Сакура

iT EXPERTISE

Возможности комплекса САКУРА для обеспечения информационной безопасности и контроля рабочих мест

Обзор продукта

© 2024 ИТ-Экспертиза. Все права защищены.

О компании ИТ-Экспертиза

НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ:

САКУРА – программный комплекс информационной безопасности для мониторинга и активного контроля удалённых рабочих мест

Консалтинг по информационной безопасности — аудит и разработка рекомендаций по совершенствованию систем информационной безопасности (ГИС, КИИ, персональные данные), подготовка необходимой документации для регуляторов.

1С:Интеграция КОРП – корпоративная шина данных (КШД/ESB) с универсальным коннектором 1С и открытым кодом. Совместный продукт с Фирмой 1С.

Технологические услуги компании ИТ-Экспертиза для решений на платформе 1С:Предприятие:

- Корпоративное информационно-техническое сопровождение
- Повышение отказоустойчивости и производительности
- Разработка на платформе 1С: Предприятие в рамках проектов

НАШИ КЛИЕНТЫ:

Что такое комплекс САКУРА?

Программный комплекс САКУРА – российская разработка, помогающая обеспечить:

- Соответствие удаленных рабочих мест внутренним политикам безопасности
- Двухфакторную аутентификацию
- Контроль доступа к корпоративным ресурсам
- Мониторинг действий сотрудника на рабочем месте
- Инвентаризацию оборудования и ПО

Реестр Российского программного обеспечения
Реестровая запись № 9018 от 05.02.2021

САКУРА и возможности импортозамещения в ИБ

В условиях ухода иностранных вендоров ИБ с российского рынка всё более актуально применение полностью отечественных разработок для обеспечения безопасности ИТ-инфраструктуры.

Комплекс информационной безопасности САКУРА **является полностью российской** разработкой и внесен в реестр Минцифры (отечественного ПО). САКУРА совместима как с ОС Windows, так и **Linux**, в том числе Astra Linux, Ред ОС и AlterOS

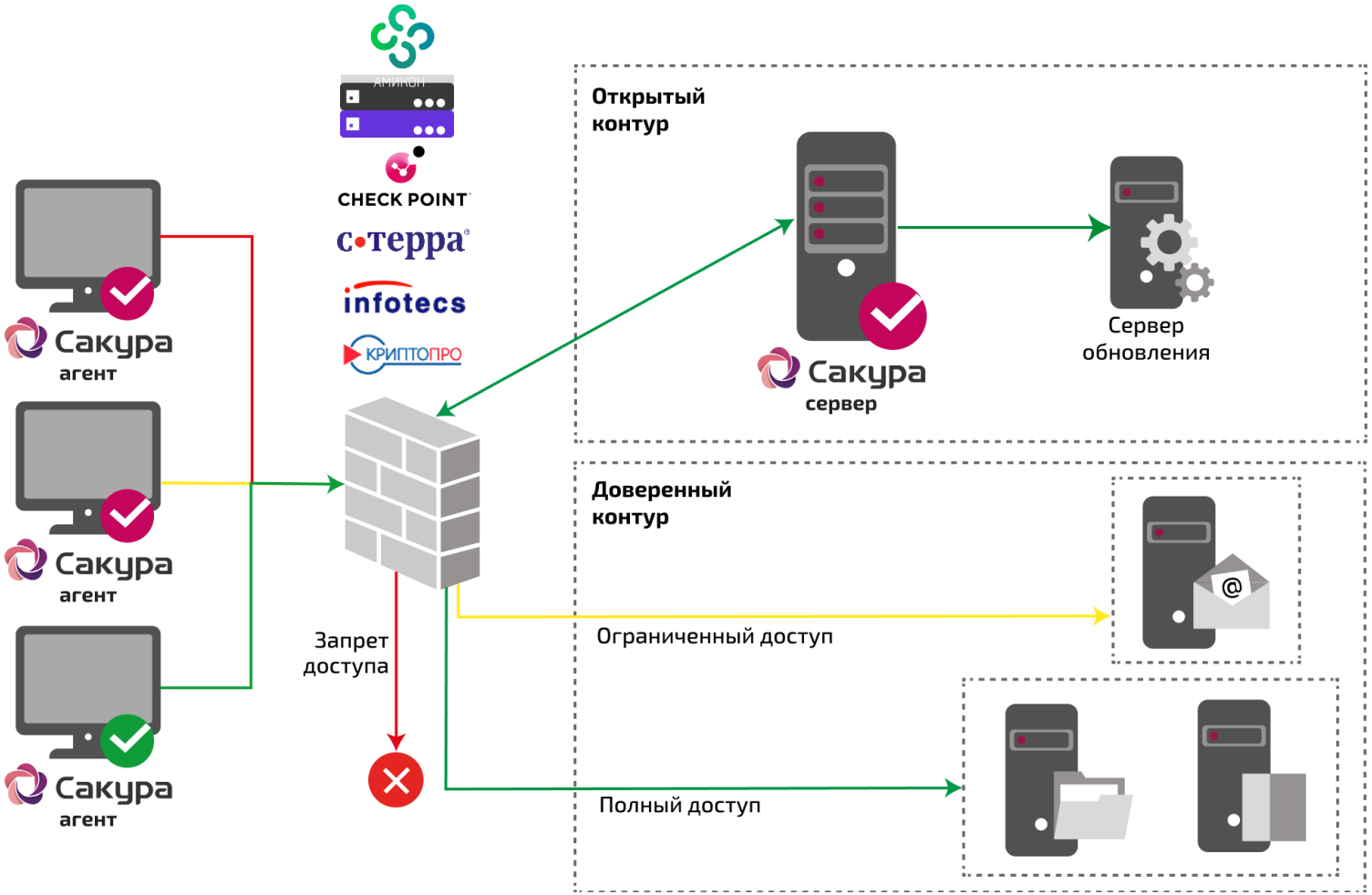
В составе комплекса САКУРА доступна **on-premise система двухфакторной аутентификации**, которая сможет стать альтернативой решениям CISCO DUO или Fortigate VPN Two-Factor Authentication после ухода зарубежных вендоров с российского рынка

Комплекс САКУРА **интегрирован с российскими VPN решениями**, такими как КриптоПро NGate, ViPNet, S-Terra, что позволяет построить инфраструктуру доступа с нулевым доверием (Zero Trust Network Access) полностью на отечественном ПО и оборудовании

Минкомсвязь России

Программный комплекс САКУРА официально включен в единый реестр российских программ для электронных вычислительных машин и баз данных, которые могут закупаться государственными и муниципальными учреждениями (https://reestr.digital.gov.ru/reestr/310368/).

Архитектура



ПК САКУРА

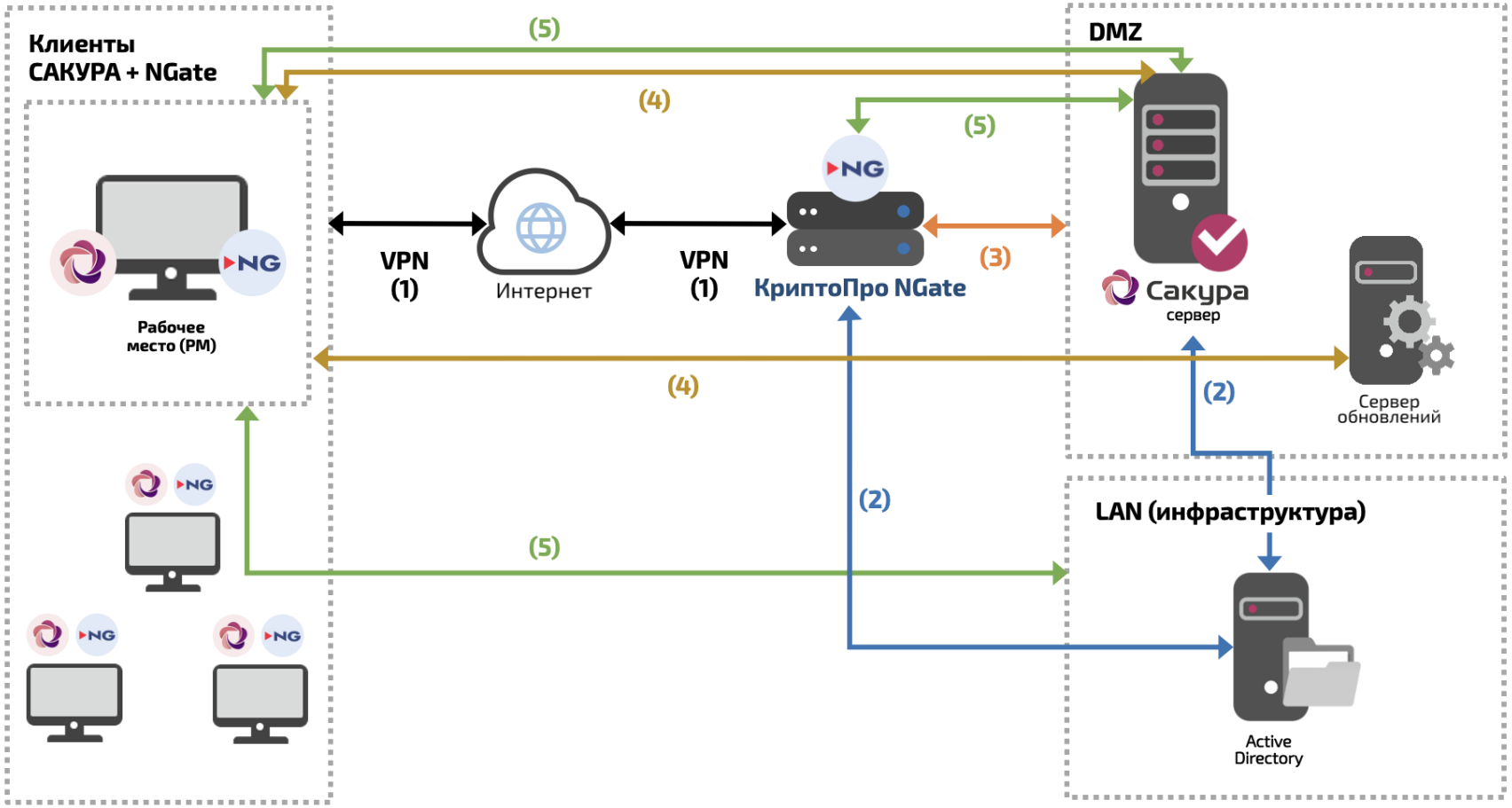
Состоит из **серверной компоненты и агентской компонеты**

Совместима с:

- ✓ **Windows**
- ✓ **Linux**
- ✓ **MacOS**

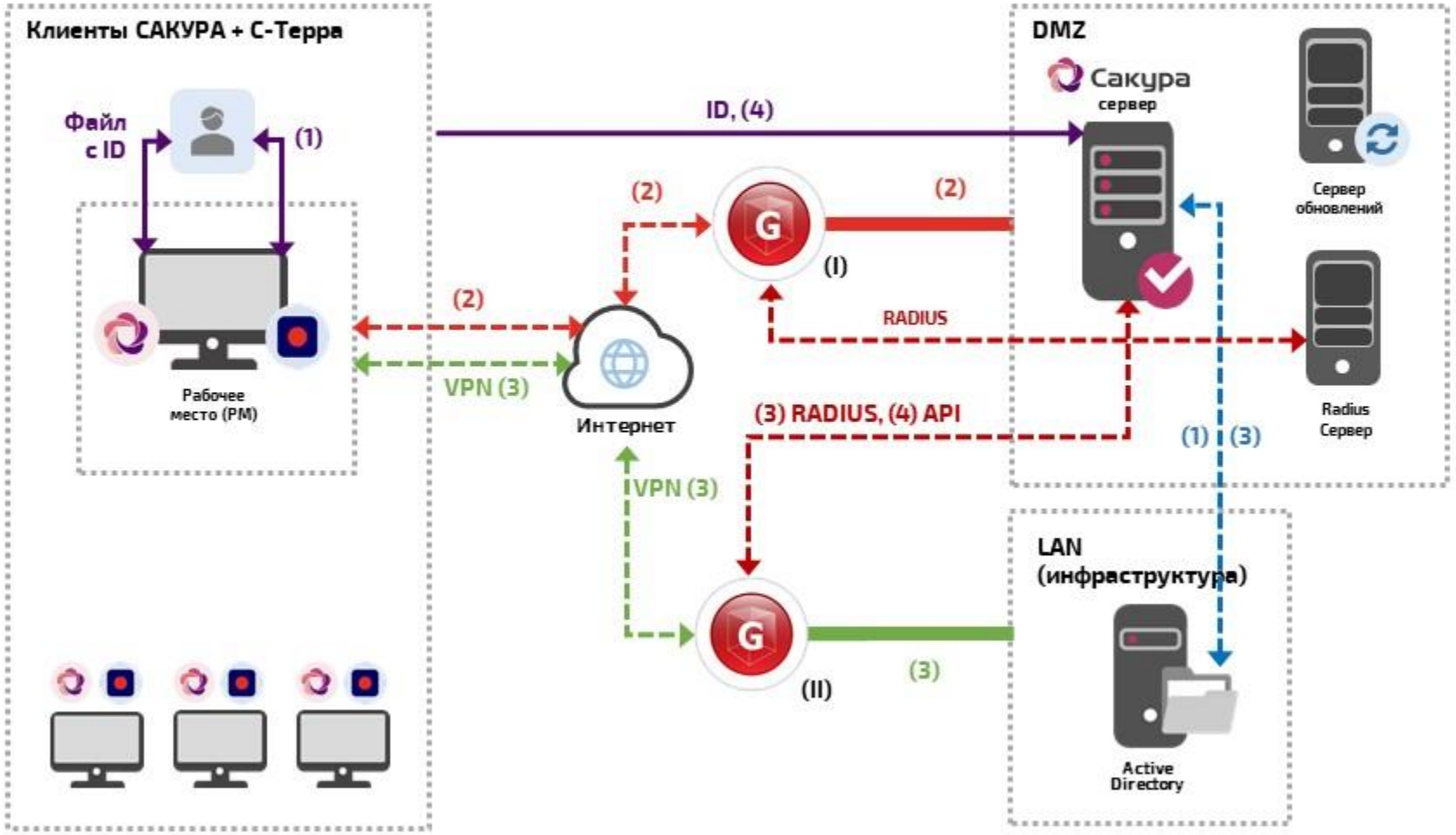
Интегрируется с VPN: КРИПТОПРО, с•терра, infotecs, КОД безопасности, АМИКОН, CHECK POINT

Интеграции программного комплекса САКУРА и шлюза NGate с клиентской инфраструктурой



1. Клиентское рабочее место подключается по VPN к шлюзу Ngate
2. Сервер САКУРА и шлюз NGate Синхронизируются с Active Directory (AD), где настроены группы доступа COMPLIANT и NON-COMPLIANT
3. По умолчанию, рабочее место находится в группе NON-COMPLIANT, имеющей доступ строго в DMZ, где расположены Сервер САКУРА и Сервер обновлений
4. Рабочее место проходит проверку на сервере САКУРА, по результатам пользователь перемещается в группу COMPLIANT, либо же клиенту САКУРА подается команда получить обновления компонентов с сервера обновлений
5. При успешном прохождении проверок РМ, сервер САКУРА перемещает пользователя в группу COMPLIANT, шлюз NGate синхронизируется с AD и затем предоставляет доступ рабочему месту пользователя в инфраструктуру (LAN)

Интеграция программного комплекса САКУРА и шлюза С-Терра клиентской инфраструктурой



1. На РМ Клиент Сакура получает ID Пользователя из файла в системе для идентификации С-Терра Клиент Сервер САКУРА Синхронизируются с Active Directory (AD), где настроены группы доступа COMPLIANT и NON-COMPLIANT

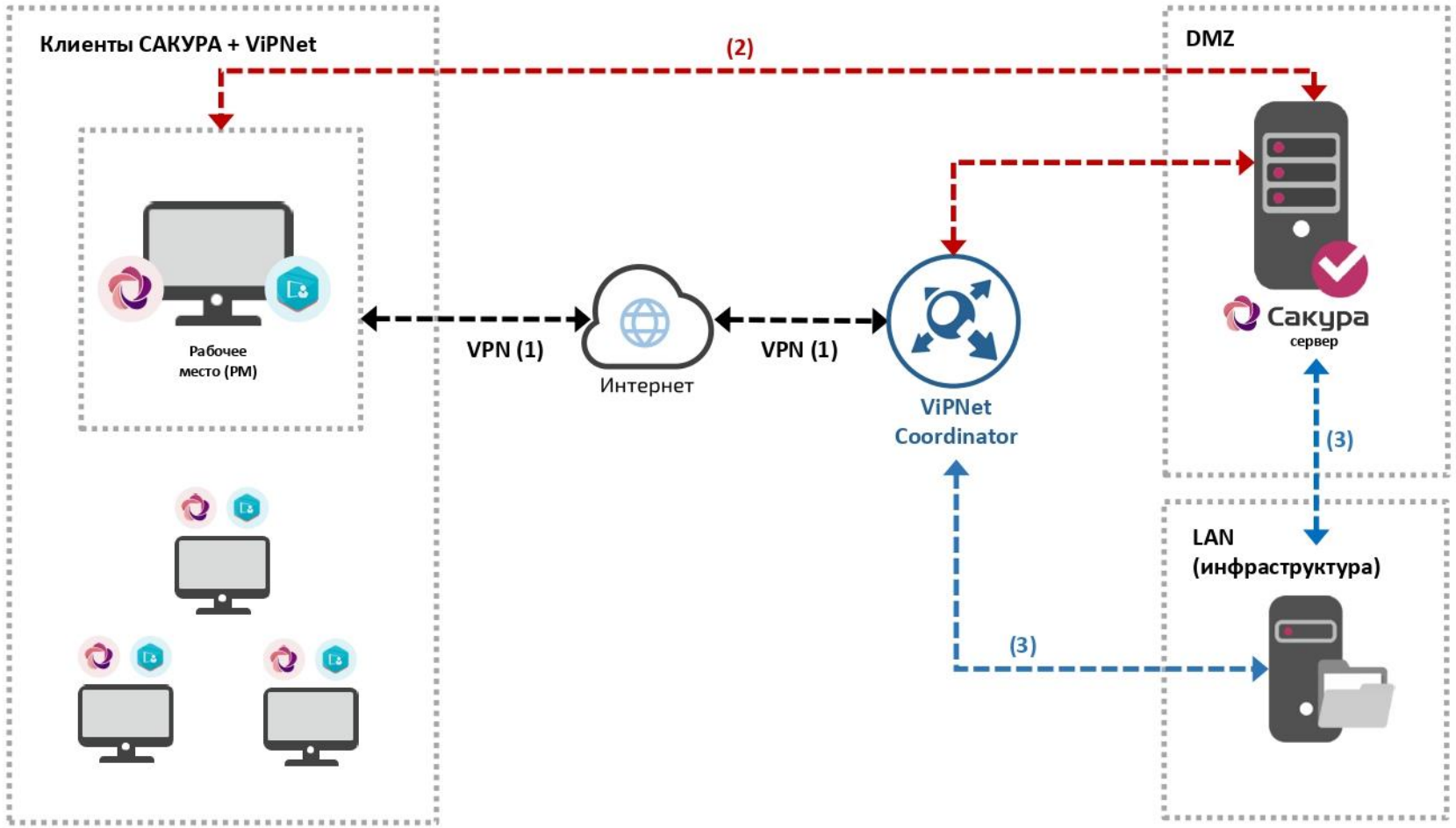
2. Данные об аутентификации пользователя передаются на С-Терра Шлюз (I). Строится VPN тоннель (2). Radius Сервер используется для аутентификации пользователей на С-Терра Шлюзе.

3. С-Терра Агент периодически посылает запрос на подключение к С-Терра Шлюз (II) для доступа в VPN тоннель (3). Рабочее место проходит проверку на сервере САКУРА, по результатам пользователь перемещается в группу COMPLIANT, либо же клиенту САКУРА подается команда, например, получить обновления компонентов с сервера обновлений (по VPN тоннелю (2)). Как только Сервер Сакура подтверждает статус РМ COMPLIANT, Он по RADIUS дает разрешение на С-Терра Шлюз (II), строится VPN тоннель (3) для доступа РМ к LAN

В случае изменения состояния АРМ:

4. Клиент Сакура обнаруживает изменение состояния и оповещает об этом Сервер Сакура (4). Сервер Сакура инициирует сброс сессии по API (4) Пользователя по ID на С- Терра Шлюз (II) в LAN. VPN Тоннель (3) сброшен

