

Возможности комплекса САКУРА для обеспечения информационной безопасности и контроля рабочих мест

Обзор продукта



О компании ИТ-Экспертиза



НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ:

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

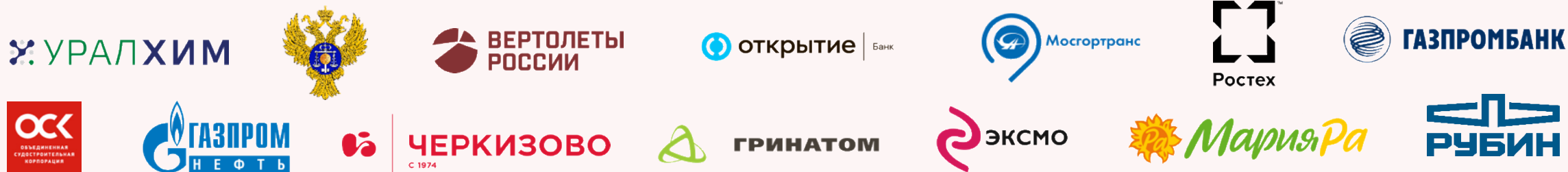
Консалтинг по информационной безопасности — аудит и разработка рекомендаций по совершенствованию систем информационной безопасности (ГИС, КИИ, персональные данные), подготовка необходимой документации для регуляторов.

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



Контроль доступа
к корпоративным
ресурсам



Двухфакторную
аутентификацию



Соответствие удаленных рабочих
мест внутренним политикам
безопасности



Инвентаризацию
оборудования и ПО



Мониторинг действий
сотрудника на рабочем месте

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 или Fortigate после ухода зарубежных вендоров с российского рынка

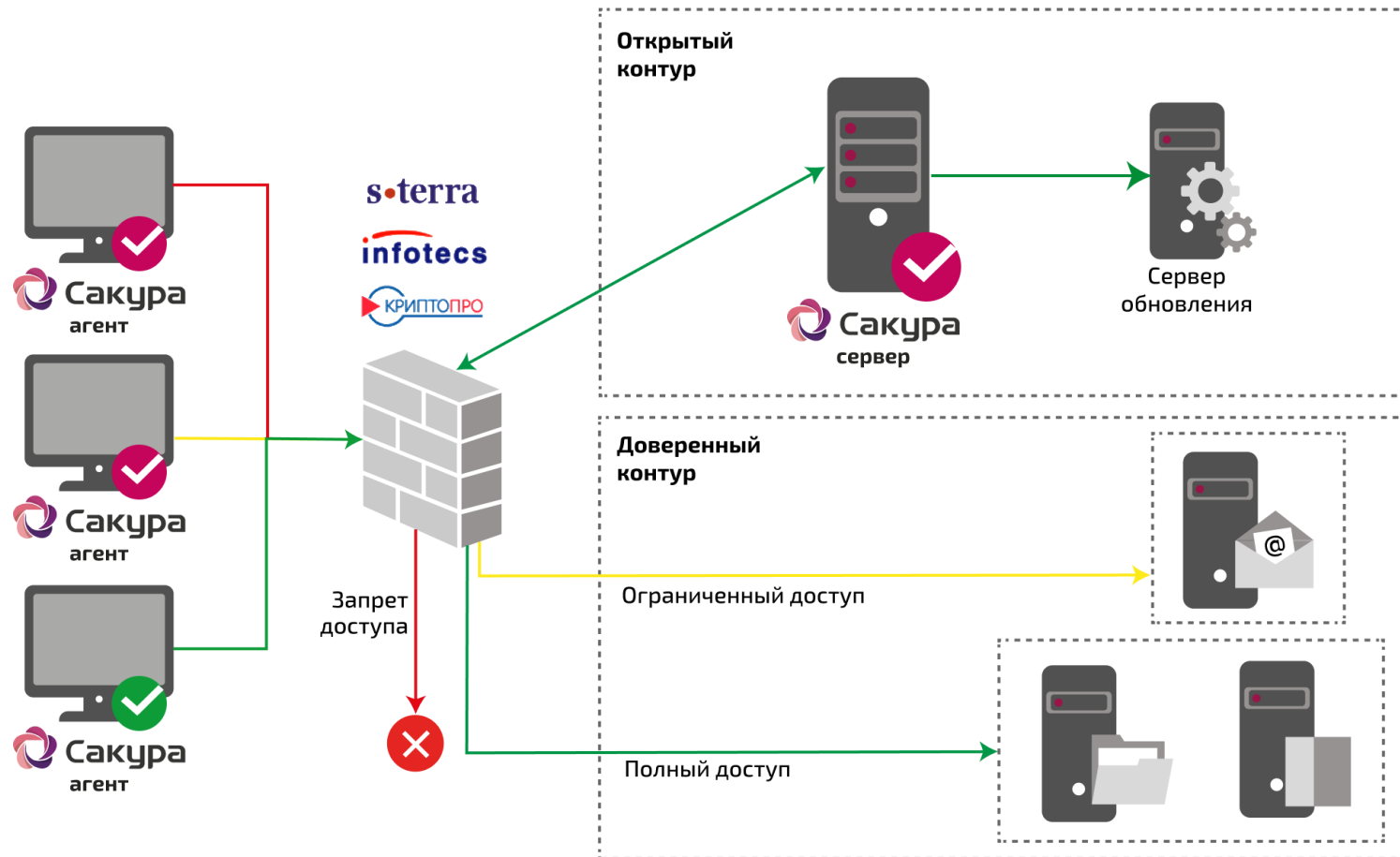


Комплекс САКУРА **интегрирован с российскими VPN решениями**, такими как КриптоПро NGate, ViPNet, S-Terra, что позволяет построить инфраструктуру доступа с нулевым доверием (Zero Trust Network Access) полностью на отечественном ПО и оборудовании



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 компоненты

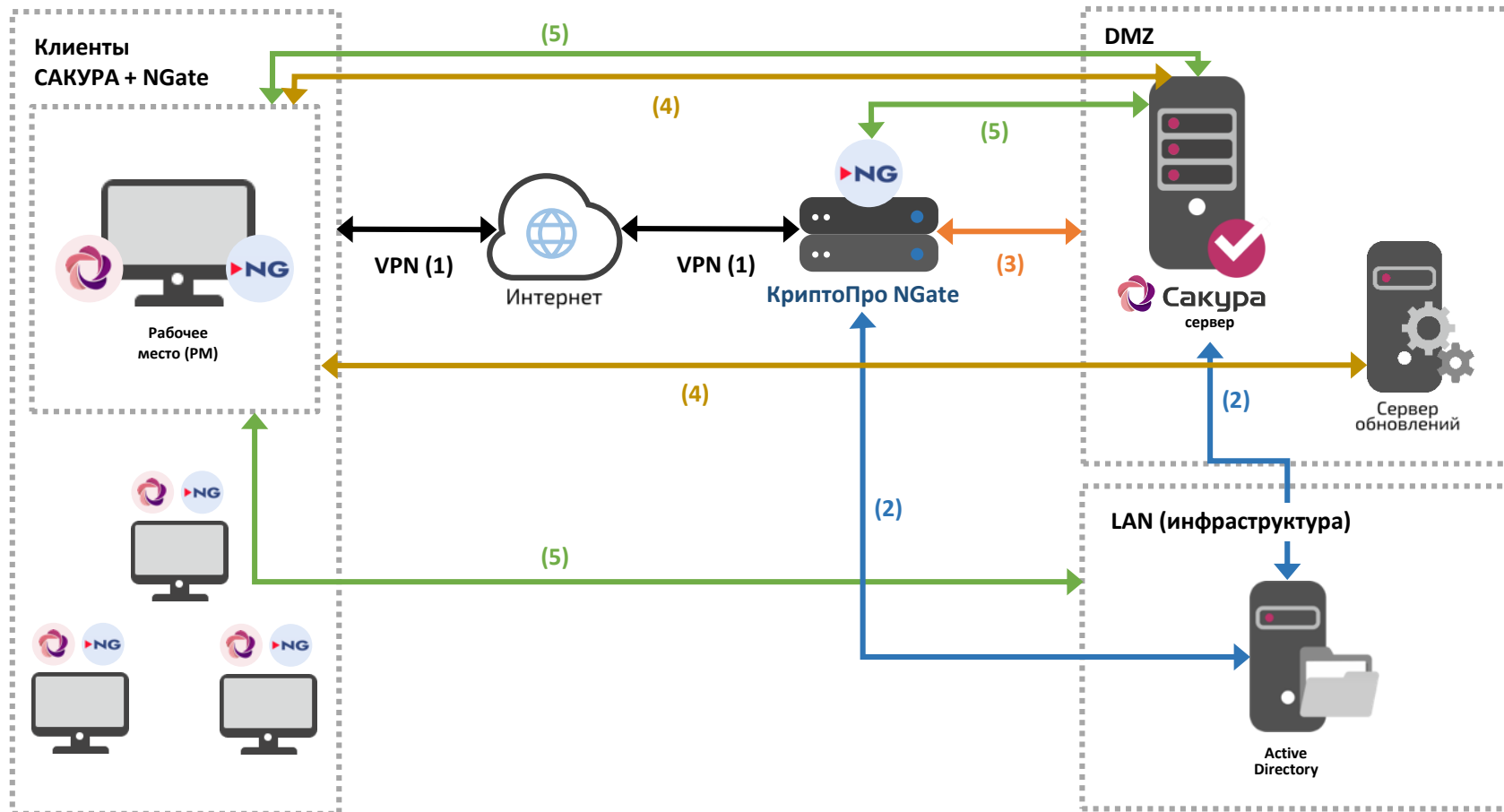
Совместима с:

- ✓ Windows
- ✓ Linux
- ✓ MacOS

Интегрируется с отечественными VPN:

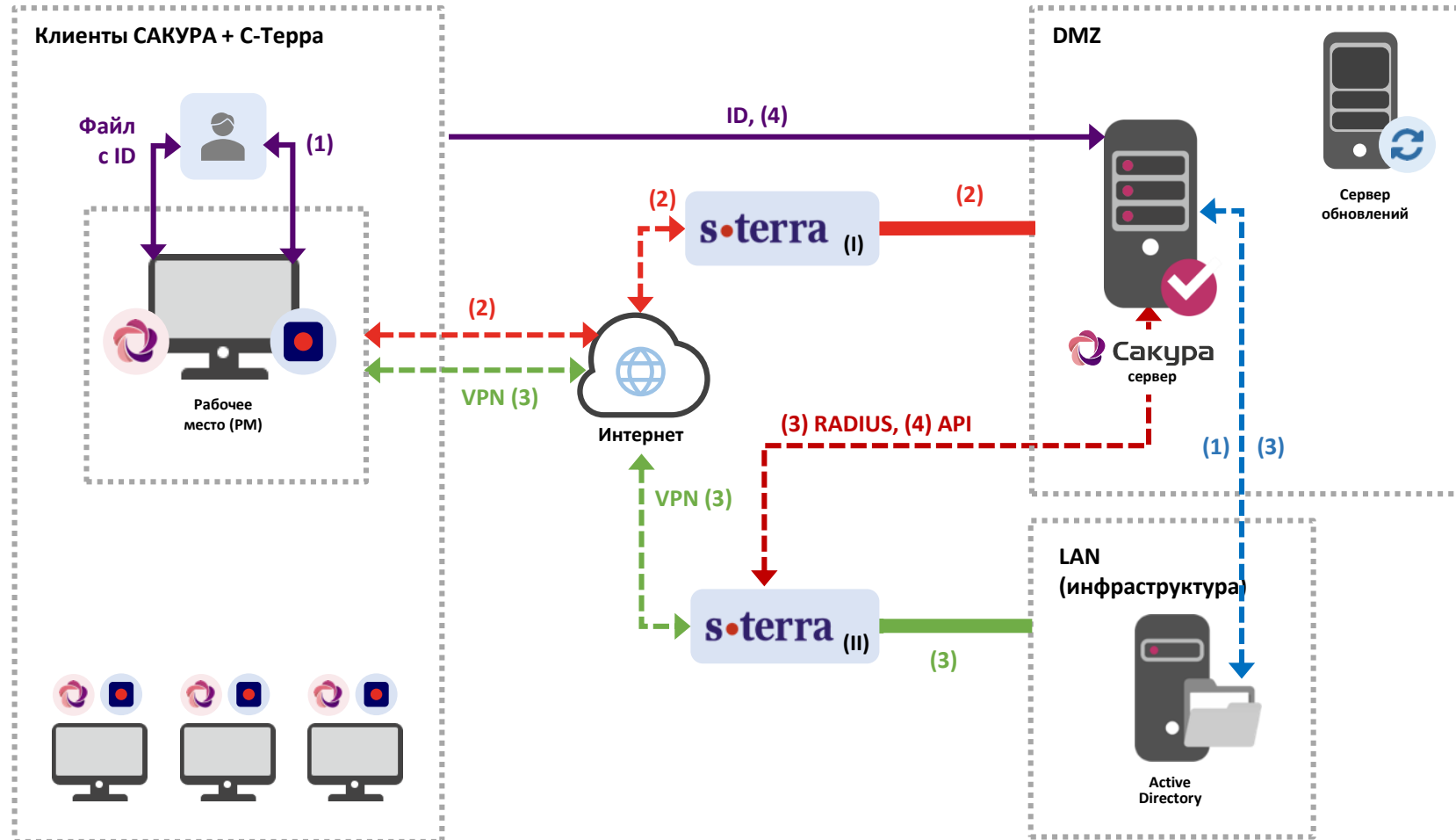


Интеграции программного комплекса САКУРА и шлюза NGate с клиентской инфраструктурой



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 PM, 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 с клиентской инфраструктурой



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

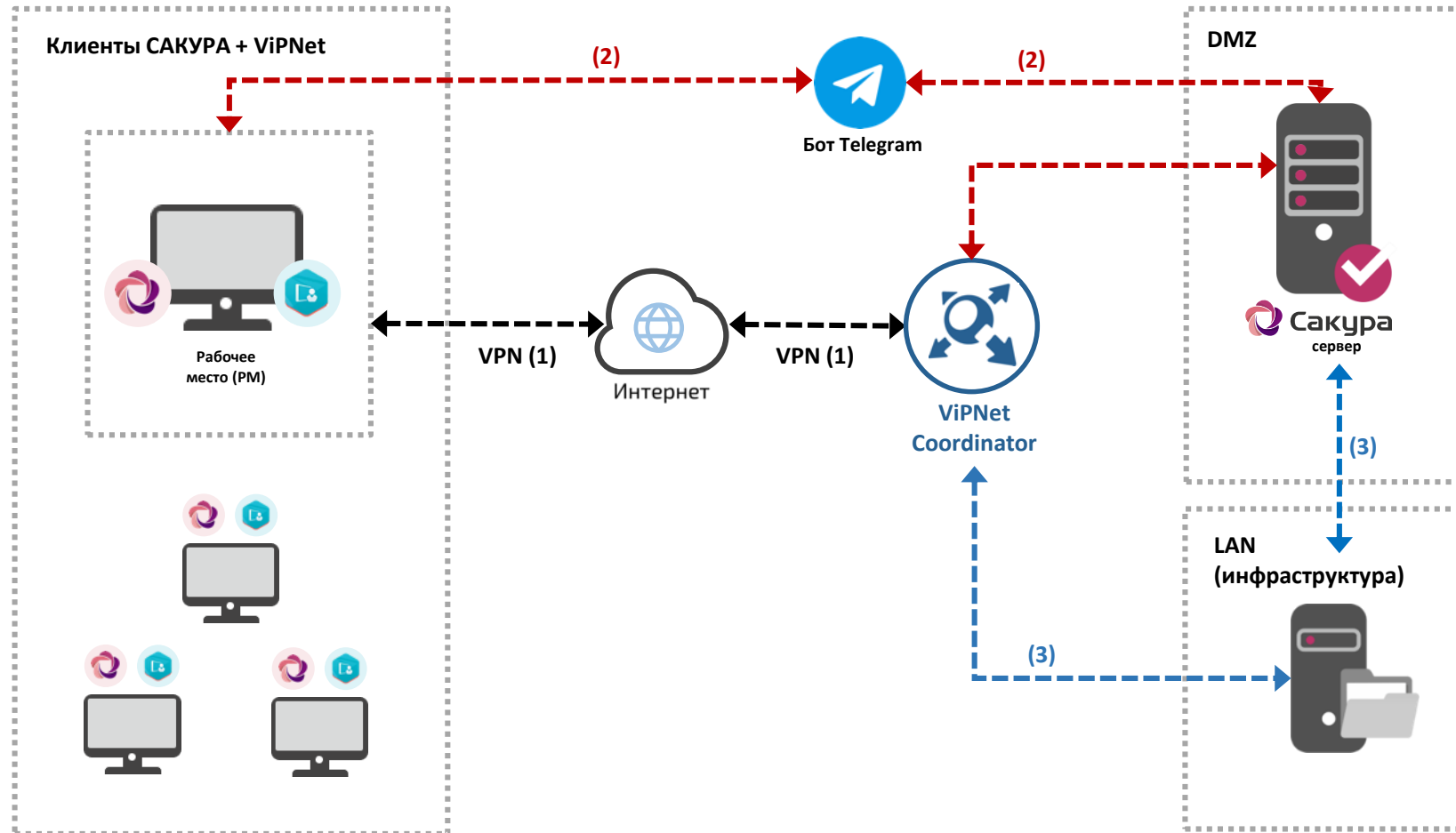
2. Данные об аутентификации пользователя передаются на Сервер С-Терра (I). Строится VPN тоннель (2).

