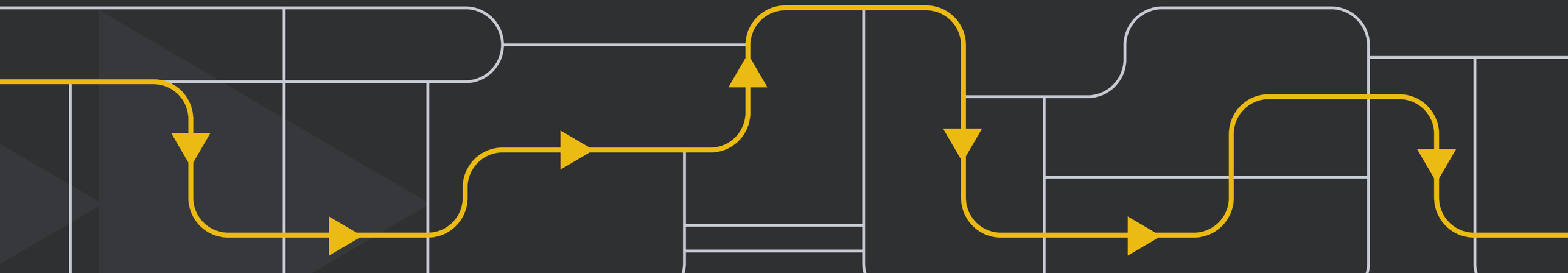
PT

Информационная безопасность



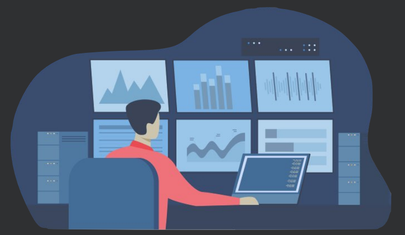
# О компании

АО «РТ-Информационная безопасность» определено единым центром компетенций по технологическому обеспечению корпоративной системы информационной безопасности Государственной корпорации «Ростех» и ее организаций на основании приказа Государственной корпорации «Ростех» №59 от 24.08.2022

## «РТ-Информационная безопасность» – это:

Построение защищенных автоматизированных /информационных систем

Поставка и настройка программных средств защиты информации



Мониторинг и реагирование на компьютерные инциденты **(SOC – центр)**

Защита критической информационной инфраструктуры (КИИ)

Защита персональных данных (ПДн) и государственных информационных систем (ГИС)

Оказание услуг в области ИБ, включая **тестирование на проникновение** и **оценку защищенности** согласно 250 указу Президента РФ.

РТ
Информационная безопасность

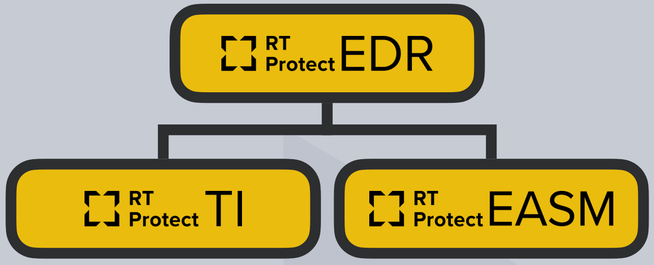
# Достижения компании

**Команда специалистов РТ-ИБ имеет большой практический опыт в области обеспечения ИБ как в государственных, так и в коммерческих организациях.**

**Государственная корпорация «Ростех»**
Реализован комплексный проект по услугам киберустойчивости ИТ-инфраструктуры корпорации

**ПАО «ОАК»**
Проведено масштабное тестирование на проникновение головного холдинга и множества его дочерних организаций

**АО «НПК “Уралвагонзавод”»**
Выстроены процессы мониторинга и реагирования на базе широкого спектра СЗИ.




Собственная экосистема продуктов по автоматизированному выявлению и пресечению киберугроз

RT Protect SOC

Единый центр мониторинга и реагирования на компьютерные инциденты ГК Ростех. Подключено более 20 организаций

RT link

Корпоративная платформа коммуникации для взаимодействия между работниками организации. Используется в ГК Ростех; АО «ОПК» АО «КБП» им. А. Г. Шипунова; АО «РТ-Регистратор», ООО «РТ-Развитие бизнеса»

Команда специалистов РТ-Информационная безопасность в роли «Blue team» заняла **1 место в Кибербитве 2022** – одном из ключевых соревнований по ИБ

# Современные тенденции

Расширение разнообразия используемых для написания вредоносного программного обеспечения языков программирования и технологий, усложнение архитектуры

Всё более сложные социотехнические атаки, что требует повышения осведомленности в информационной безопасности рядовому работнику

Рост активности группировок, связанных с одной из сторон конфликта

Эксплуатация уязвимостей:

- Microsoft Exchange (ProxyNotShell - CVE-2022-41040)
- Apache Tomcat (Log4Shell - CVE-2021-44228)
- Microsoft Outlook Elevation of Privilege (CVE-2023-23397)
- Vmware Spring Framework (Spring4Shell CVE-2022-22965)

Как следствие, повышение требований к защите конечных точек

PT
Информационная безопасность

# Линейка решений

## Услуги

- RT Protect SOC
- Оценка защищенности
- Тестирование на проникновение
- RT-Retro
- Аудит ИБ
- RT Protect Awareness
- Проектирование СОИБ

## Продукты

- RT Protect EDR
- RT Protect TI
- RT Protect EASM
- RT Protect NTA
- RT link

# Оценка защищенности

**Оценка защищенности**
– комплекс работ по оценке защищенности информационных систем организации.

Целью выполнения работ является получение достоверных сведений об уровне защищенности информационной инфраструктуры Заказчика от реализации недопустимых событий (НС), выявление следов компрометации, а также выработка маршрутной карты по модернизации информационной инфраструктуры.