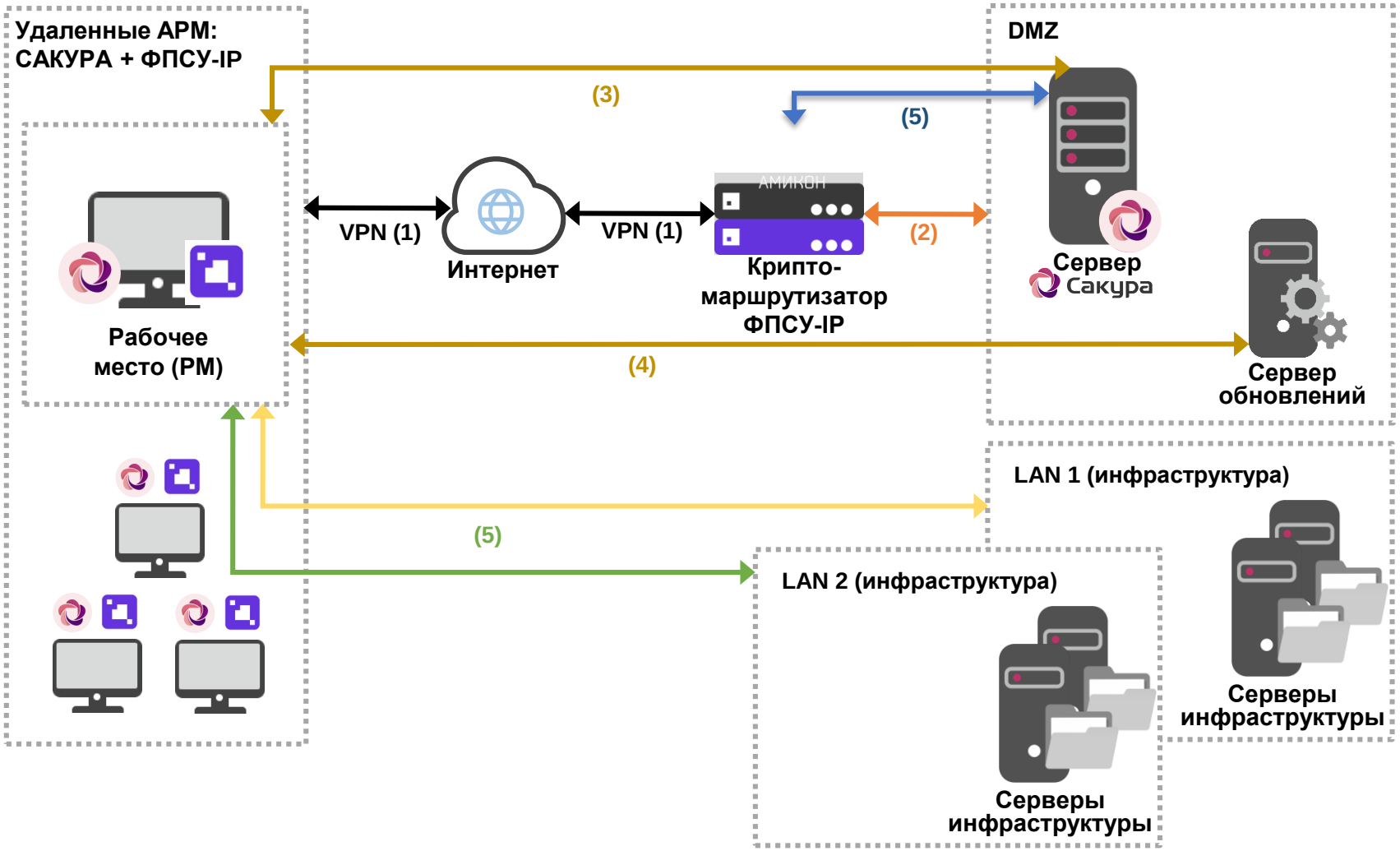
Интеграция программного комплекса САКУРА и шлюза ViPNet с клиентской инфраструктурой



1. Клиентское рабочее место подключается по VPN к шлюзу ViPNet Coordinator, где получает доступ в DMZ к серверу САКУРА

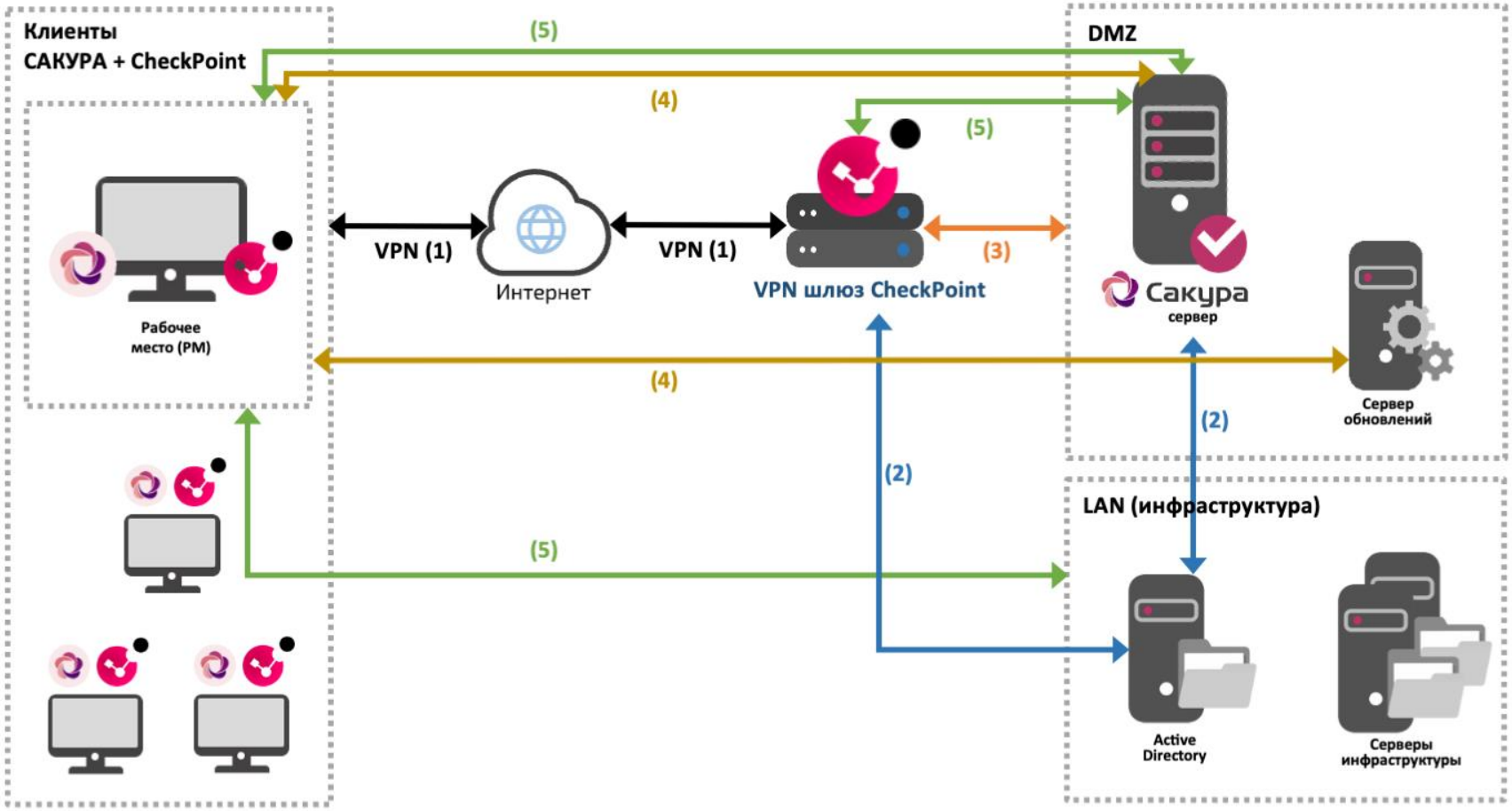
2. При успешном подтверждении, Сервер САКУРА через API ViPNet подает на шлюз ViPNet Coordinator команду с подтверждением сессии для этого пользователя, получающего доступ в инфраструктуру (LAN)

Интеграции программного комплекса САКУРА и VPN ФПСУ-IP АМИКОН



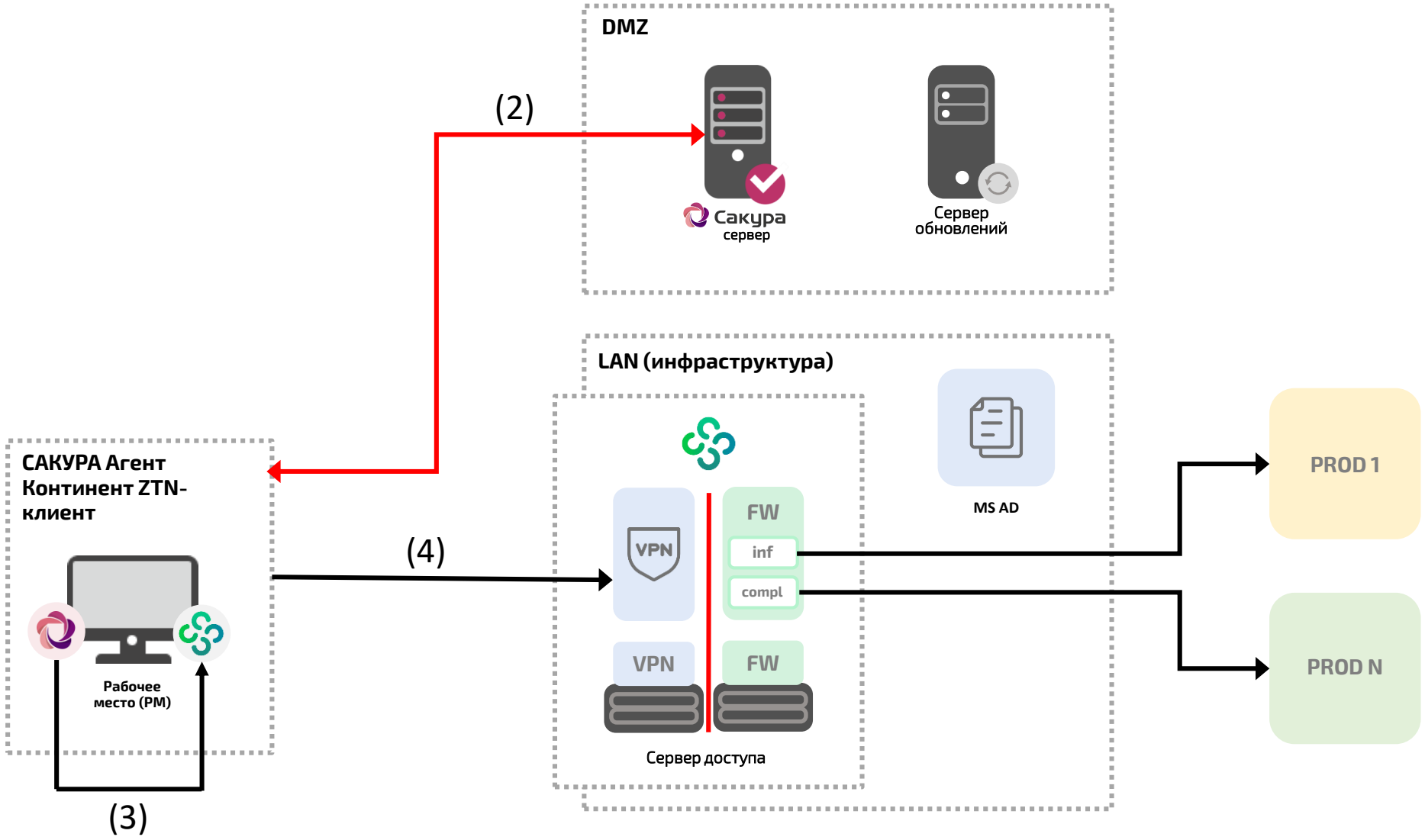
1. Удаленное рабочее место подключается по VPN криптомаршрутизатору "ФПСУ-IP"
2. Удаленное рабочее место считается недоверенным, пока не проведены проверки и получает доступ только в демилитаризованную зону (DMZ)
3. Агент САКУРА, установленный на удаленном рабочем месте проводит проверки политик безопасности и сообщает статус рабочего места и параметры VPN соединения на сервер САКУРА
4. В случае необходимости САКУРА подается команда получить обновления с сервера обновлений компании (например для АВЗ, ОС)
5. При успешном прохождении проверок РМ, сервер САКУРА сообщает криптмаршрутизатору ФПСУ-IP статус уровня нарушений. В САКУРА поддерживается несколько уровней нарушений (УН), в зависимости от УН возможно задать разный уровень доступа для удаленного АРМ

Интеграции программного комплекса САКУРА и VPN шлюза CheckPoint с клиентской инфраструктурой