3. Клиент С-Терра периодически посылает запрос на подключение к Серверу С-Терра (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 PM **COMPLIANT**, Он по RADIUS дает разрешение на Сервер С-Терра (II), строится VPN тоннель (3) для доступа PM к LAN.

В случае изменения состояния APM:

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 Сервере С-Терра (II) в LAN. VPN Тоннель (3) сброшен.

Двухфакторная авторизация (2FA) в схеме интеграции САКУРА-ViPNet



1. Клиентское рабочее место подключается по VPN к шлюзу ViPNet Coordinator, где получает доступ в DMZ к серверу САКУРА
2. В случае применения 2FA, шлюз ViPNet Coordinator подает запрос на Сервер САКУРА через **бота Telegram** отправляет пользователю запрос на подтверждение доступа
3. 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)

Функциональность

- ✓ Безопасность
- ✓ Инвентаризация
- ✓ Контроль активности сотрудников



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 **около 200 параметров безопасности**.
- По результатам проверки может быть **ограничен доступ к корпоративным информационным системам** и/или направлены уведомления офицерам информационной безопасности

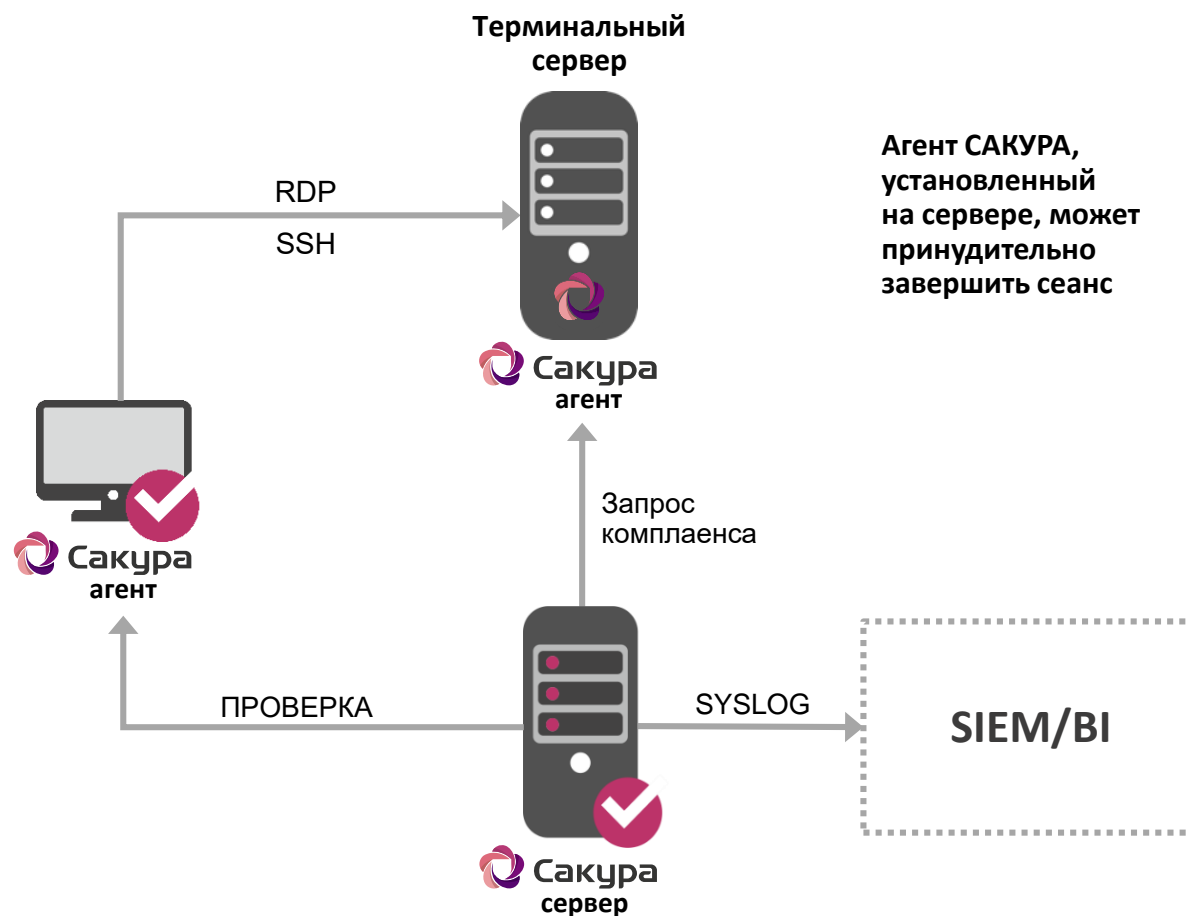


Возможность формирования собственных правил контроля с использованием скриптов PowerShell и Bash

Автоматическое реагирование на инциденты безопасности

Безопасность: Контроль доступа

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



- Разрешать подключения по RDP/SSH 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)

