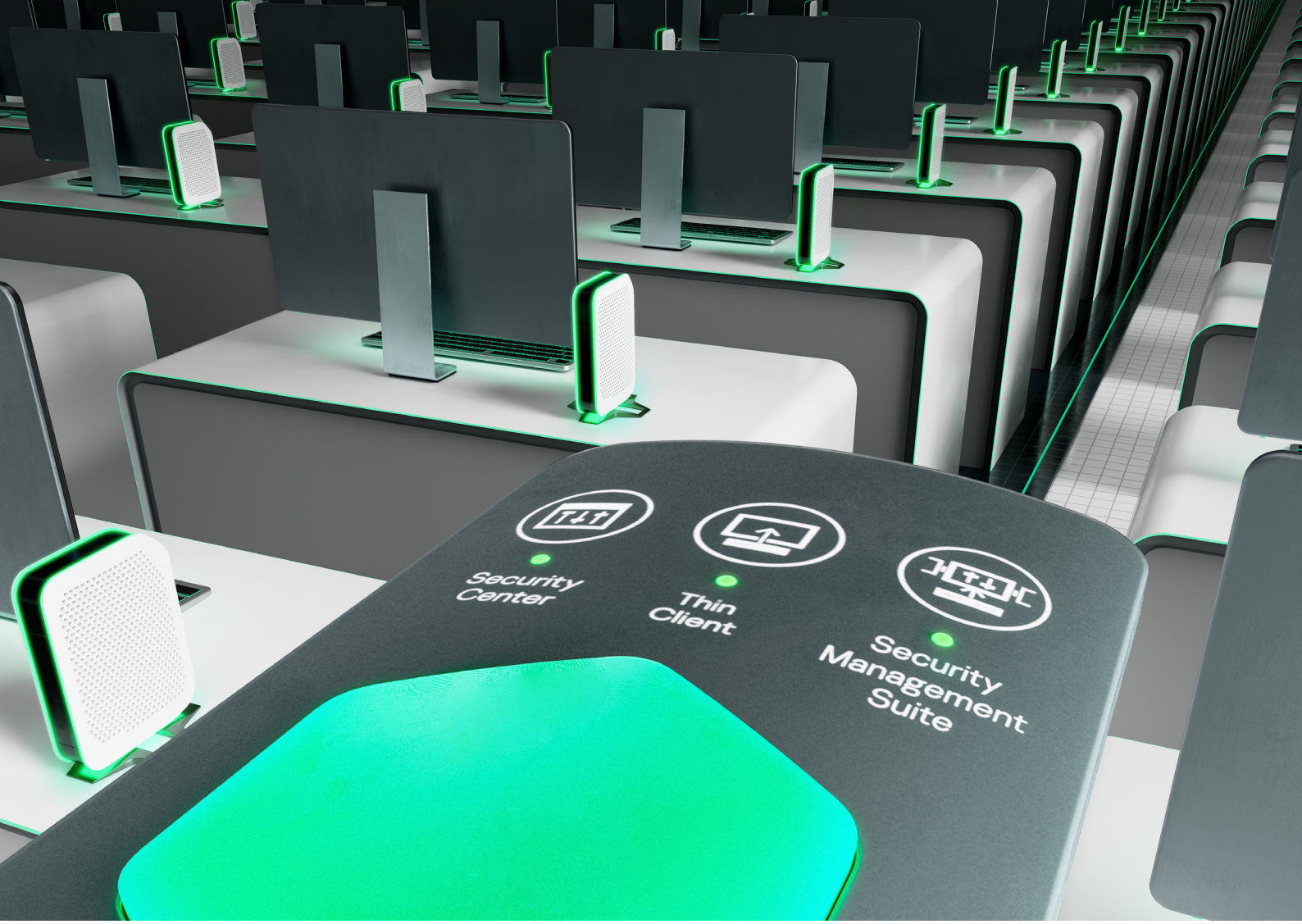


Кибериммунная, управляемая и функциональная инфраструктура тонких клиентов

Kaspersky Secure Remote Workspace

KasperskyOS

VDI – актуальная технология организации удаленных рабочих мест

Инфраструктура виртуальных рабочих столов (**Virtual Desktop Infrastructure**, или VDI) подразумевает, что сотрудники получают свои рабочие инструменты, виртуальные ПК, в виде набора программ и данных на удаленном сервере. Подключение к серверу происходит при помощи специальных терминалов – тонких клиентов (ТК). У этой концепции есть множество преимуществ перед традиционными рабочими местами:

- автоматизация процесса создания рабочих мест;
- уход от хранения и обработки данных на устройствах сотрудников;
- быстрое восстановление данных после инцидентов;
- управление удаленными рабочими местами из одной точки;
- сниженный риск атак удаленных рабочих мест.