**! Дополнительно может производиться ретроспективный поиск индикаторов компрометации**

PT
Информационная безопасность

# Тестирование на проникновение

PT
Информационная безопасность

**Целью выполнения работ является имитация действия реального злоумышленника.**
Работы проводятся методом «черного ящика» с целью проверки полноты, эффективности и достаточности мер по защите информации, принятых на основании требований действующего законодательства и общепринятых практик по обеспечению безопасности информационной инфраструктуры Объекта.

**Тестирование включает следующие этапы:**

**01.** Атаки методами социальной инженерии

**02.** Эксплуатация уязвимостей

**03.** Закрепление в системе

**04.** Поиск слабых паролей (как пользователей, так и администраторов)

**05.** Анализ веб-приложений

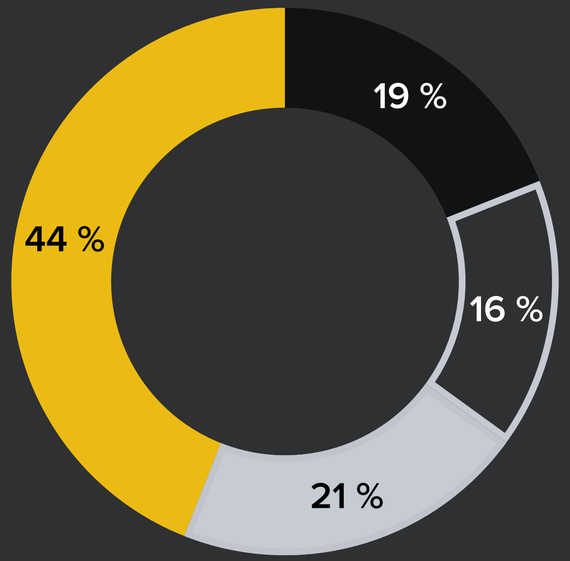
**06.** Поиск утечек (документы, учетные записи Организации)

**07.** Анализ сервисов на предмет наличия ошибок кофигураций

**08.** Выработка рекомендаций по повышению защищенности и закрытию векторов атак, выявленных при исследовании информационной инфраструктуры организации

# Тестирование на проникновение

## Результаты внешнего тестирования (+ комплексное):




- Прошли внешний периметр, попали в локальную сеть
- Захватили ресурсы, но не прошли во внутреннюю сеть
- Получили наивысшие привилегии в ЛВС
- Не захватили ни одного ресурса

**Самые популярные векторы атак**

**ошибки конфигурации (доступна директория .git, LFI)**
- ➜ получение конфигурационных файлов
- ➜ создание пользователя с правами администратора
- ➜ проксирование трафика во внутреннюю сеть

**устаревшее ПО (RCE)**
- ➜ создание пользователя с правами администратора
- ➜ проксирование трафика в локальную сеть

**ошибки в исходном коде web приложения (SQLInjection, LFI, RCE)**
- ➜ получение конфигурационных файлов
- ➜ создание пользователя с правами администратора
- ➜ проксирование трафика во внутреннюю сеть

**социальная инженерия**
- ➜ получение учётной записи пользователя, получение Reverse Shell

**Социальная инженерия**

**10/15**

**успешно получен Reverse Shell**

**Самые популярные уязвимости**

CVE-2022-27228 (Bitrix vote module RCE),CVE-2021-34473 (MS Exchange RCE ProxyShell)

CVE-2022-41040+CVE-2022-41082 (MS Exchange RCE ProxyNotShell)

PT Информационная безопасность

# RT-Retro

**RT-Retro**
– ретроспективный анализ инфраструктуры на предмет компрометации

**RT-Retro – услуга ретроспективного анализа информационной инфраструктуры на предмет компрометации.** Включает в себя централизованный сбор данных с конечных систем их обработку и дальнейший анализ. Она необходима как для определения текущей активности злоумышленников в информационной инфраструктуре, так и установления фактов взлома, имевших место в прошлом.

**Преимущества RT-Retro:**

Автоматизация процесса сбора данных

Оптимизация процесса анализа собранных данных

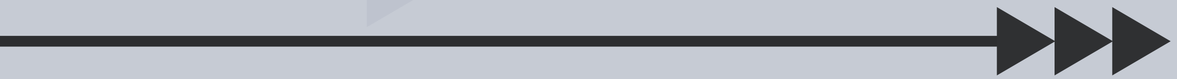
Оптимизация используемых инструментов в зависимости от точек сбора

Автоматизация процессов нормализации и обогащения данных

PT
Информационная безопасность

# Этапы ретроспективного анализа инфраструктуры

PT Информационная безопасность



Выявление критических узлов информационной инфраструктуры

Централизованный запуск инструмента сбора данных

Передача, нормализация и обработка данных в Apache NiFi

Передача данных в Logstash, обогащение через TI-платформу

Корреляция полученных данных

Визуализация и анализ событий по временной шкале

+

Формирование отчета

# Методики анализа конечных точек

## Генерация инцидентов из собранных данных

- Сигнатурный анализ файловой системы и памяти процессов
- Корреляция логов
- Статистический анализ данных со всех систем, поиск аномалий
- Типичные места закрепления ВПО
- Обогащение собранных данных с помощью Threat Intelligence