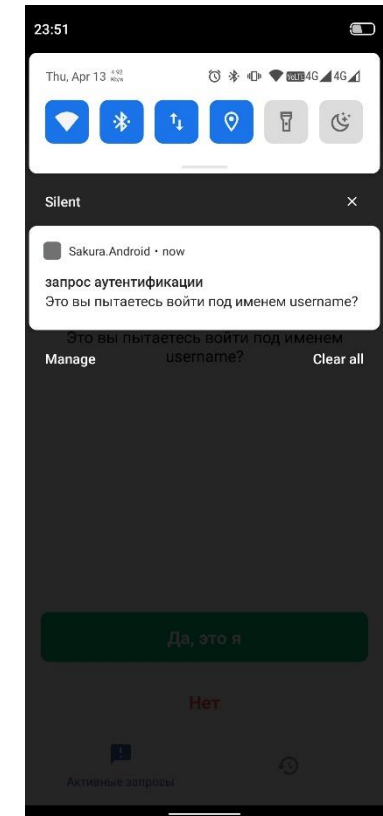
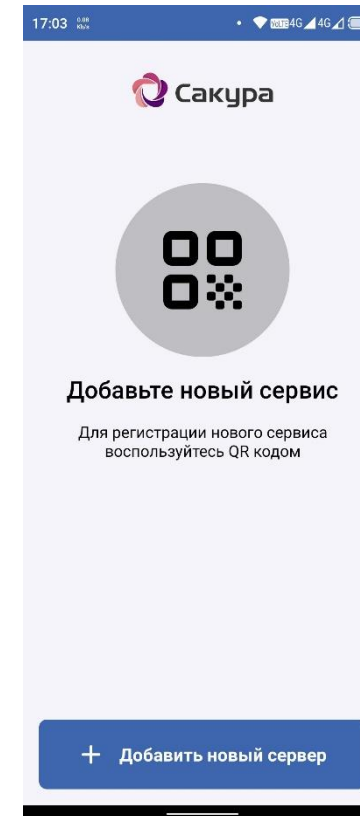
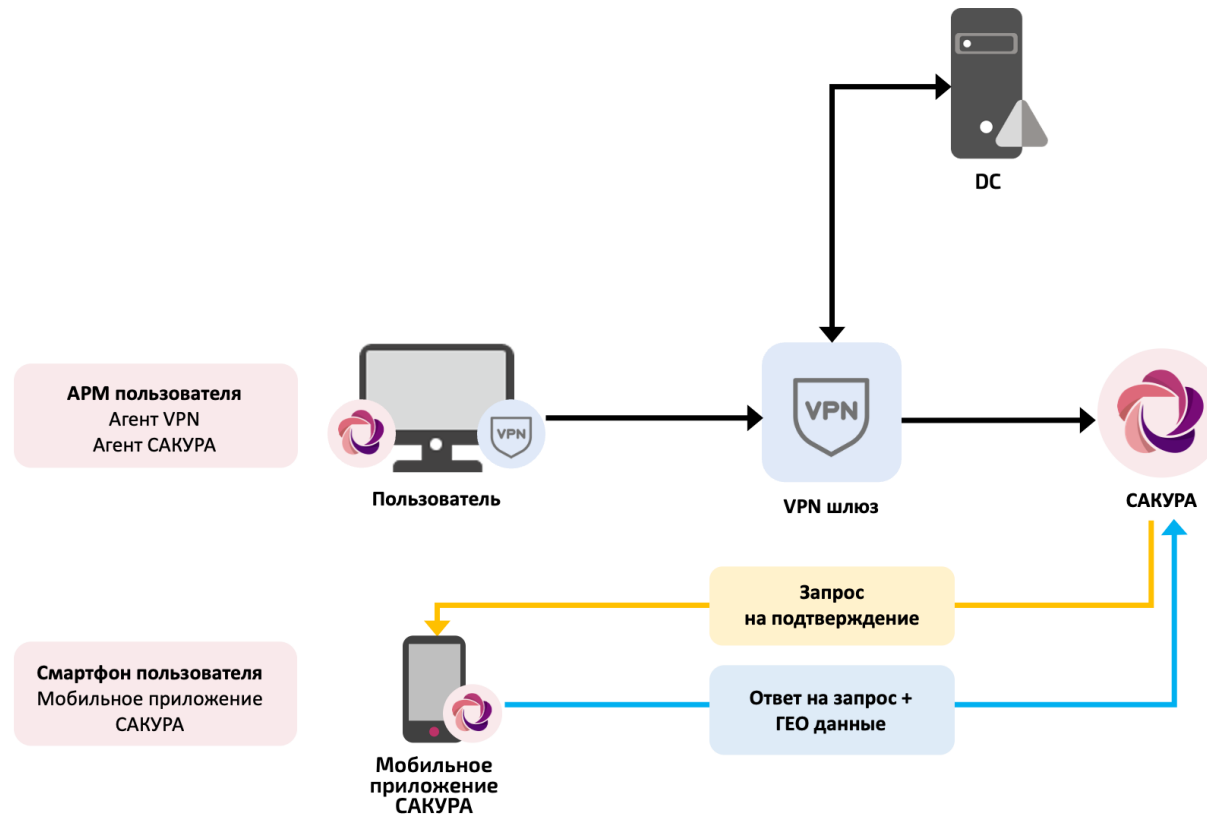


Схема подключения к сети предприятия с использованием второго фактора идентификации в виде мобильного приложения САКУРА

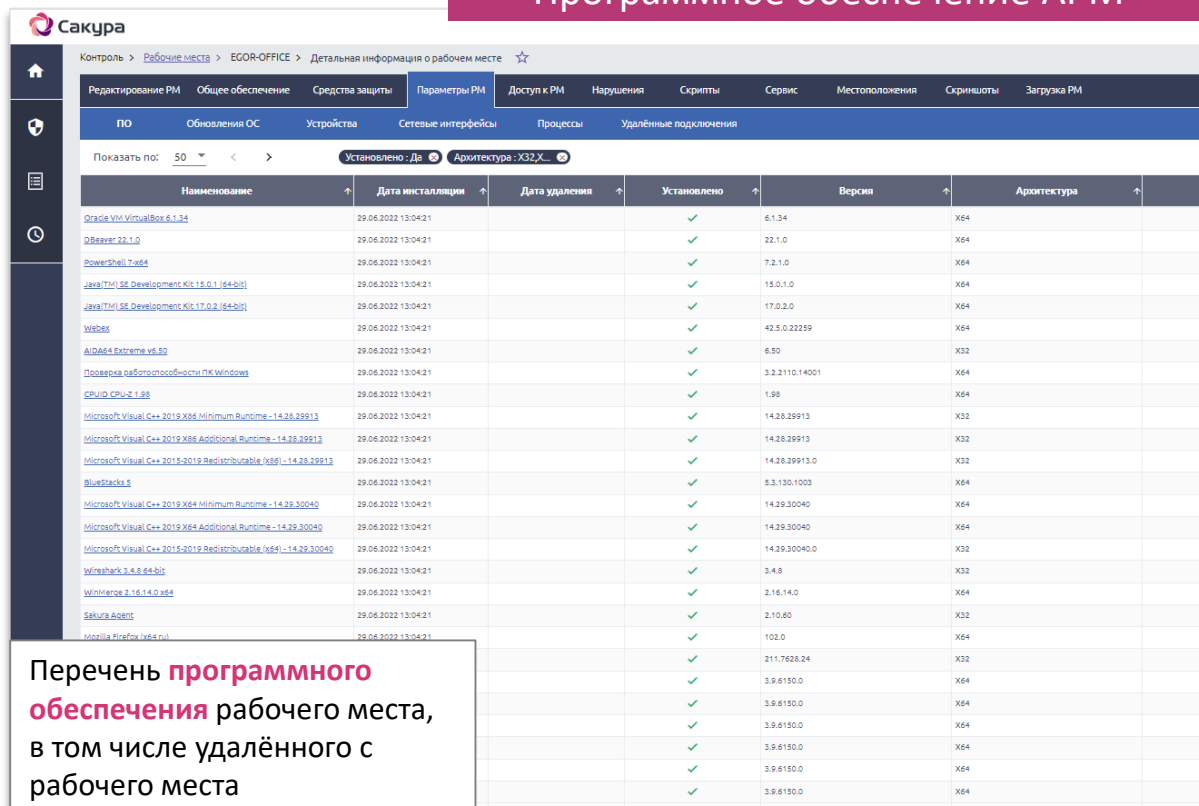


1. Пользователь инициирует VPN соединение с VPN шлюзом передавая логин/пароль Домена (DC)
2. VPN Шлюз сверяет логин/пароль пользователя на DC. VPN Шлюз делает запрос на сервер САКУРА, в запросе указывается логин пользователя
3. Сервер САКУРА сопоставляет логин пользователя с идентификатором пользователя 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