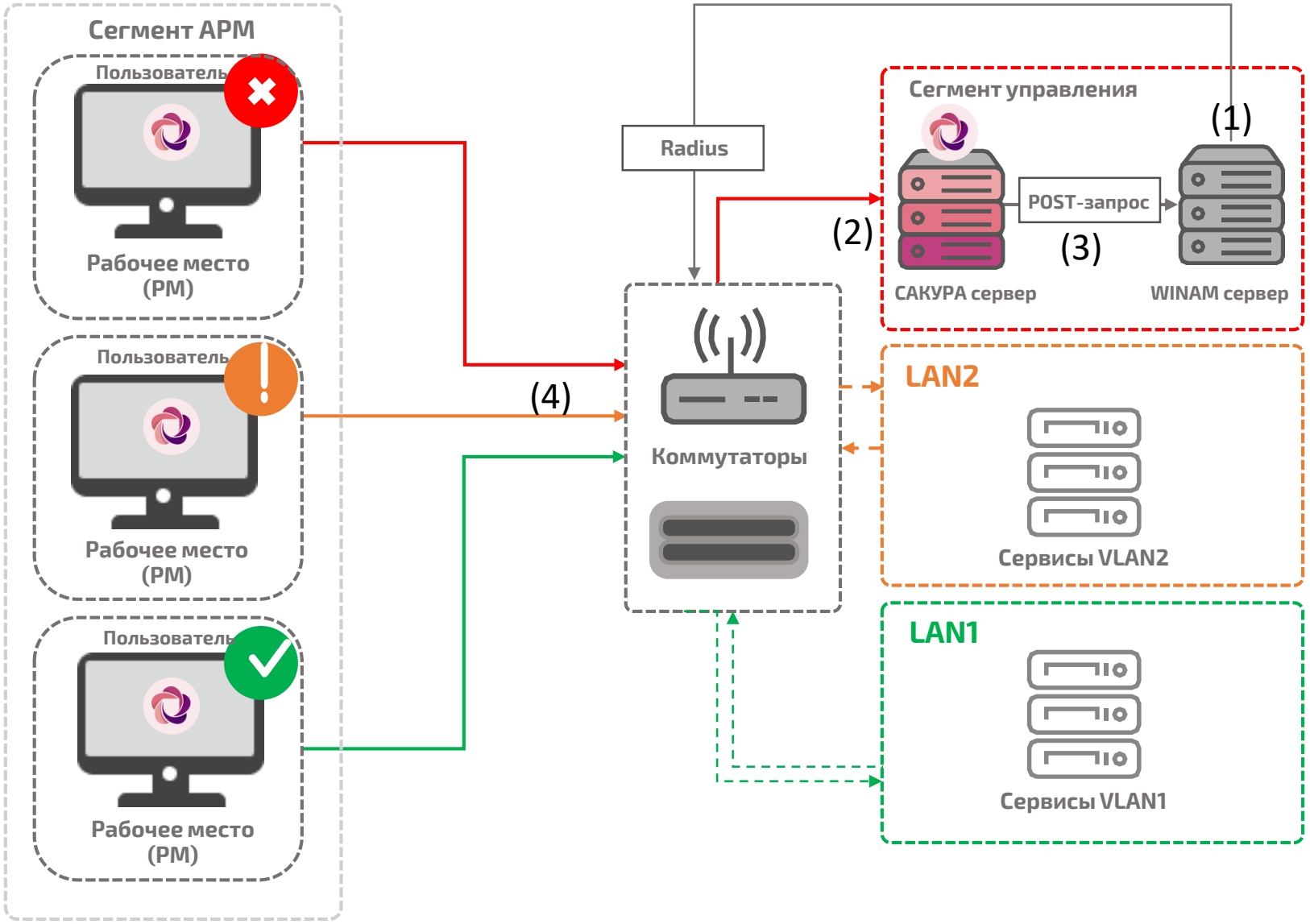
1. Клиентское рабочее место подключается по VPN к шлюзу CheckPoint
2. Сервер САКУРА и шлюз CheckPoint Синхронизируются с Active Directory (AD), где настроены группы доступа **COMPLIANT** и **NON-COMPLIANT**
3. По умолчанию, рабочее место находится в группе **NON-COMPLIANT**, имеющей доступ строго в DMZ, где расположены Сервер САКУРА и Сервер обновлений
4. Рабочее место проходит проверку на сервере САКУРА, по результатам пользователь перемещается в группу **COMPLIANT**, либо же клиенту САКУРА подается команда получить обновления компонентов с сервера обновлений
5. При успешном прохождении проверок РМ, сервер САКУРА перемещает пользователя в группу **COMPLIANT**, шлюз CheckPoint синхронизируется с AD и затем предоставляет доступ рабочему месту пользователя в инфраструктуру (LAN)

Интеграция Континент ZTN-клиент и программного комплекса САКУРА



1. На PM устанавливается Агент САКУРА и ZTN-клиент
2. Агент САКУРА на PM проводит проверку на комплайенс (соответствие политикам информационной безопасности)
3. Агент САКУРА передает полученный результат проверки в виде статуса PM на ZTN-клиент
4. ZTN-клиент, в зависимости от полученного статуса PM, устанавливает соединение либо разрывает соединение с инфраструктурой

Интеграция программного комплекса САКУРА и WNAM (NETAMS)



1. Рабочее место подключается к оборудованию под управлением сервера WNAM
2. Агент подключается к серверу САКУРА, который определяет статус АРМ
3. Сервер САКУРА направляет на WNAM сервер POST запрос, в котором указывает статус и ip адрес АРМ, WNAM предоставляет соответствующий доступ
4. Интеграция реализует пять сценариев маршрутизации: нет нарушений/информационный/ предупреждение/критический/ устройство не идентифицировано САКУРА (например, не агента)

Функциональность

- ✓ Безопасность
- ✓ Инвентаризация
- ✓ Контроль активности сотрудников

© 2024 ИТ-Экспертиза. Все права защищены.

Безопасность:
Контроль комплаенса рабочих мест

- САКУРА позволяет получить практически все параметры рабочих мест и проверить их на соответствие требованиям **политик информационной безопасности**.
- В продуктивных внедрениях контролируется **более 200 параметров безопасности**.
- По результатам проверки может быть **ограничен доступ к корпоративным информационным системам** и/или направлены уведомления офицерам информационной безопасности

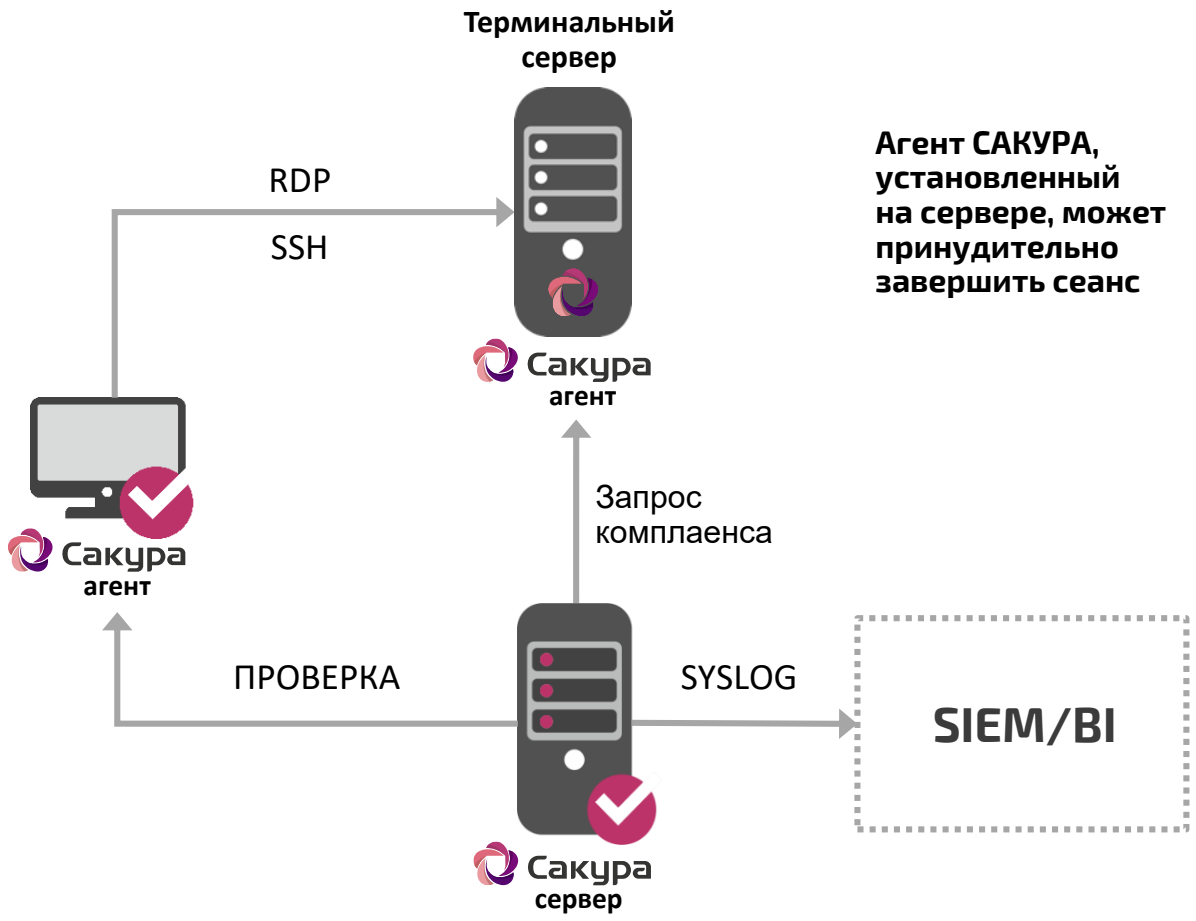
Операционная система	ПО	Настройки	Антивирус
Местоположение	Оборудование	Процессы	Канал связи

Возможность формирования собственных правил контроля с использованием скриптов PowerShell и Bash

Автоматическое реагирование на инциденты безопасности

Безопасность: Контроль доступа

Применение комплекса САКУРА позволяет **ограничивать несанкционированные удаленные подключения** к защищаемым ресурсам:



- Разрешать подключения по RDP к защищаемым серверам только с рабочих мест, на которых установлена САКУРА и выполняются требования комплаенса рабочих мест
- Запрещать (останавливать процессы, формировать инциденты ИБ) нерегламентированное ПО удаленного доступа на рабочих станциях и серверах (TeamViewer, DameWare и пр.)
- Информация об инцидентах информационной безопасности **может быть в режиме «онлайн» передана во внешнюю систему (например, SIEM или BI)**, развернутую в корпоративной системе Заказчика (по протоколу SYSLOG)

Безопасность: Двухфакторная аутентификация

Применение комплекса САКУРА позволяет реализовать **доступ к ресурсам через VPN с применением двухфакторной аутентификации пользователя по:**