Тонкие клиенты обладают преимуществами перед ПК и ноутбуками:

- отсутствие движущихся частей (вентиляторов и HDD) положительно сказывается на сроке эксплуатации (7-10 лет);
- небольшие габариты и вес, эргономичность и простота обслуживания и эксплуатации;
- низкое энергопотребление и тепловыделение;
- выгодная цена и стоимость владения по сравнению с классическими десктопами и ноутбуками.

VDI нужно защищать

При всем своем удобстве, VDI не может полноценно обеспечивать безопасность виртуальной инфраструктуры. При недостаточной защищенности оконечных устройств, VDI может стать объектом для разного типа атак.

Возможные угрозы для тонких клиентов

Вредоносное ПО и сетевые атаки

При недостаточной защищенности тонкий клиент может стать объектом для атаки вредоносным кодом. Это заблокирует работу с устройством и подвергнет опасности данные на удаленной машине или даже всю VDI

Опасные подключаемые устройства

Неконтролируемые съемные носители информации — это потенциальный путь распространения вредоносного ПО и инструмент для кражи информации

Перехват нажатий клавиш клавиатуры

Хотя обработка информации идет на стороне виртуальной машины, пользователь все еще активно использует клавиатуру для ввода паролей учетных записей на тонком клиенте, а значит, злоумышленник может использовать кейлоггер

Новые уязвимости в системном ПО

Наложенные средства безопасности не могут гарантировать защищенность без регулярной установки обновлений системного ПО

Обязательное условие: управляемость инфраструктуры

Без удобной централизованной системы управления тонкими клиентами их настройка, обновление или аудит — трудоемкий и рискованный процесс. В полной мере достоинства тонких клиентов раскрываются при наличии централизованной системы управления, позволяющей упростить процессы настройки, администрирования и поддержки.

Подход «Лаборатории Касперского» к защите VDI и управляемости инфраструктуры тонких клиентов

Потенциальные угрозы можно предотвратить и защитить парк тонких клиентов благодаря кибериммунному подходу, который применен в решении **Kaspersky Secure Remote Workspace** (KSRW). Тонкие клиенты в составе решения построены на базе операционной системы KasperskyOS. Безопасная по умолчанию (Secure by Design) операционная система избавляет от необходимости использовать наложенные средства защиты. Еще один компонент решения — единая консоль управления — решает проблемы управляемости и мониторинга инфраструктуры тонких клиентов.

Состав решения

Kaspersky Secure Remote Workspace

Kaspersky Thin Client

Программный продукт на базе операционной системы KasperskyOS, устанавливаемый на аппаратную платформу

Бессрочная лицензия на мажорную версию

Kaspersky Security Center

Единая консоль управления тонкими клиентами и другими продуктами «Лаборатории Касперского»

Бесплатная установка (в случае отсутствия консоли в инфраструктуре)

Kaspersky Security Management Suite

Модуль расширения для организации централизованного администрирования тонких клиентов через единую консоль управления KSC

Лицензия на подключение к KSC. Подписочная модель по количеству устройств на 1, 2 или 3 года

Где применяется Kaspersky Secure Remote Workspace

Решение **Kaspersky Secure Remote Workspace** подходит для многих сфер, где используется большое количество рабочих мест со схожими задачами и типовым набором приложений. Примерами вертикалей могут служить:

- государственный сектор;
- образовательные учреждения;
- промышленность;
- ТЭК, энергетика;
- здравоохранение;
- финансовые организации;
- розничная торговля.

Киберимунитет — это «врожденная» защищенность IT-системы, ее способность противостоять кибератакам без использования дополнительных (наложенных) средств безопасности. Подавляющее большинство видов атак на киберимунную систему неэффективно и не может повлиять на выполнение ею критических функций.

Киберимунные продукты практически невозможно скомпрометировать в плановых режимах работы, в них принципиально минимизировано число возможных уязвимостей.