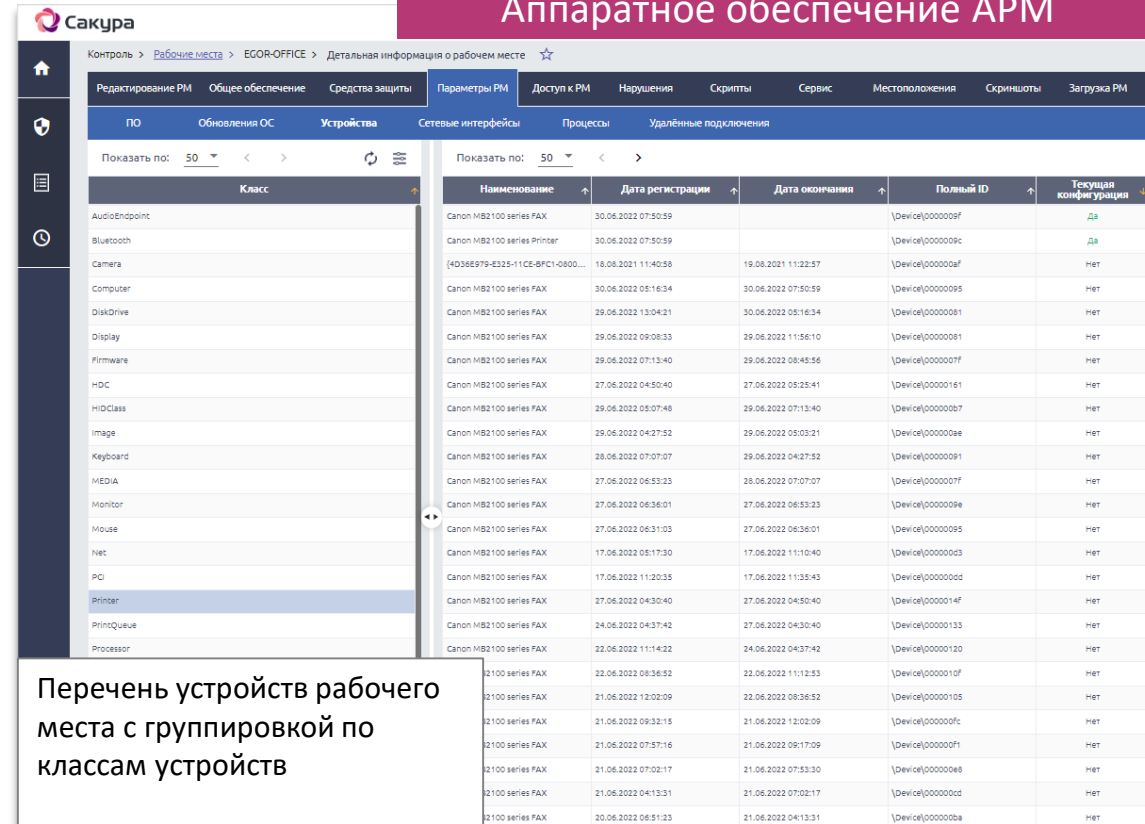
Программное обеспечение АРМ



Наименование	Дата инсталляции	Дата удаления	Установлено	Версия	Архитектура
Oracle VM VirtualBox 6.1.34	29.06.2022 13:04:21		✓	6.1.34	X64
PowerShell 7.x64	29.06.2022 13:04:21		✓	7.2.1.0	X64
Java(TM) SE Development Kit 15.0.1 (64-bit)	29.06.2022 13:04:21		✓	15.0.1.0	X64
Java(TM) SE Development Kit 17.0.2 (64-bit)	29.06.2022 13:04:21		✓	17.0.2.0	X64
Webex	29.06.2022 13:04:21		✓	42.5.0.22259	X64
АИДА64 Эксперте v6.50	29.06.2022 13:04:21		✓	6.50	X32
Проверка работоспособности ПК Windows	29.06.2022 13:04:21		✓	3.2.2110.14001	X64
CPUPID CPU-Z 1.98	29.06.2022 13:04:21		✓	1.98	X64
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.29.32913	29.06.2022 13:04:21		✓	14.29.32913	X32
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.29.32913	29.06.2022 13:04:21		✓	14.29.32913	X32
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.29.32913	29.06.2022 13:04:21		✓	14.29.32913.0	X32
BlueStacks 5	29.06.2022 13:04:21		✓	5.3.130.1003	X64
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.29.30040	29.06.2022 13:04:21		✓	14.29.30040	X64
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.29.30040	29.06.2022 13:04:21		✓	14.29.30040	X64
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.29.30040	29.06.2022 13:04:21		✓	14.29.30040.0	X32
WinRAR 6.40.0.64-beta	29.06.2022 13:04:21		✓	6.40	X32
WinMerge 2.16.14.0-rc4	29.06.2022 13:04:21		✓	2.16.14.0	X64
Sakura Agent	29.06.2022 13:04:21		✓	2.10.60	X32
Mozilla Firefox (64-bit)	29.06.2022 13:06:21		✓	102.0	X64
			✓	211.7628.24	X32
			✓	3.9.6150.0	X64
			✓	3.9.6150.0	X64
			✓	3.9.6150.0	X64
			✓	3.9.6150.0	X64
			✓	3.9.6150.0	X64
			✓	3.9.6150.0	X64

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

Аппаратное обеспечение АРМ



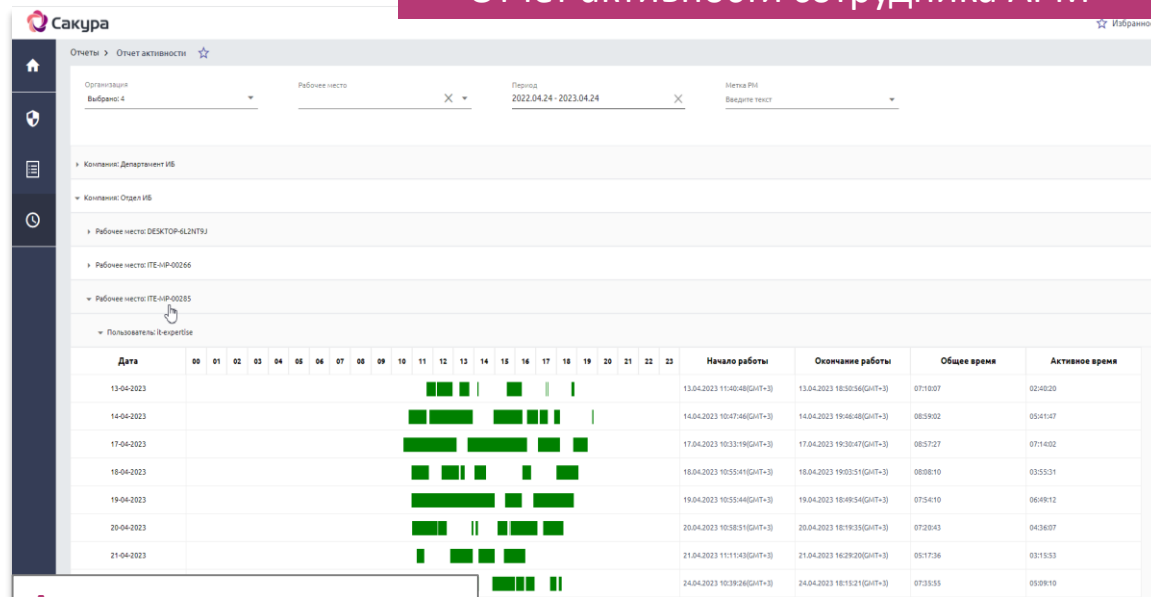
Класс	Наименование	Дата регистрации	Дата окончания	Пользов ID	Текущая конфигурация
AudioEndpoint	Canon MB2100 series FAX	30.06.2022 07:50:59		\\Device\{0000009F}	да
Bluetooth	Canon MB2100 series Printer	30.06.2022 07:50:59		\\Device\{0000009C}	да
Camera	{4D36E979-8325-11CE-8FC1-0800...	18.08.2021 11:40:58	19.08.2021 11:22:57	\\Device\{000000A0}	нет
Computer	Canon MB2100 series FAX	30.06.2022 05:16:34	30.06.2022 07:50:59	\\Device\{00000095}	нет
DiskDrive	Canon MB2100 series FAX	29.06.2022 13:04:21	30.06.2022 05:16:34	\\Device\{00000081}	нет
Display	Canon MB2100 series FAX	29.06.2022 09:08:33	29.06.2022 11:56:10	\\Device\{00000081}	нет
Firmware	Canon MB2100 series FAX	29.06.2022 07:13:40	29.06.2022 08:45:36	\\Device\{00000077}	нет
HDClass	Canon MB2100 series FAX	27.06.2022 04:50:40	27.06.2022 05:25:41	\\Device\{00000161}	нет
HiDClass	Canon MB2100 series FAX	29.06.2022 05:07:48	29.06.2022 07:13:40	\\Device\{000000B7}	нет
Image	Canon MB2100 series FAX	29.06.2022 04:27:52	29.06.2022 05:03:21	\\Device\{000000A8}	нет
Keyboard	Canon MB2100 series FAX	28.06.2022 07:07:07	29.06.2022 04:27:52	\\Device\{00000091}	нет
MEDIA	Canon MB2100 series FAX	28.06.2022 06:53:23	28.06.2022 07:07:07	\\Device\{00000077}	нет
Monitor	Canon MB2100 series FAX	27.06.2022 06:36:01	27.06.2022 06:53:23	\\Device\{00000098}	нет
Mouse	Canon MB2100 series FAX	27.06.2022 06:31:03	27.06.2022 06:36:01	\\Device\{00000095}	нет
Net	Canon MB2100 series FAX	17.06.2022 05:17:30	17.06.2022 11:10:40	\\Device\{000000C3}	нет
PCI	Canon MB2100 series FAX	17.06.2022 11:20:35	17.06.2022 11:35:43	\\Device\{0000000D}	нет
Printer	Canon MB2100 series FAX	27.06.2022 04:30:40	27.06.2022 04:50:40	\\Device\{0000014F}	нет
PrintQueue	Canon MB2100 series FAX	24.06.2022 04:37:42	27.06.2022 04:30:40	\\Device\{00000133}	нет
Processor	Canon MB2100 series FAX	22.06.2022 11:14:22	24.06.2022 04:37:42	\\Device\{00000120}	нет
	2100 series FAX	22.06.2022 08:36:52	22.06.2022 11:12:53	\\Device\{0000010F}	нет
	2100 series FAX	21.06.2022 12:02:09	22.06.2022 08:36:52	\\Device\{00000105}	нет
	2100 series FAX	21.06.2022 09:32:15	21.06.2022 12:02:09	\\Device\{0000009C}	нет
	2100 series FAX	21.06.2022 07:57:16	21.06.2022 09:17:09	\\Device\{000000F1}	нет
	2100 series FAX	21.06.2022 07:02:17	21.06.2022 07:53:30	\\Device\{000000A8}	нет
	2100 series FAX	21.06.2022 04:13:31	21.06.2022 07:02:17	\\Device\{000000C0}	нет
	2100 series FAX	20.06.2022 06:51:23	21.06.2022 04:13:31	\\Device\{000000BA}	нет