- **Параметрам подключения (логин/пароль)**

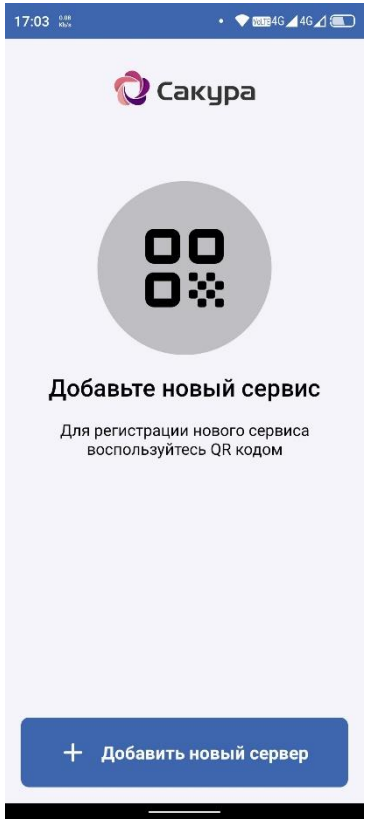
- **Дополнительному фактору аутентификации:**

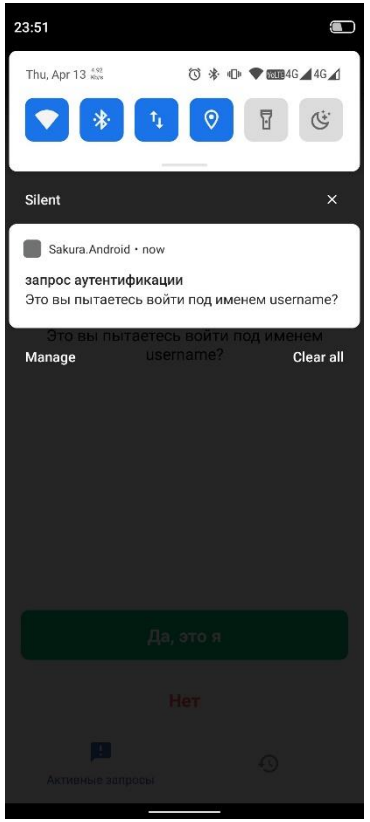
  Мобильное приложение «САКУРА 2FA» либо Telegram бот

- **Дополнительно:**

  Авторизации рабочего места пользователя

  (состав программного и аппаратного обеспечения, геолокация, общий комплаенс безопасности)

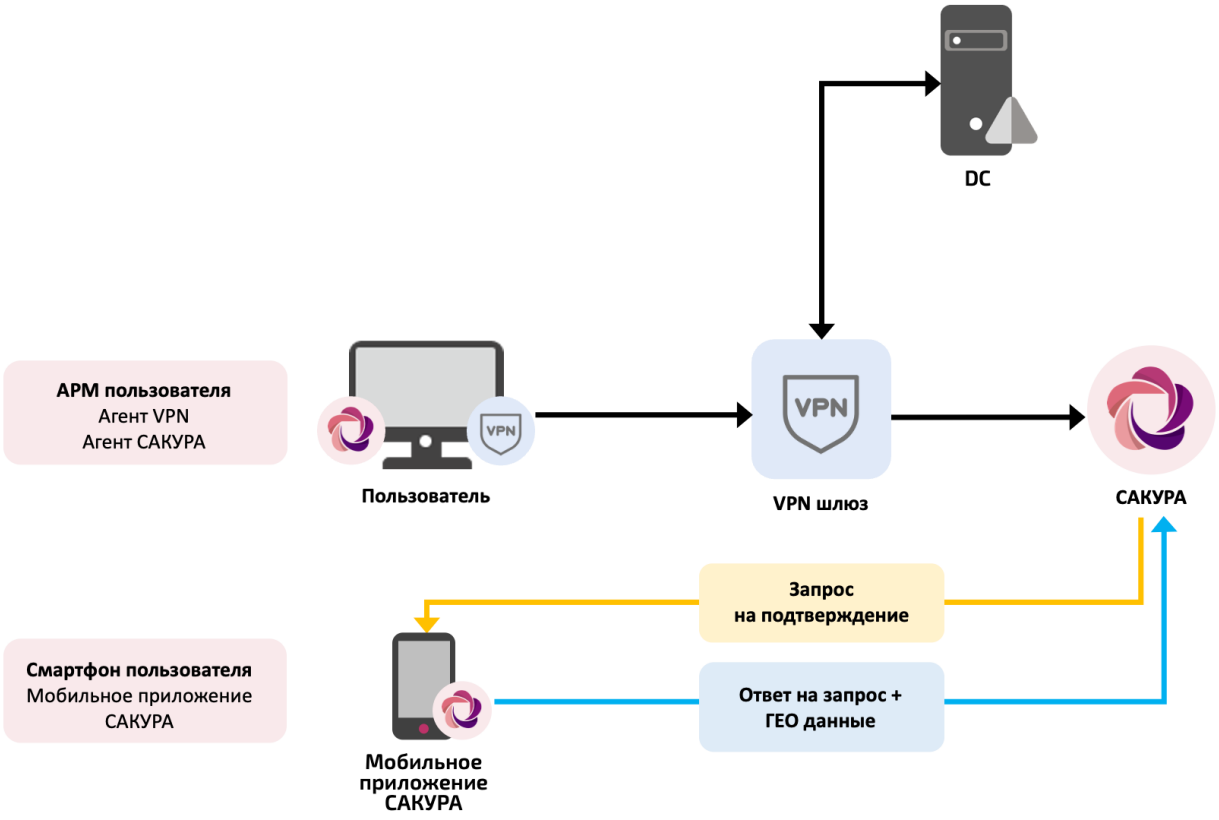




RuStore **Уже можно скачать**

App Store **Уже можно скачать**

Схема подключения к сети предприятия с использованием второго фактора идентификации в виде мобильного приложения САКУРА



1. Пользователь инициирует VPN соединение с VPN шлюзом передавая логин/пароль Домена (DC)

2. VPN Шлюз сверяет логин/пароль пользователя на DC. VPN Шлюз делает запрос на сервер САКУРА, в запросе указывается логин пользователя

3. Сервер САКУРА сопоставляет логин пользователя с идентификатором пользователя в Мобильном приложении САКУРА. Сервер САКУРА отправляет запрос на подтверждение факта о подключении к VPN в Мобильное приложение САКУРА

4. Пользователь получает уведомление о подключении в Мобильном приложении САКУРА с возможностью подтвердить или отклонить подключение

5. Ответ пользователя поступает на сервер САКУРА

6. Сервер САКУРА отвечает на запрос о подключении пользователя к VPN Шлюзу в зависимости от ответа пользователя

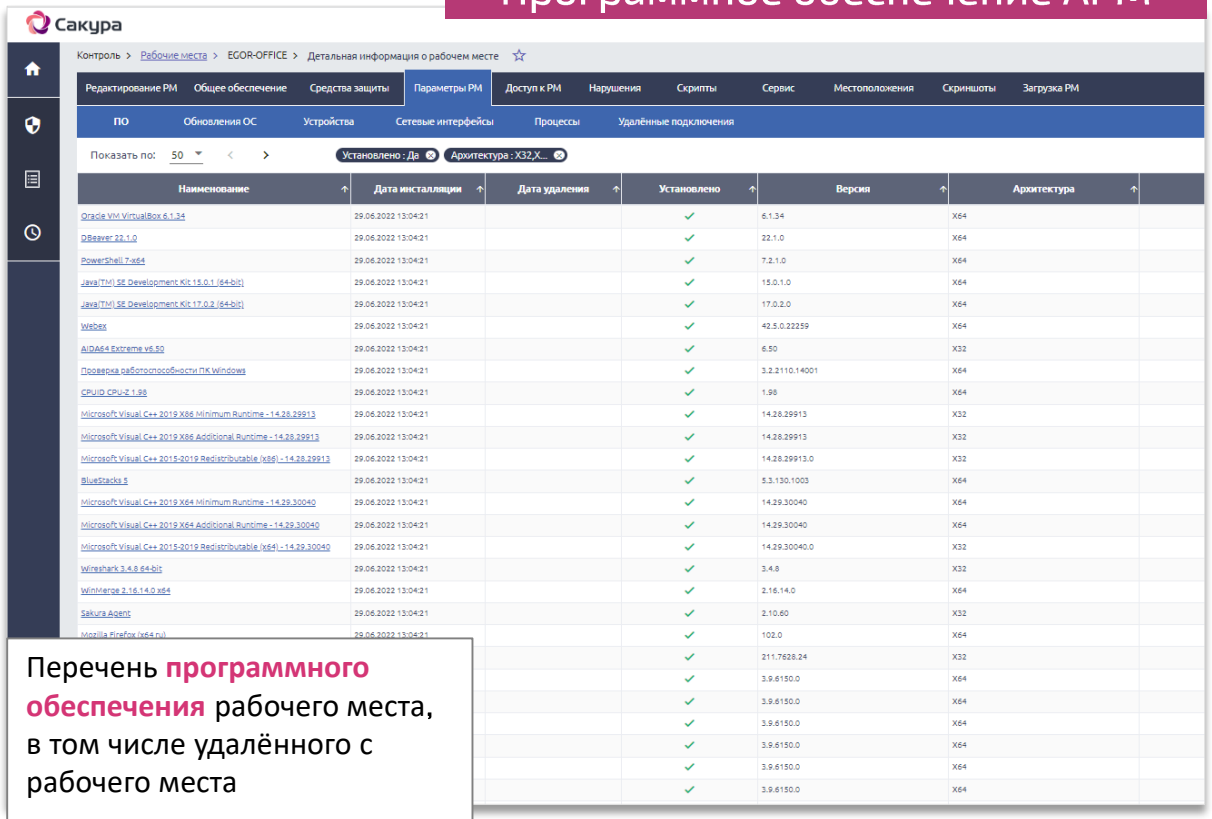
7. VPN Шлюз на основании ответа Сервера САКУРА:

- устанавливает VPN соединение и разрешает доступ Пользователю во внутреннюю сеть,
- или не устанавливает VPN соединение и возвращает пользователя на этап ввода логина/пароля в Агенте VPN