## Углубленный анализ конечных точек, участвующих в инцидентах

- Журналы ОС
- Информации о файловой системе
- Информация о процессах, сервисах, активных сетевых соединениях
- История активности процессов и пользовательских сессий
- Сработки с СЗИ

PT
Информационная безопасность

# RT Protect SOC

**RT Protect SOC**
– центр мониторинга и реагирования на инциденты информационной безопасности.

## Основные характеристики:

Подключение самых разнообразных источников событий ИБ для эффективного мониторинга

**более 500**
правил детектирования вредоносной активности

Общий объем обрабатываемых событий в секунду

**50 000 EPS**

Среднее время обработки инцидента:

**12 мин 30 сек**

Среднее время расследования:

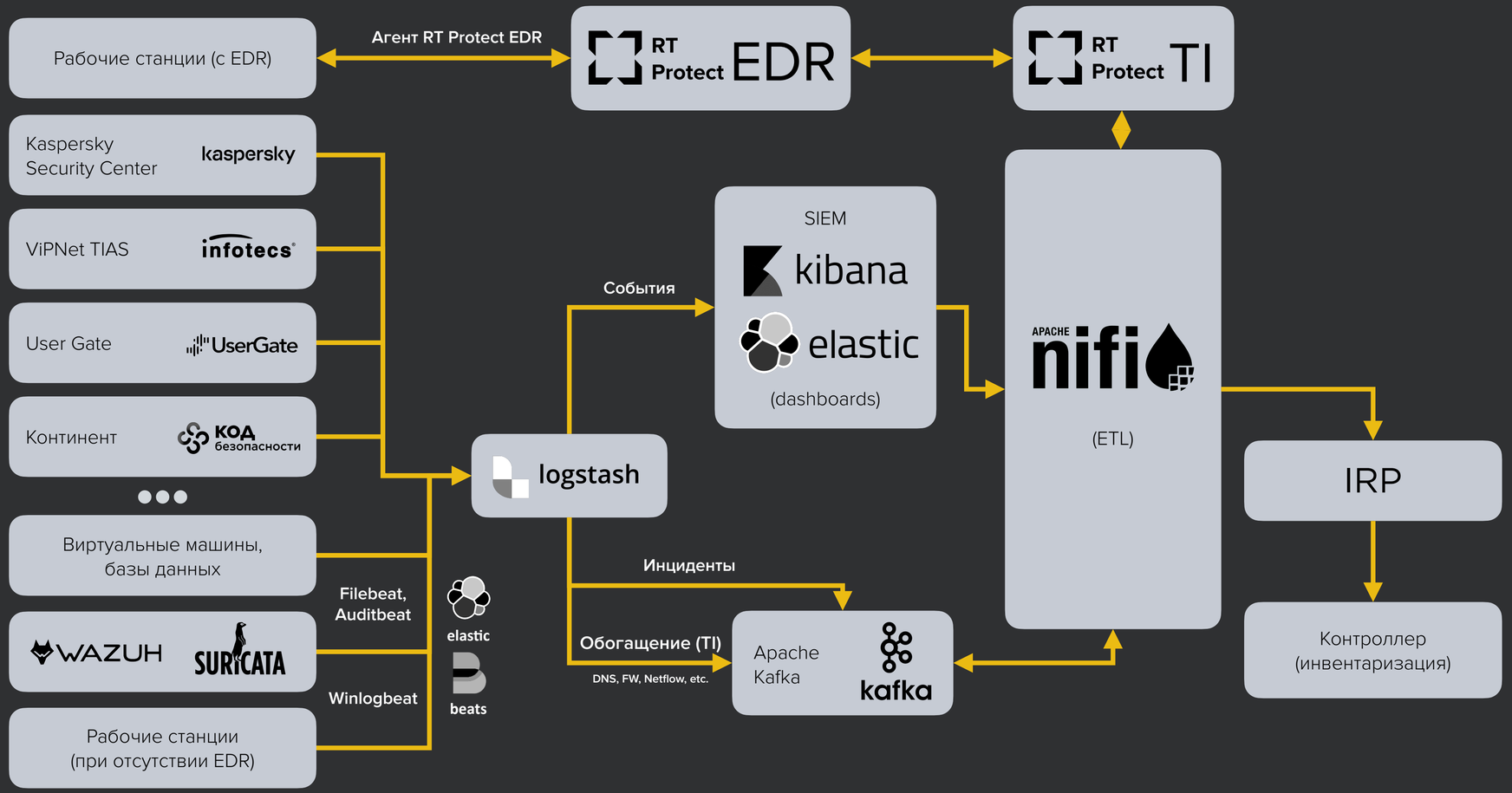
**20 мин 25 сек**

PT
Информационная безопасность