Перечень устройств рабочего места с группировкой по классам устройств

Учет рабочего времени

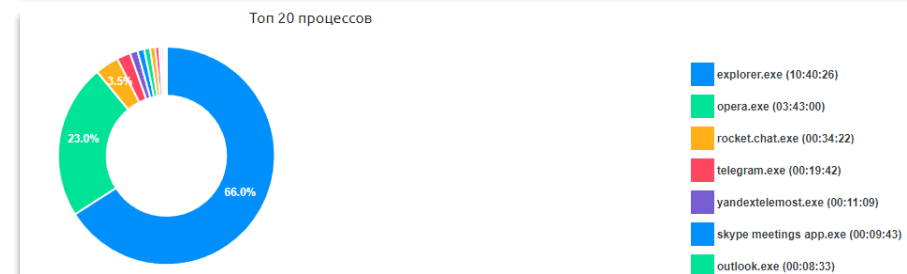
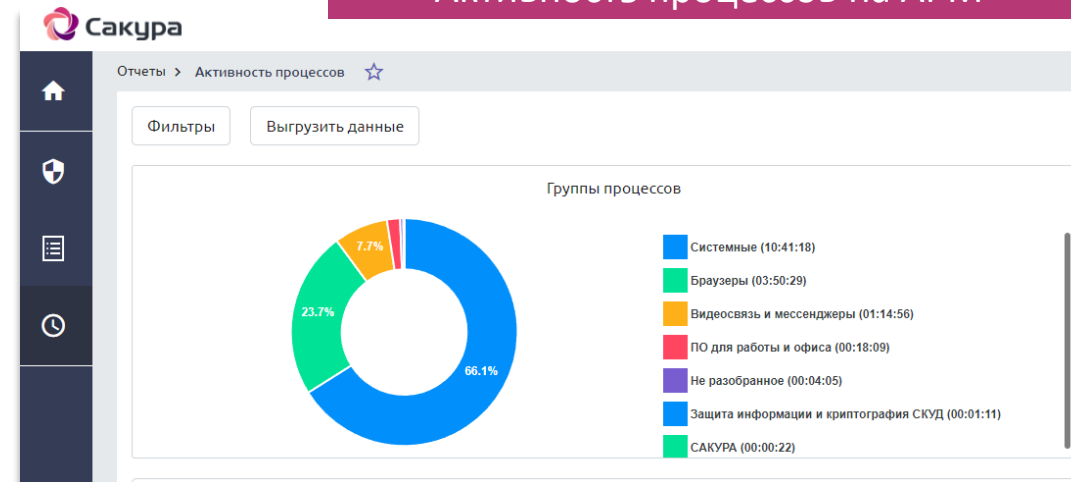
- Контроль деятельности пользователей
- Статистика посещенных сайтов
- Получение информации по рабочему времени

Отчет активности сотрудника АРМ



Активность сотрудника на рабочем месте в заданный период времени

Активность процессов на АРМ



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

Сравнение функционала



Расширенная безопасность приложений SaaS. Обеспечивает полное покрытие за счет защиты всех приложений, как локальных, так и облачных. Сканирует трафик, порты и протоколы; автоматически обнаруживает новые приложения.



Обеспечивает применение единых политик безопасности для пользователей распределенных структур, осуществляет контроль и мониторинг использования интернета внутри компании. Позволяет связать сети предприятия в единое целое, что дает возможность удобного и безопасного использования корпоративных ресурсов, соответствующего заданным различным правам доступа.



Многофакторная аутентификация. Может использоваться, скорее, как дополнение или альтернатива в 2ФА. В Сакура: мобильное приложение для 2ФА – полная альтернатива Мультифактору



Предотвращение фишинга, вредоносных программ. Защита от атак программ-вымогателей. Видимость входящих, исходящих и внутренних сообщений. Выявление и блокировка потоков с помощью аналитики потоков от группы исследователей угроз Cisco. Работа с протоколом 802.1x