Инвентаризация

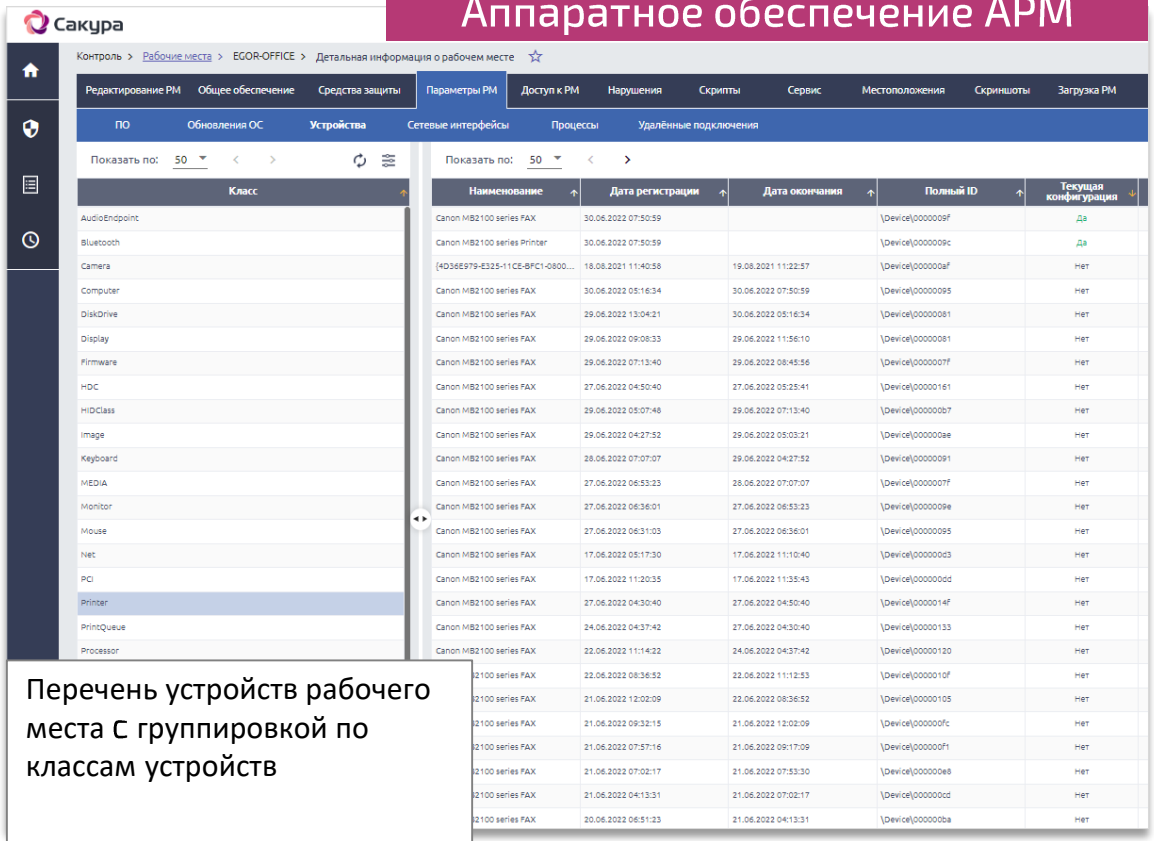
- Сбор информации об используемом аппаратном и программном обеспечении
- Статистика загрузки рабочих мест и ресурсоемких приложений
- Ведение истории изменений состава рабочих мест

Программное обеспечение АРМ



Перечень **программного обеспечения** рабочего места, в том числе удалённого с рабочего места

Аппаратное обеспечение АРМ

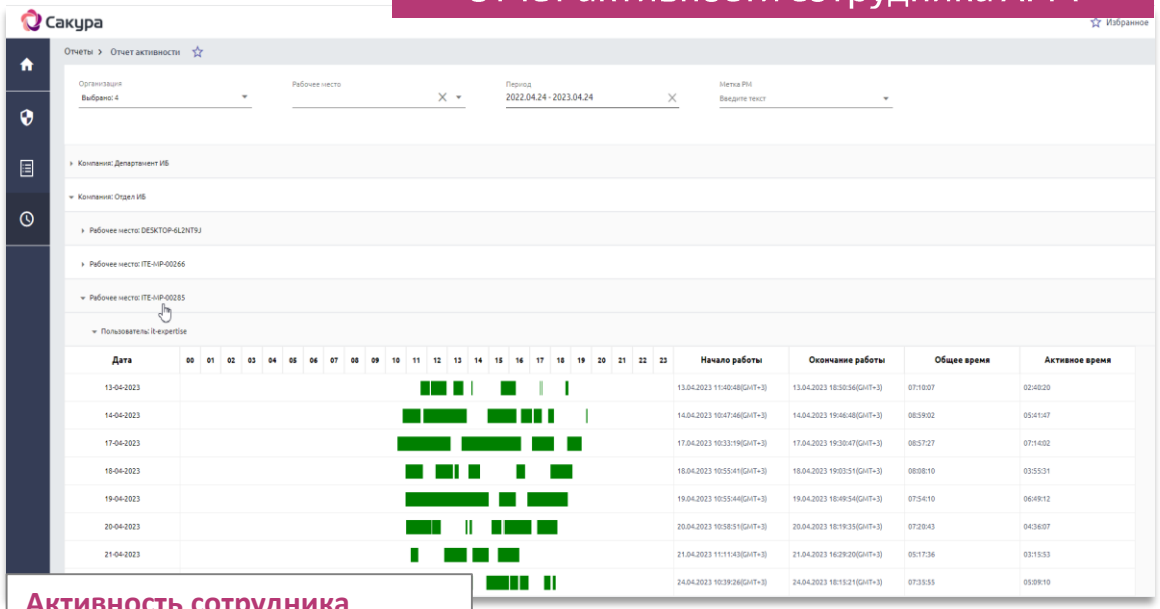


Перечень устройств рабочего места С группировкой по классам устройств

Учет рабочего времени

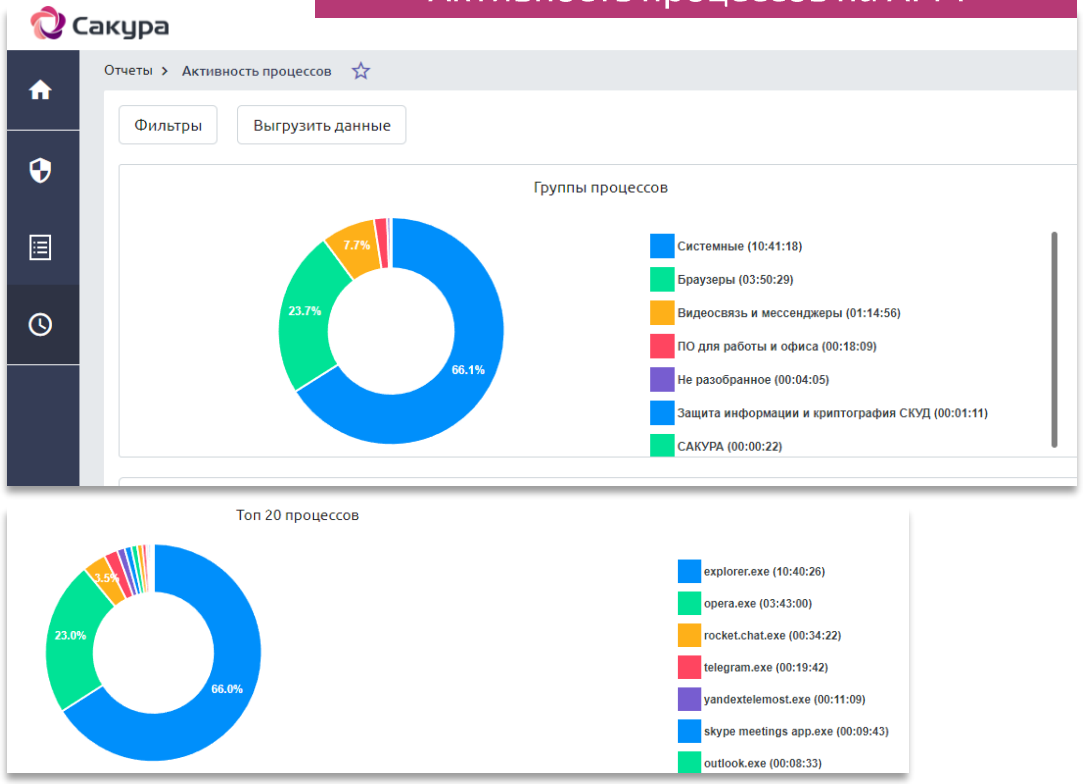
- Контроль деятельности пользователей
- Статистика посещенных сайтов
- Получение информации по рабочему времени

Отчет активности сотрудника АРМ



Активность сотрудника
на рабочем месте в заданный период времени

Активность процессов на АРМ



Контроль работы пользователей

Сакура

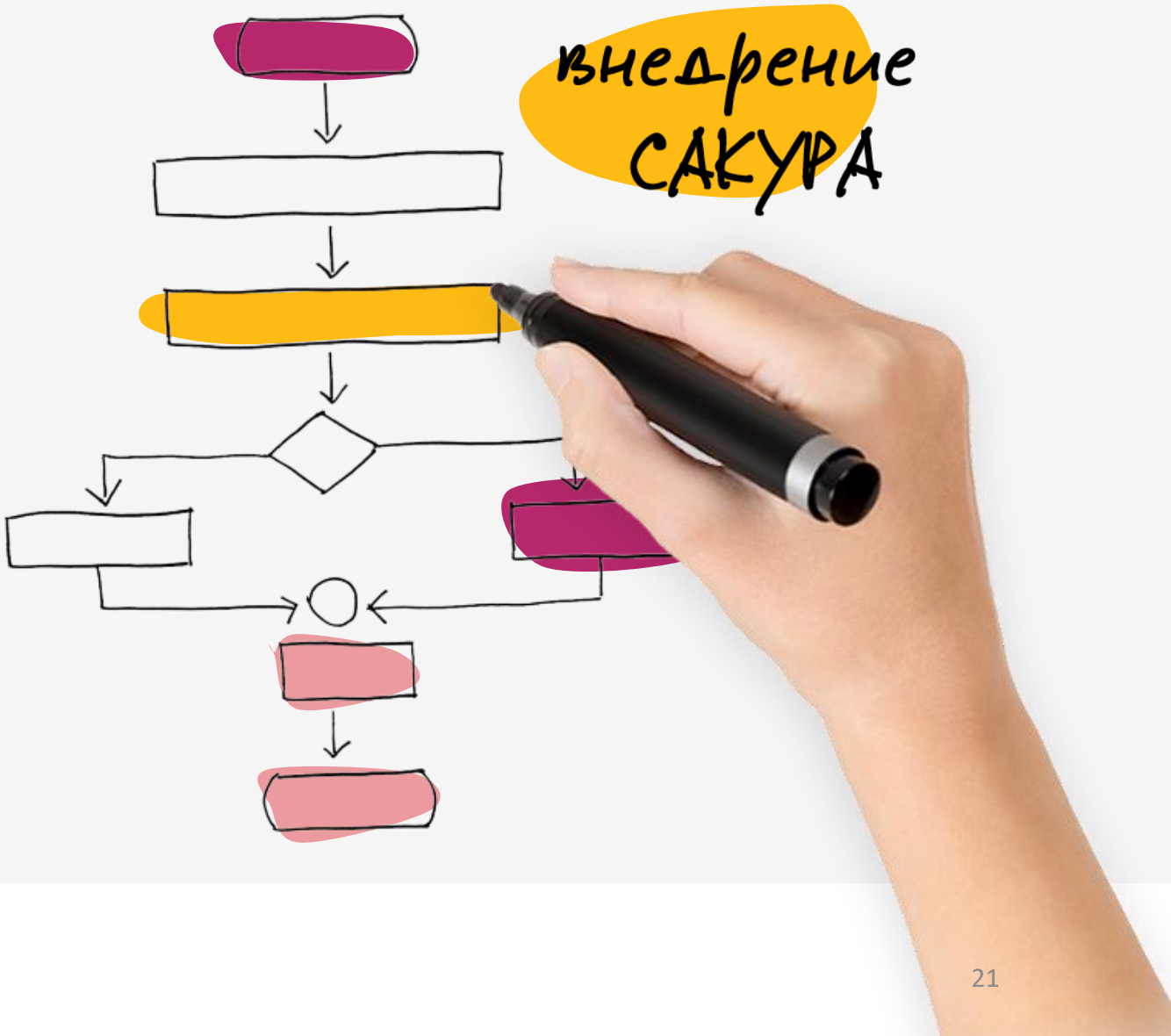
САКУРА позволяет контролировать следующие параметры работы пользователей:

- Время начала и окончания работы пользователя
- Используемые приложения и процессы
- Периоды активной работы и неактивности
- Способ подключения к рабочему месту (локальный/удаленный)
- Географическое местоположение рабочих мест

САКУРА может:

- Выполнять «скриншоты» экрана по таймеру или при наступлении подозрительного события
- Уведомлять пользователя (если необходимо) о том, что его действия нарушают правила использования рабочего места
- Обеспечивать необходимый уровень информационной безопасности на рабочем месте, контролируя целостность среды ИБ и compliance рабочего места
- Интегрироваться с любыми аналитическими инструментами для проведения дополнительного анализа

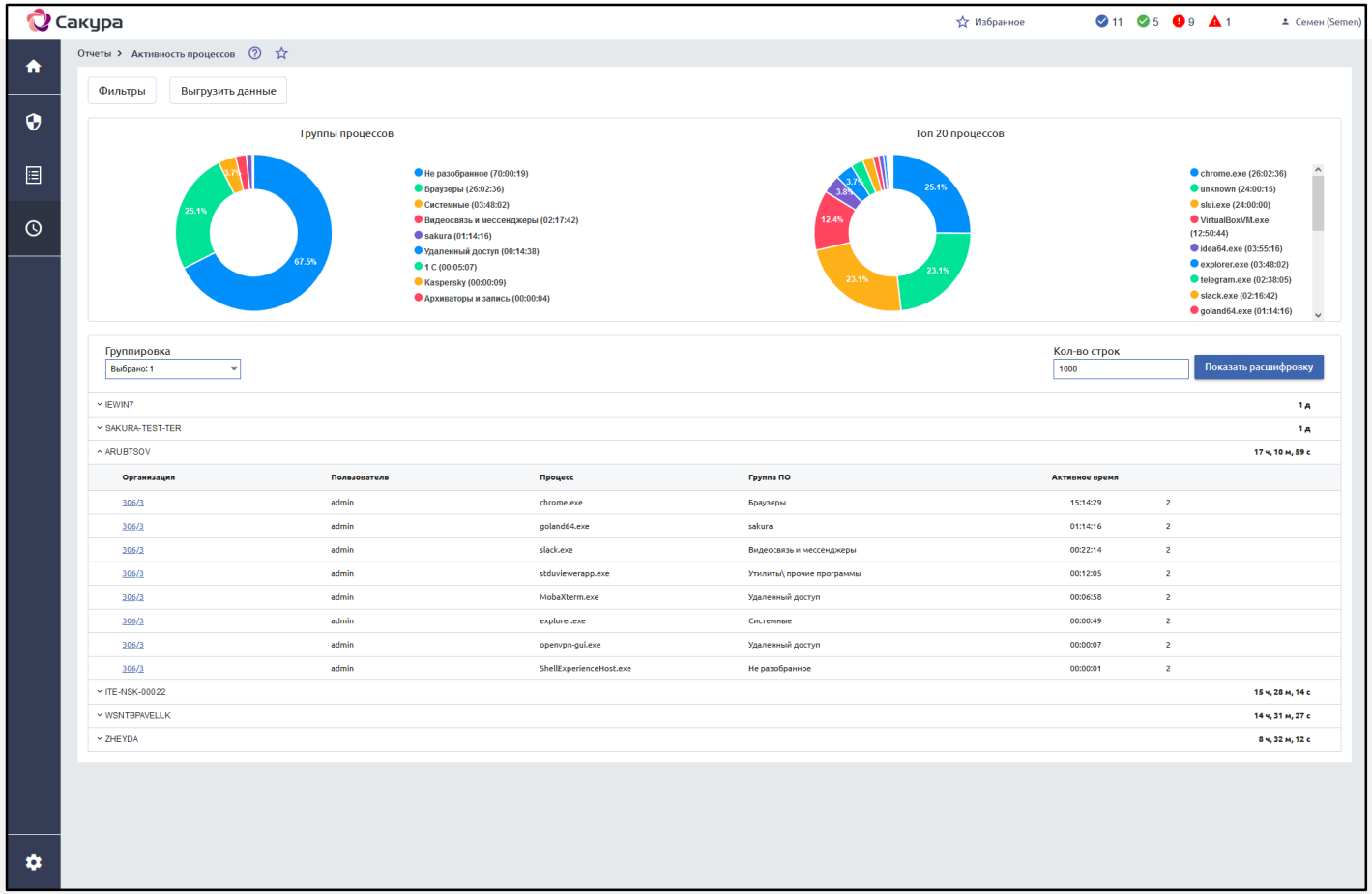
Проектные внедрения



© 2024 ИТ-Экспертиза. Все права защищены.

Госкорпорация «Ростех»
Более 30 000 мест

Комплекс САКУРА позволяет собирать и анализировать информацию об используемых приложениях в различных разрезах от организационных единиц до пользователей или процессов



Безопасность

Проверка комплаенса безопасности

Контроль и управление доступами к корпоративным ресурсам

Контроль используемого программного обеспечения

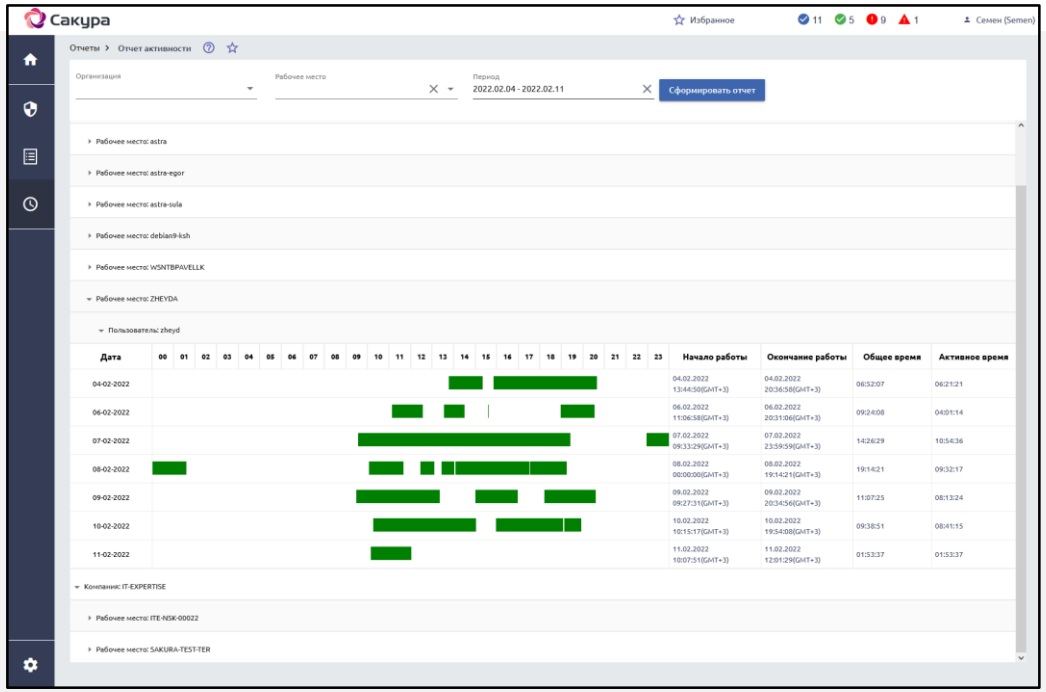
Сбор и анализ информации об используемых приложениях

Выявление случаев нецелевого использования ПК

Анализ отклонений от базового сценария работы пользователей

АО «КБП имени А.Г.Шипунова» 6000 АРМ

САКУРА может строить наглядные **графики работы пользователей** с возможностью детализации каждого дня или интервала работы по используемым программам

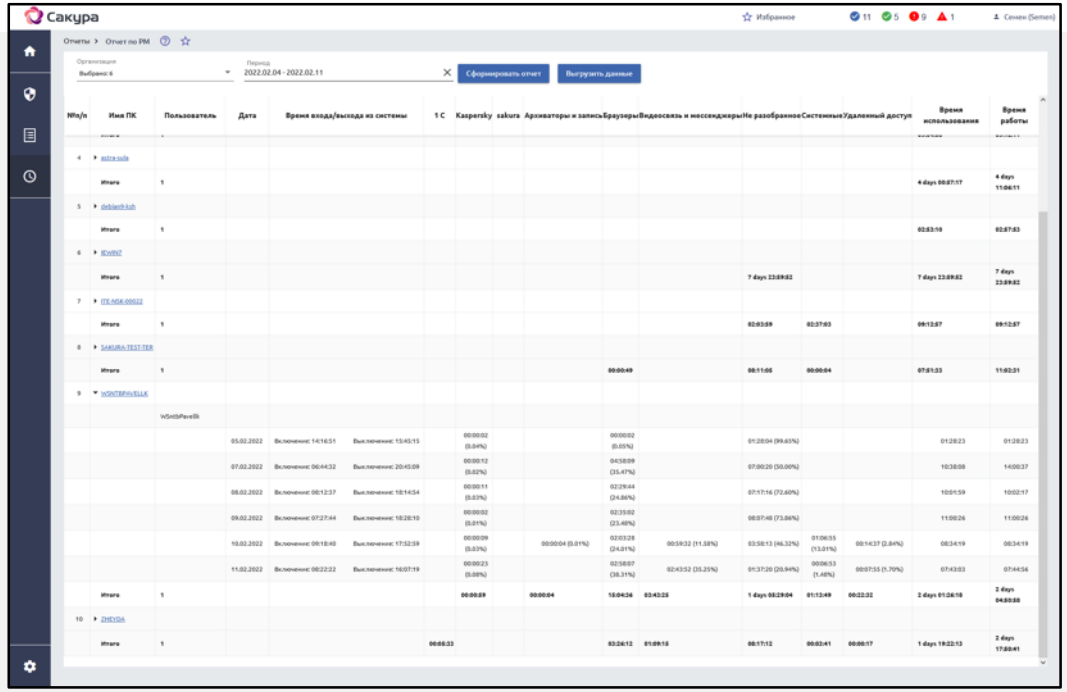


Отчет по активности пользователей

Контроль графика работы сотрудников

Анализ загрузки сотрудников в любых временных разрезах

САКУРА дает возможность **автоматического формирования рабочих табелей** с возможностью доработки формы отчета под внутренние требования