# RT Protect SOC

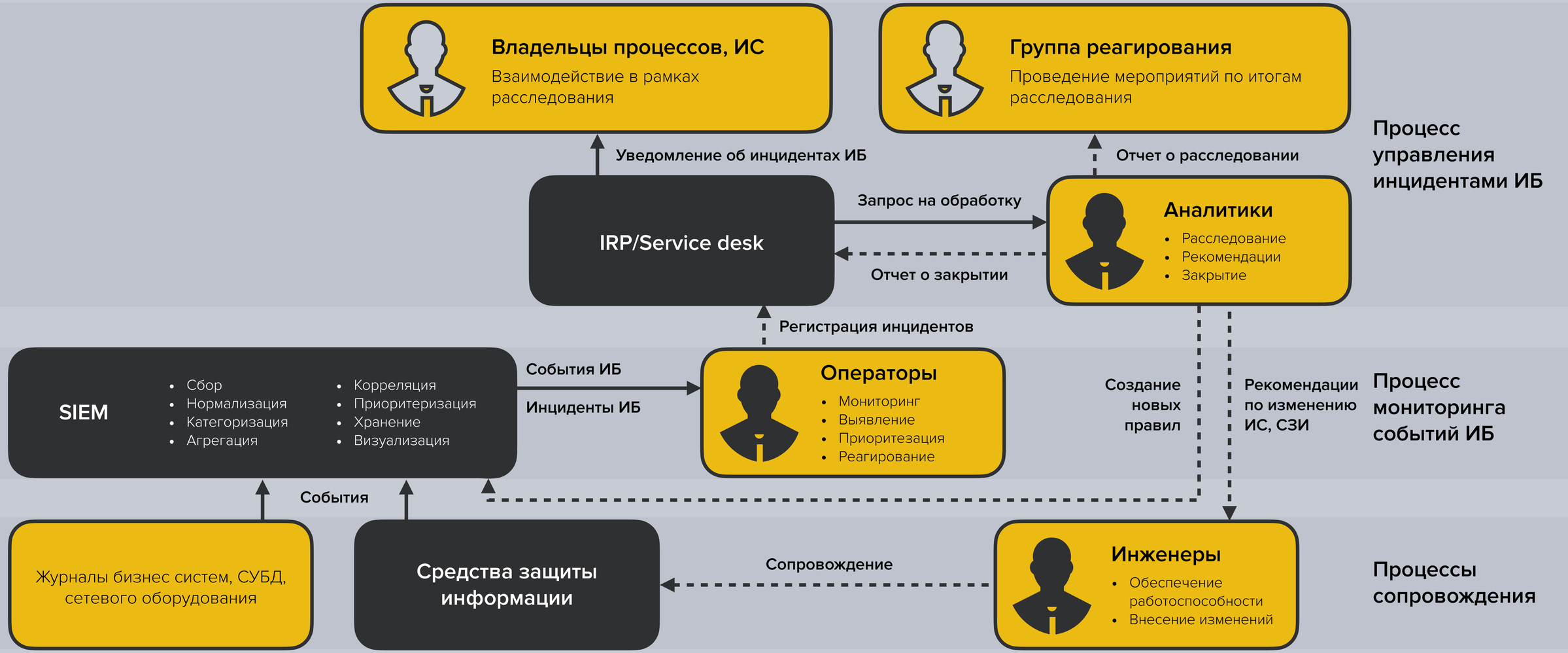
**Задачи:**

- Круглосуточный мониторинг корпоративной IT-инфраструктуры
- Сокращение времени обнаружения продвинутых атак
- Эффективное противодействие и устранение последствий
- Расследование инцидентов ИБ любого типа сложности
- Обеспечение непрерывности бизнес процессов




PT
Информационная безопасность

# Процессы SOC



# RT Protect EDR

**RT Protect EDR**
– система обнаружения целенаправленных атак на конечных устройствах, обеспечивающая автоматическое противодействие.

## РТ-ИБ за 2022 год выявлено:

Увеличение количества внутренних и внешних атак на организации

**в 1,5 раза**

по сравнению с данными 2021 года.

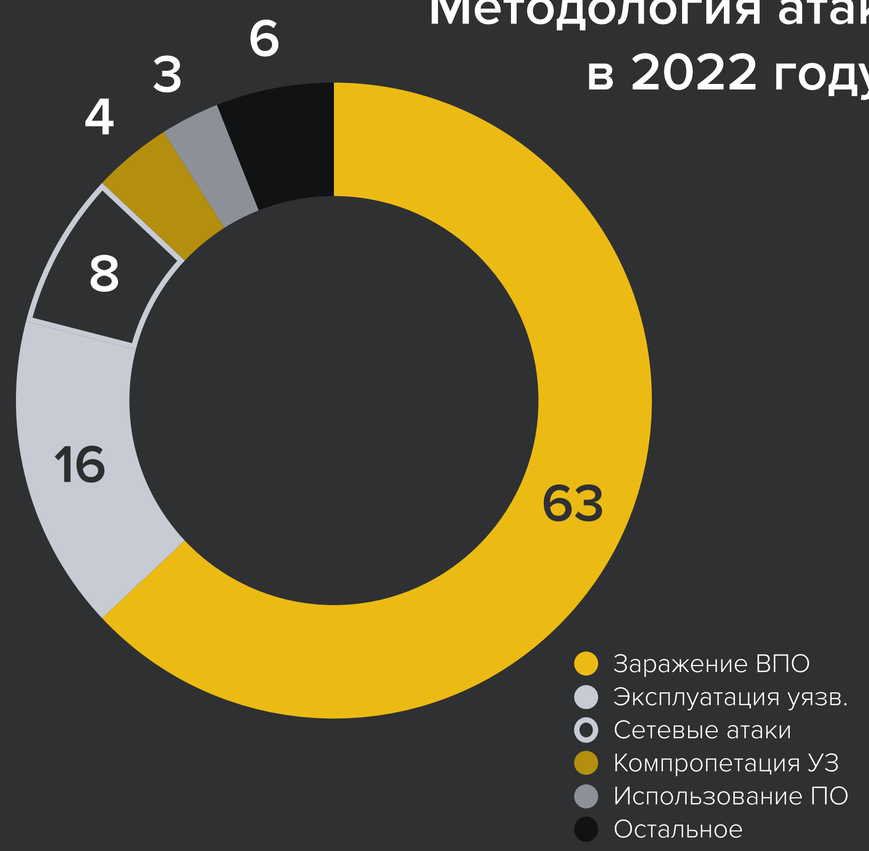
Увеличение количества атак на госучреждения практически