KasperskyOS — операционная система, которая применяется там, где существуют повышенные требования к безопасности: в умном городе, транспорте, промышленности, электроэнергетике, госсекторе и других областях. Она позволяет обеспечить конфиденциальность и целостность данных и обезопасить их от подмены.

Киберимунные тонкие клиенты — важный компонент безопасности VDI

Врожденная безопасность решения **Kaspersky Secure Remote Workspace** обеспечивает выполнение следующих требований:

- целостность данных, полученных от пользователя, от сервера централизованного управления **Kaspersky Security Center** и от серверов брокеров соединения;
- безопасное обновление **Kaspersky Thin Client**;
- конфиденциальность и целостность данных, передаваемых между **Kaspersky Thin Client**, удаленным рабочим столом, сервером **Kaspersky Security Center** (KSC), сервером логирования и брокером соединения.

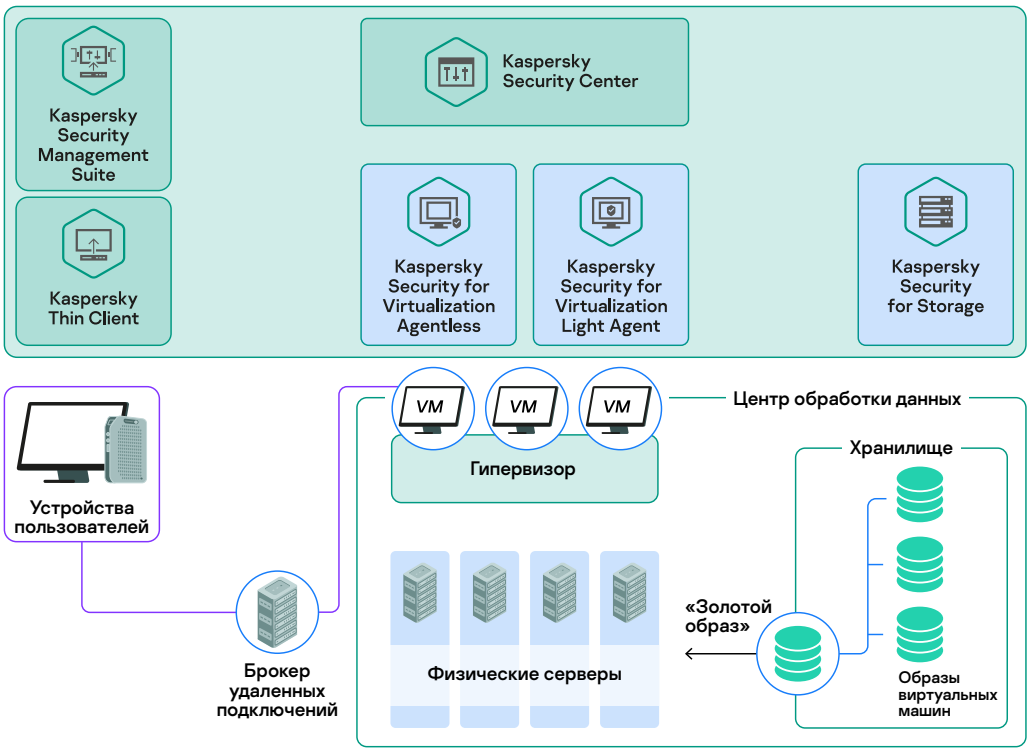
Киберимунные тонкие клиенты – это защищенная «последняя миля» построения надежной IT-инфраструктуры для работы с виртуальными рабочими столами.

Централизованное управление инфраструктурой тонких клиентов

Консоль **Kaspersky Security Center**, входящая в состав решения, позволяет управлять тонкими клиентами из единого центра, настраивать их, администрировать, доставлять обновления и собирать системные события. KSC активно используется другими продуктами «Лаборатории Касперского», и благодаря этому интеграция KSRW в существующую экосистему защиты корпоративных IT-систем может стать максимально бесшовной и не потребует найма дополнительных специалистов.

Роль Kaspersky Secure Remote Workspace в комплексной защите VDI продуктами «Лаборатории Касперского»

Kaspersky Secure Remote Workspace является частью комплексного проекта по организации защиты VDI.. Решение работает совместно с классическими антивирусными средствами защиты виртуальных и облачных сред, а также систем хранения данных. Все эти продукты также управляются с помощью **Kaspersky Security Center**.