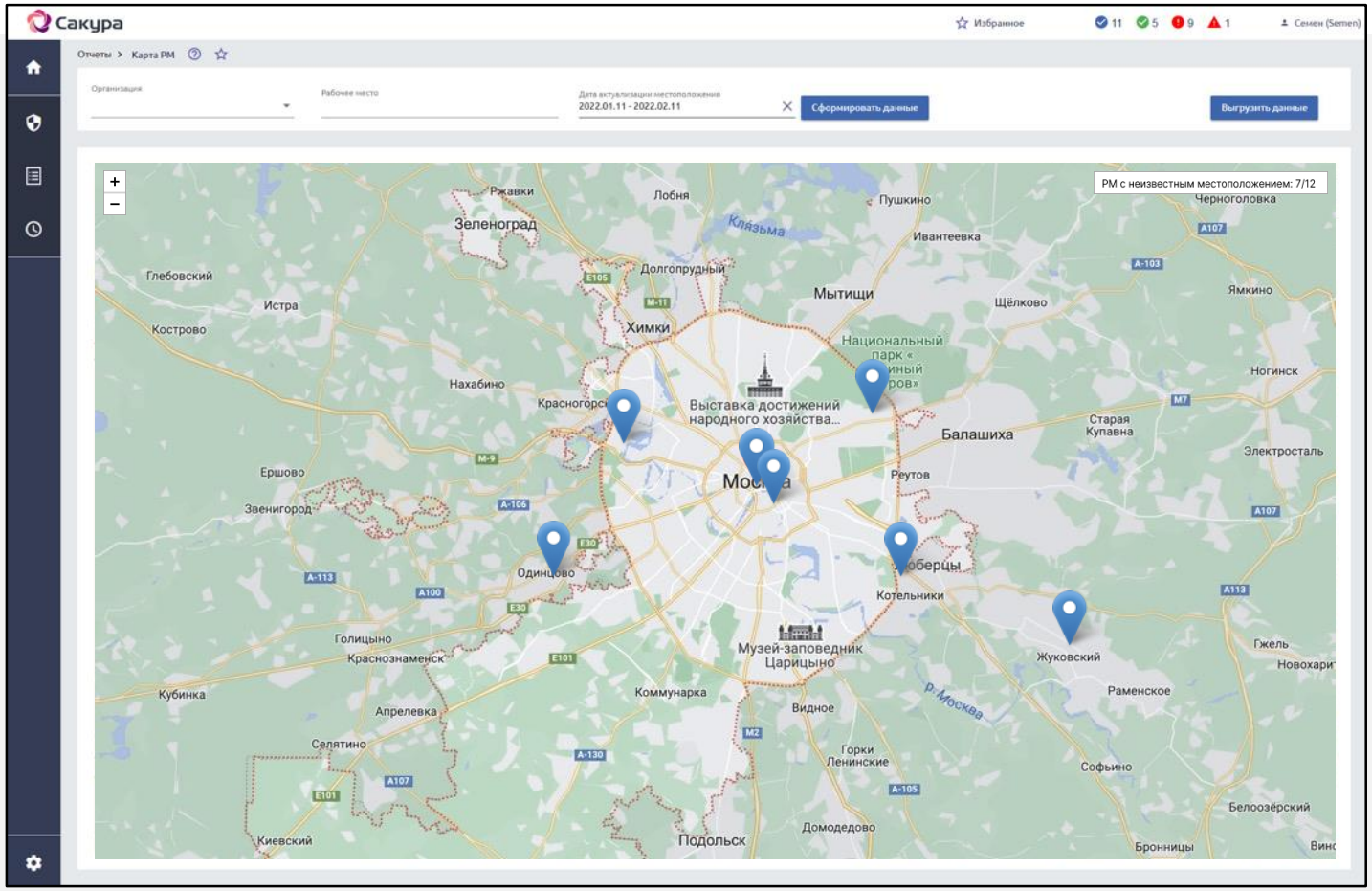


Табель работы пользователей

Формирование рабочих табелей сотрудников

Контроль «типового рабочего дня» сотрудников со стороны руководителей и отдела персонала

ДИТ города Москвы
Более 9000 АРМ



Безопасность

Проверка комплаенса безопасности
Контроль и управление доступами к корпоративным ресурсам

Местоположение рабочих мест

Контроль местоположения мобильной офисной техники

Контроль местоположения сотрудников

Ограничение подключений
по местоположению источника

САКУРА контролирует местоположение как офисных, так и удаленных рабочих мест, и помогает предотвратить несанкционированные подключения или перемещения рабочей техники

Лицензирование

Сакура

Основная поставка:

Серверный компонент

по количеству РМ
лицензия на год + пролонгация

Агентский компонент

по количеству РМ,
лицензия на год + пролонгация

Техническая поддержка

базовая входит в поставку / **расширенная** приобретается отдельно
(по желанию клиента)

Дополнительные модули:

Лицензия на Модуль двухфакторной аутентификации

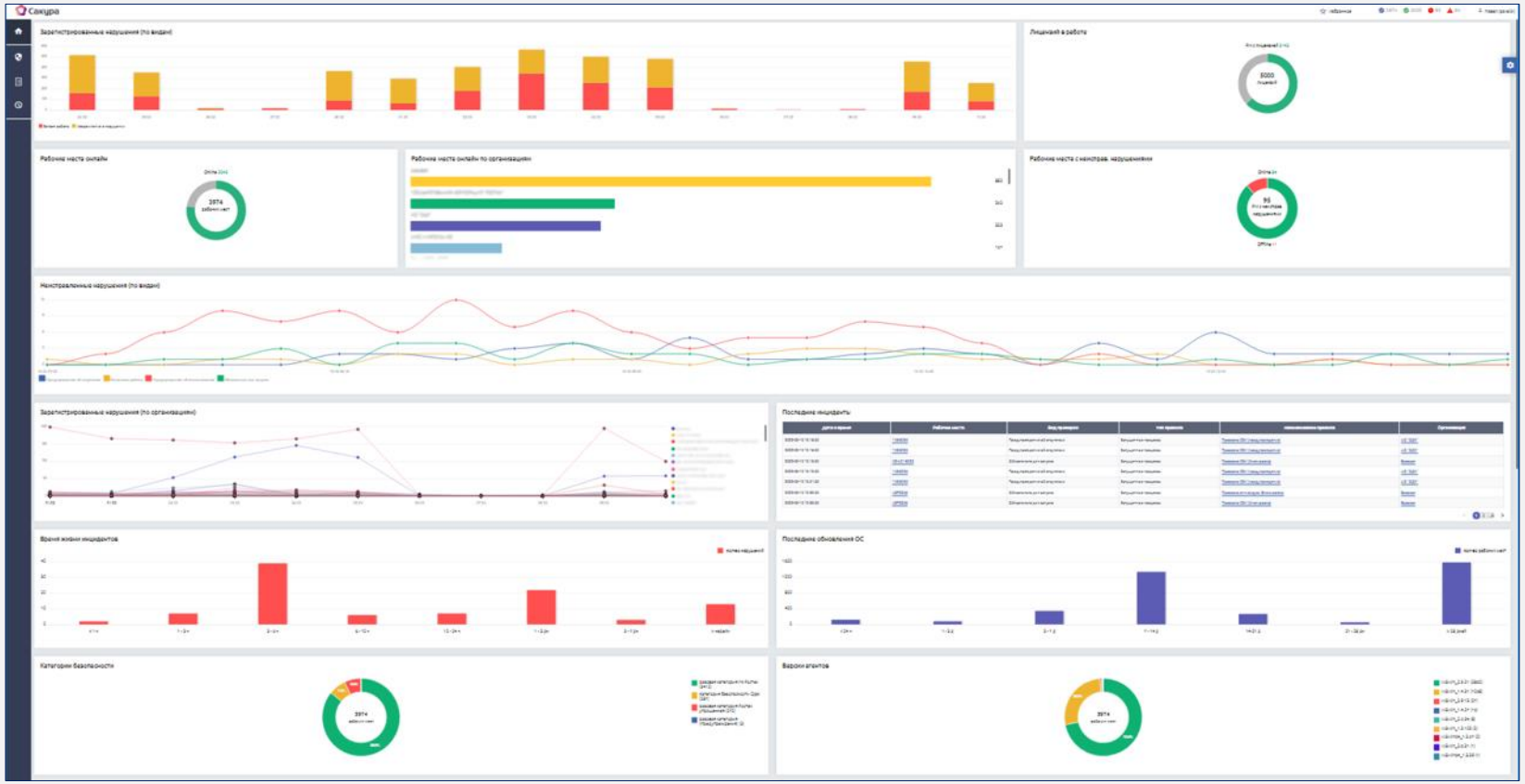
для ПО «САКУРА-Агент»

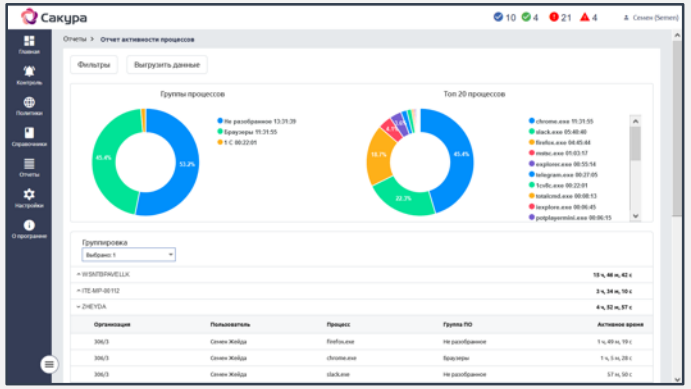
по количеству РМ
лицензия на год + пролонгация

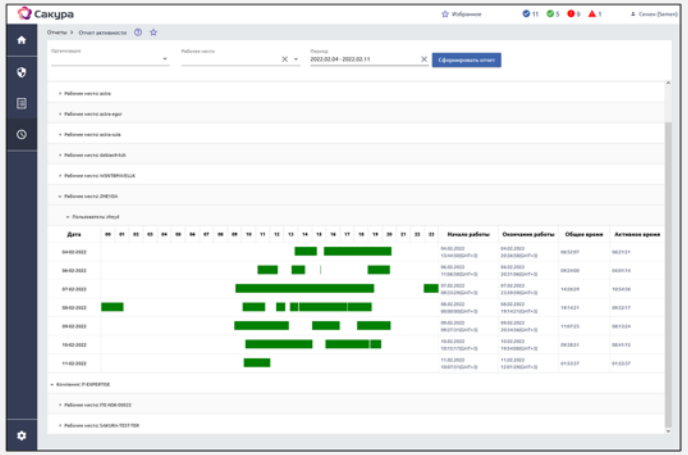
Расчёт стоимости приобретения комплекса предоставляется по вашему запросу

Интерфейс комплекса САКУРА

Наглядные интерактивные дашборды позволяют руководителю и офицеру безопасности получать информацию в режиме реального времени.







Применяя комплекс САКУРА, вы получите

Сакура

- Выполнение **требований государственных регуляторов (ФСТЭК и т.д.)**
- Снижение количества инцидентов информационной безопасности **более чем в 10 раз**
- Возможность использования **двухфакторной аутентификации**
- Полную информацию об **инфраструктуре и ПО**, используемых в компании
- Полную информацию о загруженности сотрудников и эффективности **использования** ими **рабочего времени**
- Контроль **соответствия** рабочих мест **политикам безопасности** независимо от их расположения и архитектуры
- Управление **доступом к приложениям на платформе 1С:Предприятие** согласно требованиям комплаенса и безопасности

Дорожная карта внедрения САКУРА

1. Свяжитесь с нами и **закажите дистрибутив** для пилотного проекта
2. Проведите **пилотный проект** с полным сопровождением силами наших экспертов
3. Получите **расчет и коммерческое предложение** на необходимое вам количество серверных и клиентских лицензий
4. Заключите **договор** и получите **консультации** по внедрению системы
5. Оплатите заказ и получите комплекс САКУРА **для контроля комплаенса** безопасности и **управления доступом**

Контакты

Получите бесплатную консультацию по возможностям и применению комплекса САКУРА

САЙТ
it-expertise.ru

EMAIL
info@it-expertise.ru

ТЕЛЕФОН
+7 499 450 28 86

АДРЕС
119435 г. Москва, ул. Малая Пироговская, 16