**в 2 раза**

по сравнению с данными 2021 года.

**RT Protect EDR - актуальное средство защиты ИБ, отразившее 100% атак на Киберполигоне 2022**

## Методология атак в 2022 году




РТ
Информационная безопасность

# Классические задачи EDR

PT Информационная безопасность

## Сбор телеметрии (ingest)

- Процессы
- Файловая система
- Реестр
- Сеть
- Адреса в памяти
- Пользователи и группы
- WMI
- Автозагрузки
- Различные скрипты (PowerShell, AMSI, Bash и проч.)

## Обнаружение (detection)

**IoC / IoA**

Автоматизированное выявление следов и TTP атакующих

**YARA**

Автоматизированное выявление инструментов атакующих

**Vulnerability management**

Своевременное оповещение об уязвимостях

**Threat hunting**

Ручной проактивный поиск следов / TPP атакующих

**Золотой образ**

Отслеживание белого списка ПО

## Реагирование (response)

- Скачивание / загрузка / удаление файлов
- Завершение процесса
- Сбор данных
- Изоляция хоста
- Интерактивная консоль
- Запуск процессов / скриптов (bash)
- Антишифровальщик
- Автоматическое блокирование по хешу, имени

# Функции EDR

## Индикаторы атак

Удобная система управления индикаторами атак и их наборами

Собственные правила выявления угроз с интуитивно понятным механизмом написания IOA

Классификация по матрице MITRE ATT&CK

Регулярное обновление специалистами TI

Конвертер Sigma правил

## Защита от вирусов-вымогателей и загружаемых модулей

**Отдельный модуль на базе эвристического анализа поведения программ:**

реализует защиту от «шифровальщиков» как класса, а не его отдельных представителей

осуществляет прозрачное резервирование пользовательских файлов

## Индикаторы компрометации

Многообразие типов индикаторов компрометации

Удобная система управления индикаторами компрометации и их наборами

# Threat Hunting

Аналитика по поведенческим признакам

### Гибкий поиск угроз

Быстрый и удобный поиск угроз в корпоративной сети по событиям EDR

Настраиваемая фильтрация событий по различным параметрам

Возможность использования языка DSL для продвинутой фильтрации

# Сбор данных журналов

Взаимодействие с любыми провайдерами журналов Windows

Возможность сбора журналов со средств защиты информации заказчика

# Богатый инструментарий расследований инцидентов

Удобное представление активности процессов в виде дерева со сводной информацией о ключевых событиях

Сведения о распространенности подозрительных исполняемых модулей в агентской сети