Типовые целевые сценарии

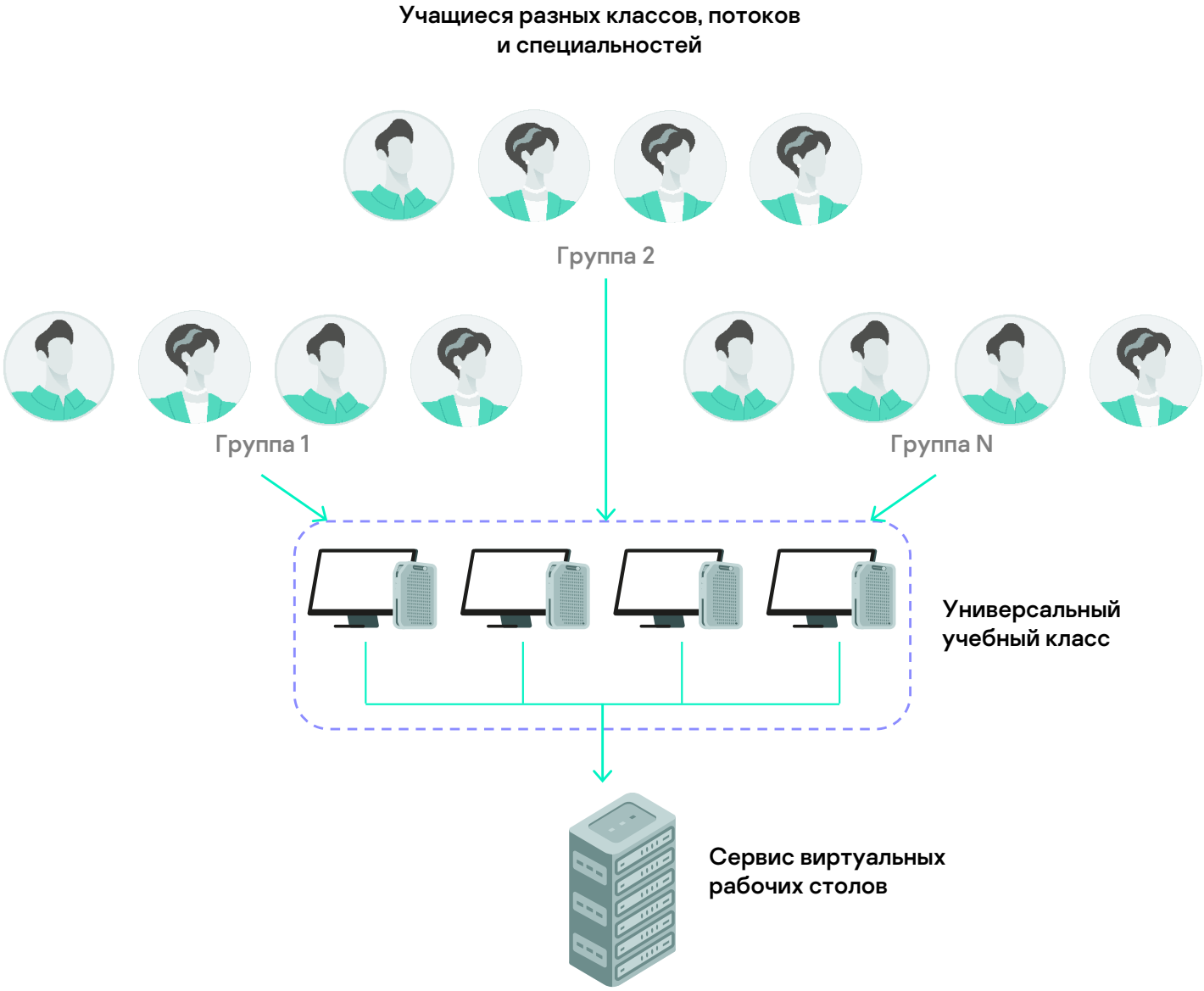
1. Офис и филиалы

Kaspersky Secure Remote Workspace эффективно для компаний с разветвленной филиальной сетью. В филиалы устанавливаются преднастроенные тонкие клиенты, которые безопасно подключаются к виртуальным рабочим местам и централизованно управляются консолью KSC. В сравнении с десктопами и ноутбуками, решение обладает выгодной стоимостью, ценой владения и меньшими затратами на поддержку.