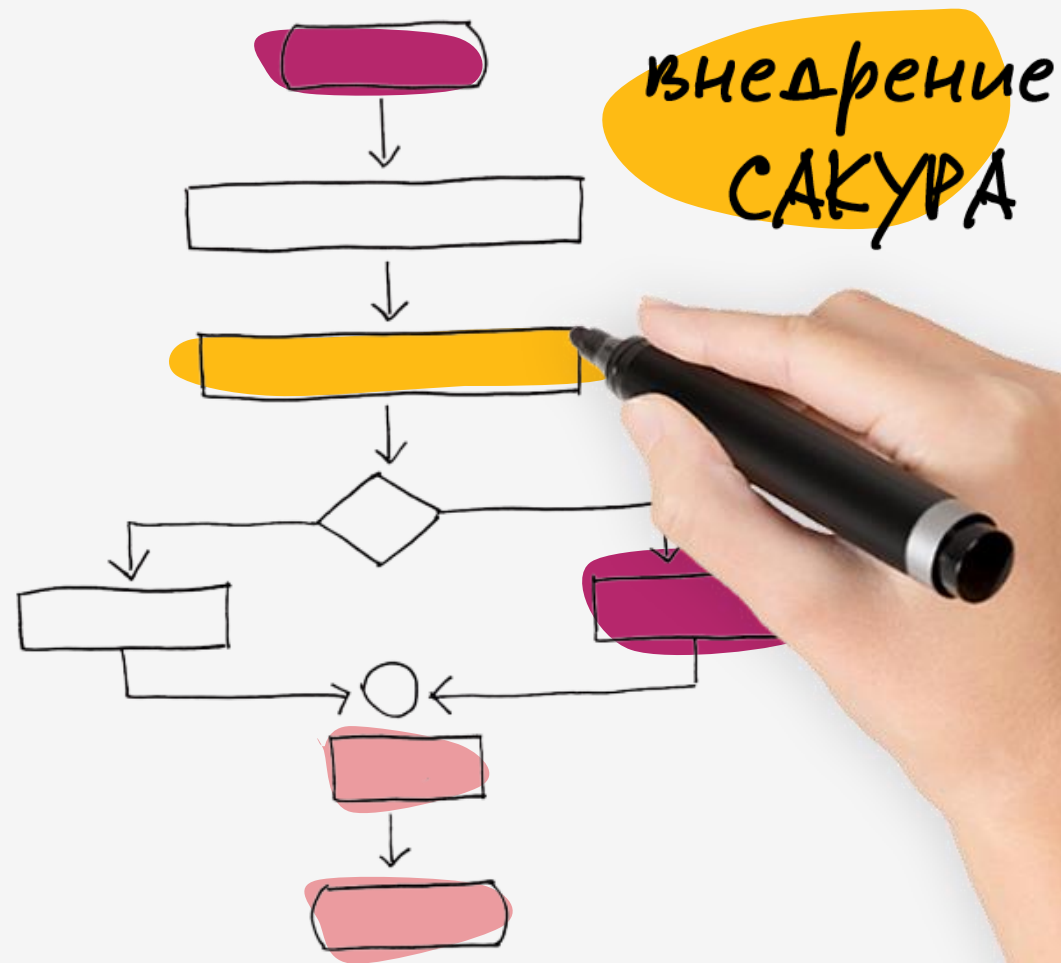
CHECK POINT™

Платформа CloudGuard, ориентирована на защиту исходного кода, анализируя код бессерверного приложения до и после развертывания, организации могут достичь непрерывного бессерверного обеспечения безопасности - автоматическая настройка безопасности ОС приложений. Строит модель нормального поведения приложений и функций для обнаружения и блокирования атак прикладного уровня для повышения бессерверной безопасности. Защита от кибератак.

Преимущества программного комплекса САКУРА



Проектные внедрения

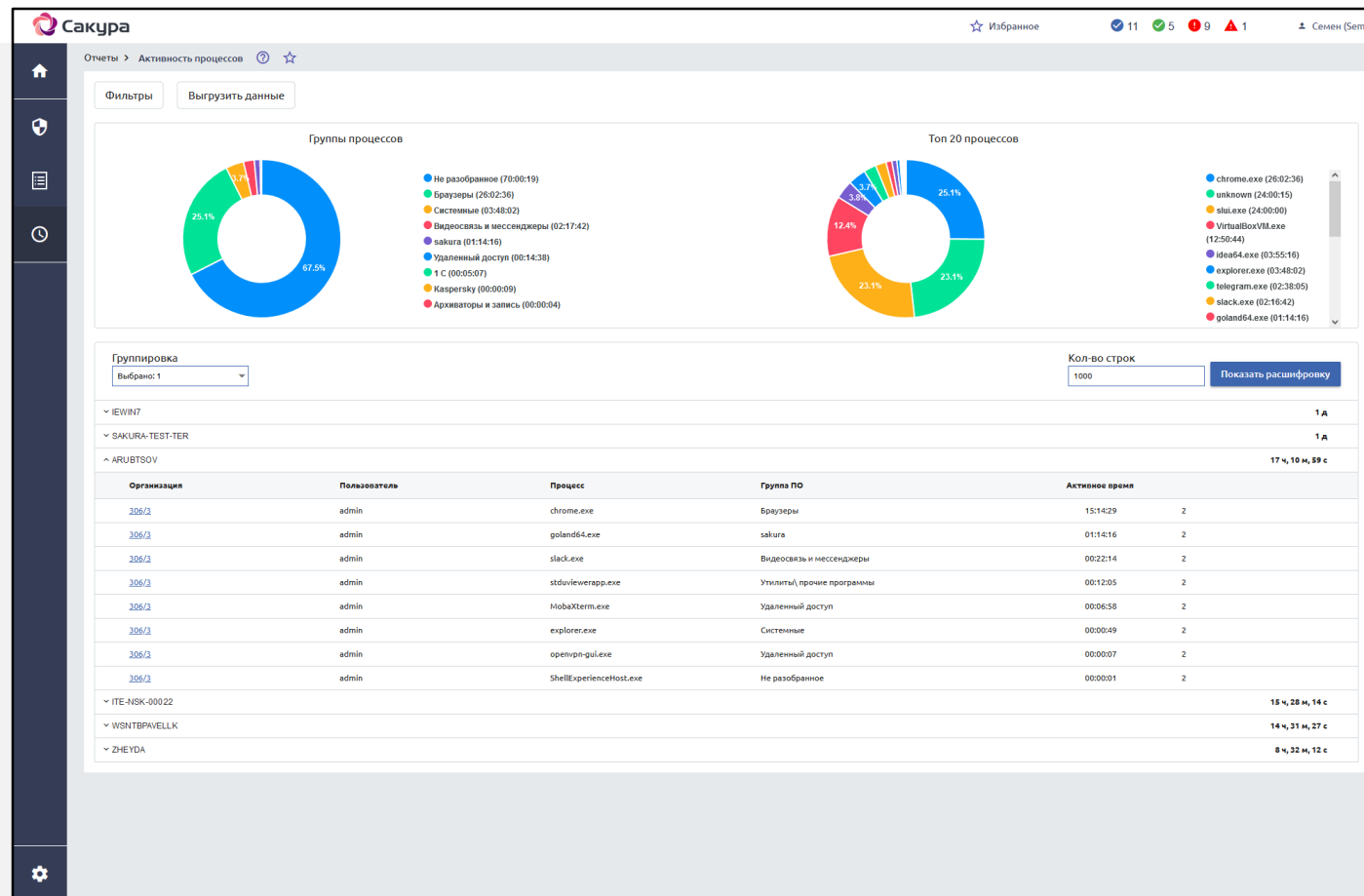


Госкорпорация «Ростех»

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

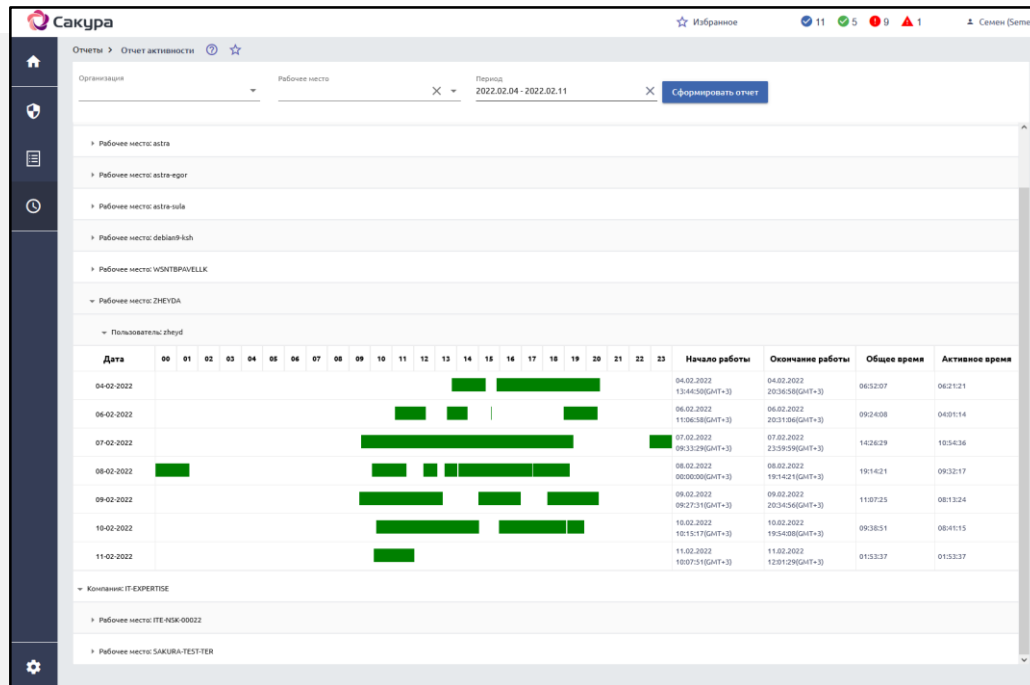
Выявление случаев нецелевого использования ПК