# Анализ запускаемых файлов

сигнатурный анализ

эвристический анализ

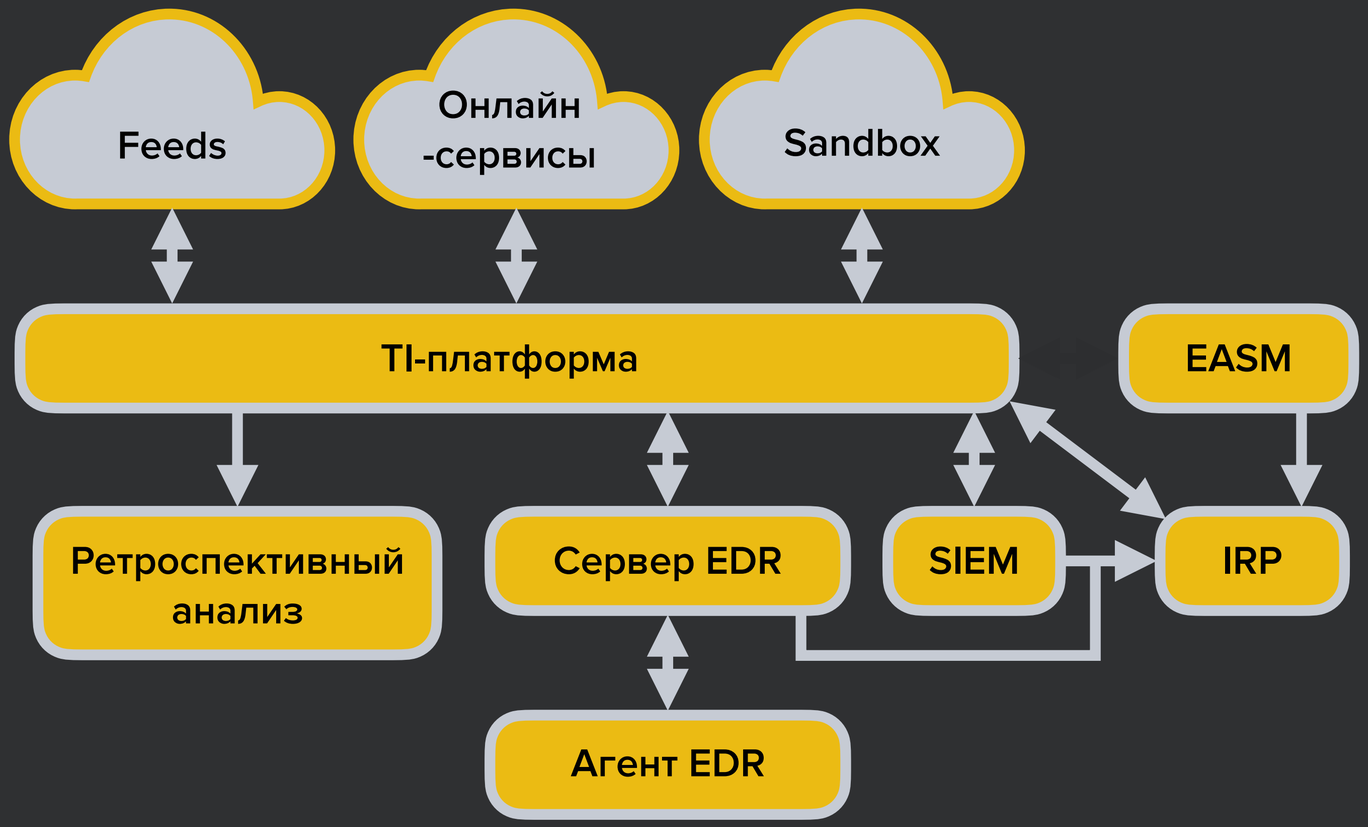
легковесная модель машинного обучения

PT
Информационная безопасность

# RT Protect TI

**RT Protect TI**
– платформа, предоставляющая функционал по агрегации, корреляции и хранения данных о киберугрозах, обеспечению своевременности мер реагирования, а также актуализации экспертизы.

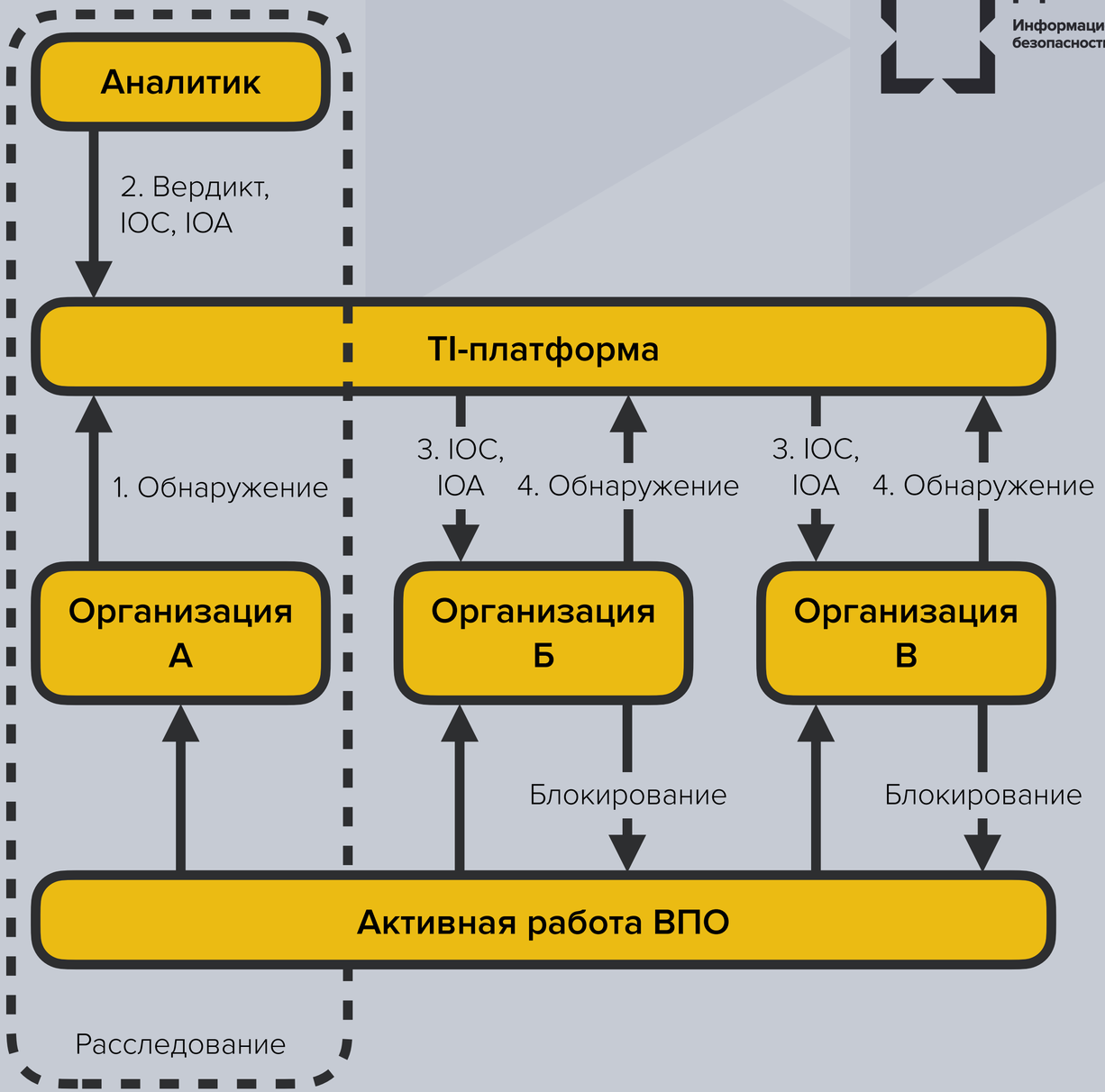
- Определение мотивов, целей, тактик и техник атакующих
- Актуализация экспертизы
- Пополнение базы знаний об актуальных угрозах
- Анализ угроз, зафиксированных в инфраструктуре Заказчиков
- Обогащение при расследовании инцидентов
- Распространение наборов аналитики EDR
- Углубление интеграции со всеми процессами
- Основа реагирования – **EDR**
- Приоритет: **проактивная защита**