2. Учебные классы в образовательных учреждениях

Частая проблема в учебных классах — нецелевое использование десктопов и ноутбуков. Также высока вероятность взлома сети или заражения вредоносным ПО со съемных носителей.
Преимущества использования тонких клиентов:

- ученики могут подключаться только к необходимым сервисам;
- возможность быстрого развертывания учебной среды для лабораторной практики студентов;
- есть возможность ограничения использования съемных носителей;
- долгий срок службы тонких клиентов, в сравнении с десктопами и ноутбуками.

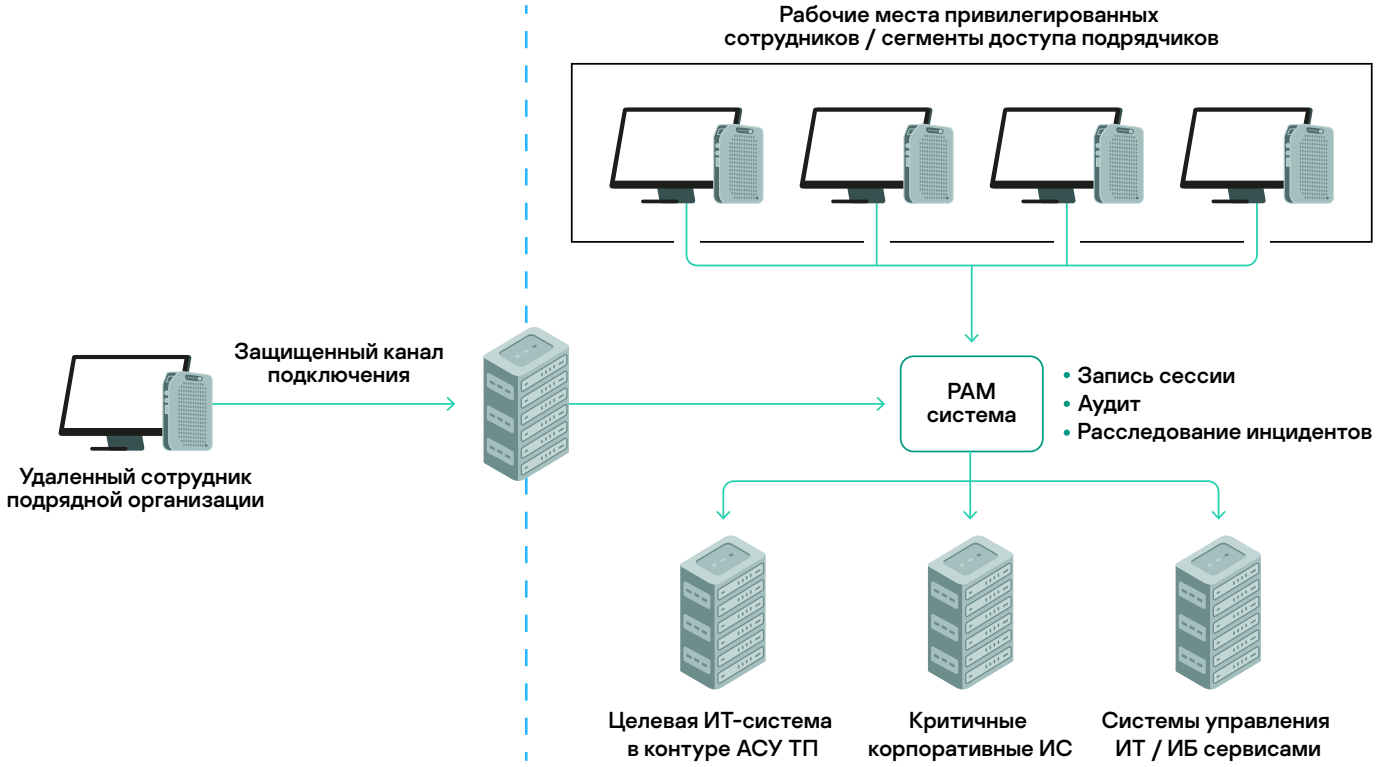


3. Подключение к системам контроля привилегированного доступа

Системы контроля доступа привилегированных пользователей (Privileged Access Management, PAM) позволяют вести аудит действий специалистов (как внутренних, так и внешних) с расширенными правами, записывать сессии, управлять настройками парольной защиты и процессами авторизации и аутентификации. Такие системы применяются в том числе там, где обслуживание ключевых объектов инфраструктуры передается на IT-аутсорсинг, а объекты, к которым осуществляется доступ, критически важны (например, АСУ ТП).