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

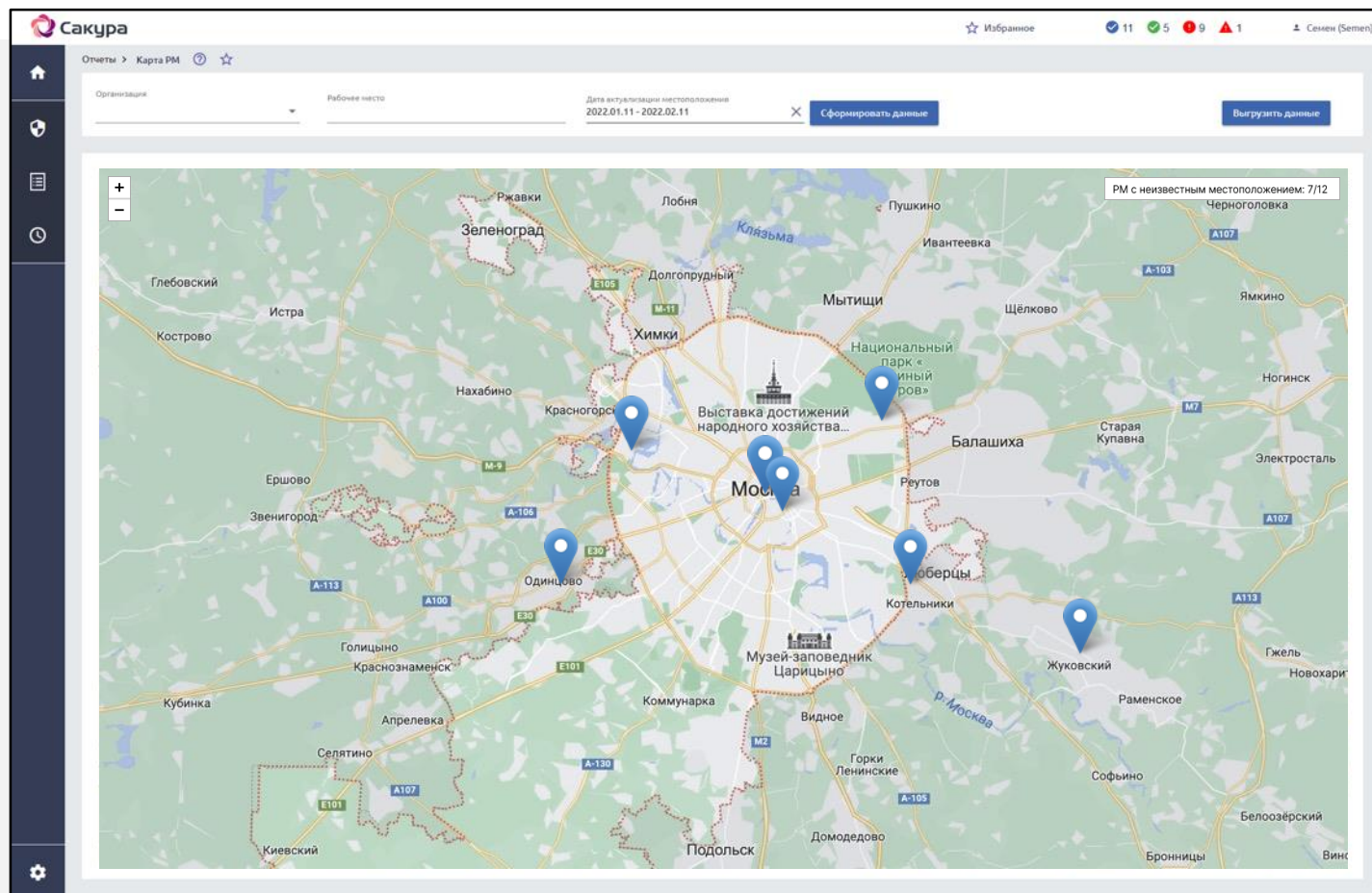
САКУРА дает возможность **автоматического формирования рабочих таблиц** с возможностью доработки формы отчета под внутренние требования

Табель работы пользователей

Формирование рабочих таблиц сотрудников

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

ДИТ города Москвы



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

Основная
поставка:

Дополнительные
модули:

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)

Лицензия
на Модуль
двухфакторной
аутентификации

для ПО «САКУРА-Агент»

по количеству РМ
лицензия на год + пролонгация

Расчёт стоимости приобретения комплекса на 1 год в расчёте на 1 рабочее место

Количество рабочих мест **20** Срок действия, лет **1**

17 000 Р
На одно рабочее место в год

При покупке
лицензий на **20**
рабочих мест

Количество рабочих мест **200** Срок действия, лет **1**

5 200 Р
На одно рабочее место в год

При покупке
лицензий на **200**
рабочих мест

Количество рабочих мест **2000** Срок действия, лет **1**

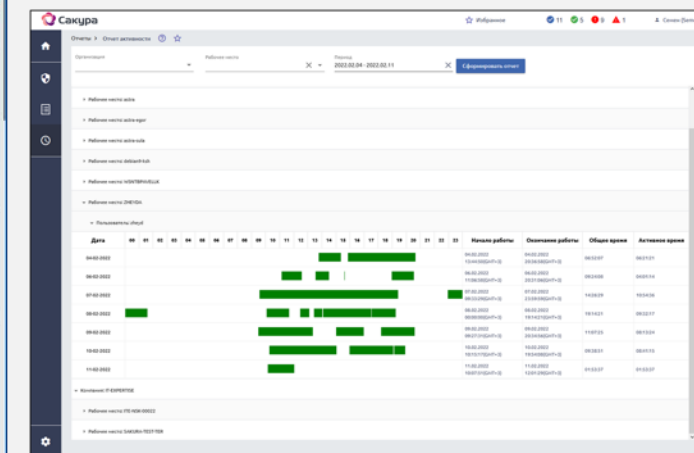
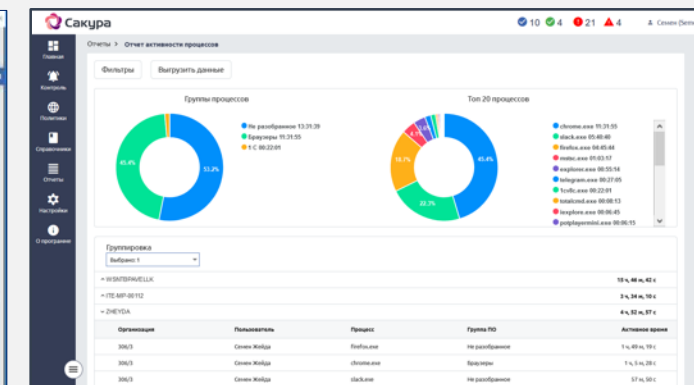
2 900 Р
На одно рабочее место в год

При покупке
лицензий на
2000 рабочих
мест

Интерфейс комплекса САКУРА



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



Применяя комплекс САКУРА, вы получите



Выполнение **требований государственных регуляторов** (ФСТЭК и т.д.)



Полную информацию о загрузке сотрудников и эффективности **использования ими рабочего времени**



Снижение количества инцидентов информационной безопасности **более чем в 10 раз**



Контроль **соответствия** рабочих мест **политикам безопасности** независимо от их расположения и архитектуры



Возможность использования **двухфакторной аутентификации**



Управление **доступом к приложениям** на платформе **1С:Предприятие** согласно требованиям комплаенса и безопасности



Полную информацию об **инфраструктуре и ПО**, используемых в компании

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 и первичное обучение** администраторов системы
5. Оплатите заказ и получите комплекс САКУРА **для контроля комплаенса безопасности и управления доступом**

Свяжитесь с нами!



Получите 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