PT
Информационная безопасность

# Практические результаты RT Protect TI

- Выделение статистики обнаружений по Организациям
- Ретроспективный поиск по IOC’ам
- Как результат, обнаружение множественных атак на ключевые Организаций



# RT Protect EASM

**RT Protect EASM**
– непрерывная практика обнаружения и оценки ресурсов, доступных из общедоступной сети Интернет, а также поиска их уязвимостей и аномалий.

**EASM представляет собой управление рисками кибербезопасности, связанными с внешними цифровыми активами организации,** что позволяет выявлять изменения в составе внешнего периметра организации, отслеживать утечки информации, связанные с компанией, а также доменные имена, которые могут быть использованы для фишинговых рассылок.

**Решаемые задачи:**

**01.** Уменьшение сроков и затрат на проведение анализа защищенности и пентеста за счет автоматизации

**02.** Поиск утечек информации

**03.** Автоматизация обнаружения потенциально фишинговых доменов

**04.** Отображение ретроспективной информации об изменении защищенности организации

**05.** Оперативное обнаружение 0-day уязвимостей

# Возможности EASM

**01.** Пассивное сканирование – поиск поддоменов и ip-адресов

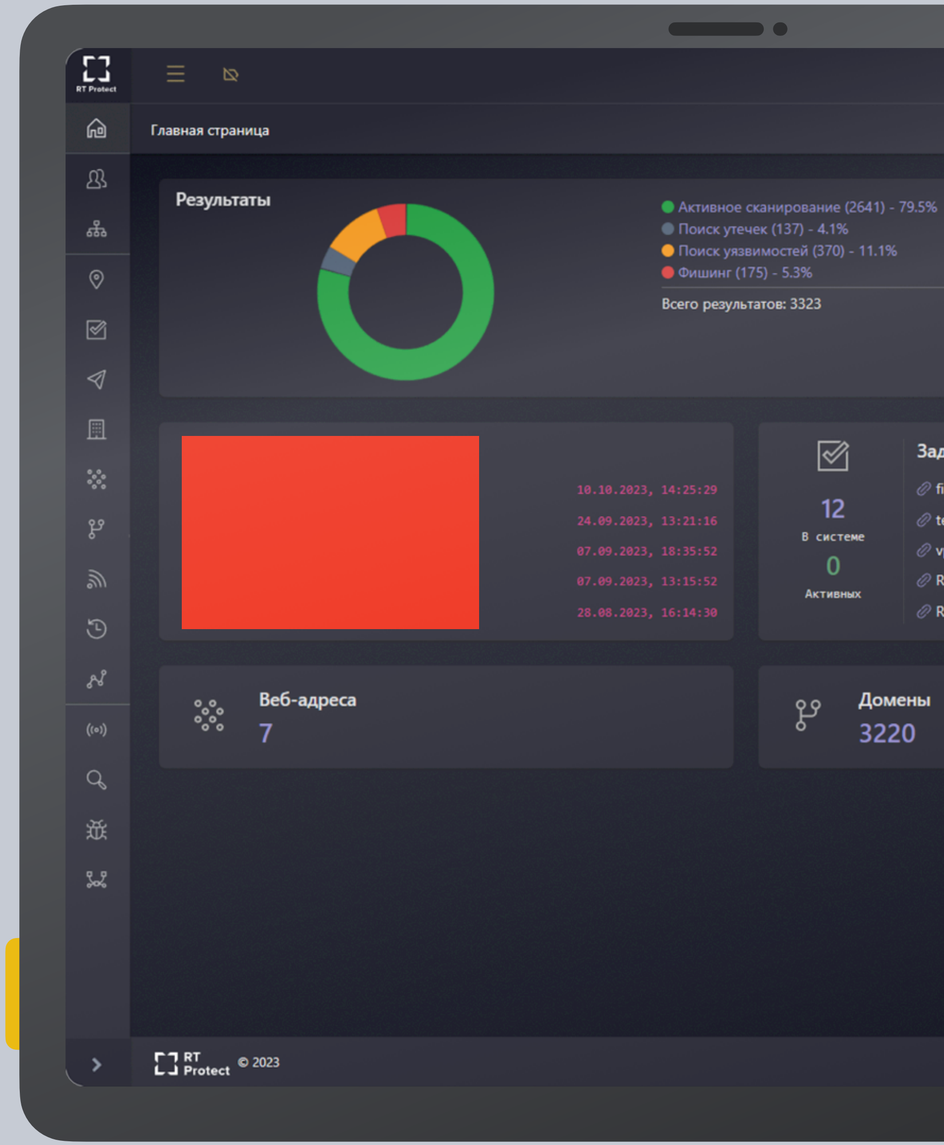
**02.** Активное сканирование – определение открытых портов, сервисов и служб