Применение решения **Kaspersky Secure Remote Workspace** совместно с системой PAM исключает использование сотрудниками собственных переносимых устройств, которые могут использоваться для атак на инфраструктуру. Также это позволяет контролировать подключение периферийных устройств.

Предустановленные на серверы PAM и тонкие клиенты сертификаты не позволяют подключиться к инфраструктуре, минуя систему контроля доступа.

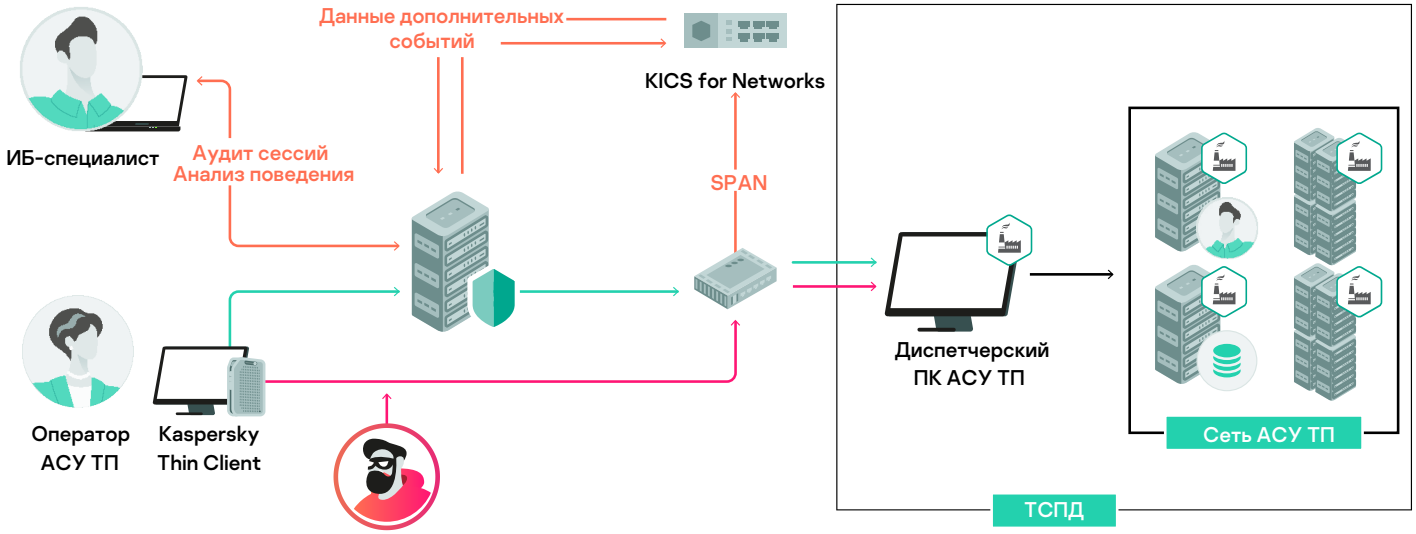


4. Изоляция сегментов и предоставление заведомо безопасного доступа к КИИ

Безопасный и сегментированный доступ реализуется на базе системы СКДПУ НТ совместно с решением **Kaspersky Secure Remote Workspace**. Данная схема доступа позволяет ограничить доступ только необходимыми для работы устройствами с возможность ограничения запуска произвольного ПО на целевом узле.

Сотруднику предоставляется удаленное рабочее место. Доступ для подключения внутрь защищаемого сегмента осуществляется с помощью тонких клиентов с установленным на них программным продуктом Kaspersky Thin Client на базе операционной системы KasperskyOS. Сбор и анализ событий в рамках сессий обеспечивается средствами системы СКДПУ НТ.

При этом за счет расширенной интеграции с продуктами «Лаборатории Касперского», Kaspersky Industrial Cyber Security for Networks, реализуются дополнительные функции по контролю доступа напрямую к защищаемым ИС объекта КИИ.



Дополнительная информация

Узнайте больше о возможностях Kaspersky Secure Remote Workspace и отправьте заявку на консультацию экспертов:
os.kaspersky.ru/solutions/kaspersky-secure-remote-workspace

os.kaspersky.ru
www.kaspersky.ru

© 2023 АО «Лаборатория Касперского»
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

KasperskyOS