**03.** Поиск уязвимостей в доступных сервисах

**04.** Анализ веб-сервисов – поиск уязвимых и устаревших компонентов, пассивный поиск уязвимостей на основании версии сервиса

**05.** Брутфорс – перебор директорий на сайте и dns имен

**06.** Поиск учетных записей в публичных утечках информации



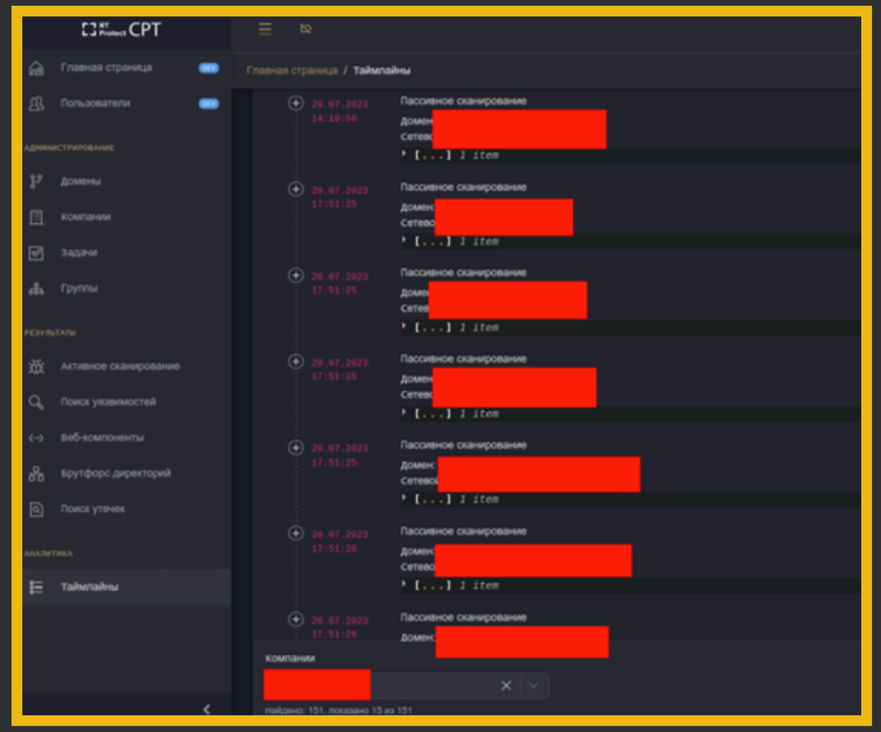

PT
Информационная безопасность

# RT Protect EASM

**Решение позволяет:**

- Определить изменения на внешнем сетевом периметре организации
- Находить и эксплуатировать уязвимости
- Искать утечки учётных записей в открытых источниках
- Определять уязвимые компоненты на веб сервисах
- Обнаружить ресурсы, доступные из сети Интернет
- Собирать информацию о SSL-сертификатах на внешних сервисах

Проект построен по принципу микросервисной архитектуры, что позволяет масштабировать необходимые сервисы в зависимости от нагрузки.




Веб-интерфейс проекта позволяет в реальном времени отображать информацию о сканируемых доменах.

# RT Protect NTA

**RT Protect NTA (система анализа сетевого трафика)** помогает эффективно контролировать сетевую активность организации, выявлять факты нарушения политики безопасности, в том числе утечки конфиденциальной информации, отказ в работе сетевых сервисов и нарушения стандартного профиля сетевых взаимодействий.

## Ретроспективный анализ

Детализация сетевой активности ранее накопленных данных с учетом специфики расследуемого инцидента, а также возможность применения новых анализаторов и методов анализа.

## Индексация и классификация трафика

Расчет и запись статистики сетевого трафика в реальном времени, включает в себя не менее 20 сетевых параметров индексации.

## Захват трафика

Захват сетевого трафика с нескольких сетевых интерфейсов одновременно с возможностью фильтрации.

## Интеграция с SIEM-системами

Экспорт событий ИБ анализаторов Комплекса.

## Запись трафика

Гарантированная запись сетевого трафика на диск со скоростью до 20 Гбит/с и предоставление его для анализа.

PT
Информационная безопасность

# RT Protect NTA

## Мониторинг в реальном времени

Оперативный мониторинг состояния сети организации в графическом и табличном представлении.

## Интеграция с внешними анализаторами трафика

Перенаправление трафика на внешние системы обнаружения вторжений.

## Анализаторы трафика

Выявление аномалий и атак в автоматическом режиме с применением методов математической статистики и машинного обучения.

## Идентификация протоколов

Определение более 1000 сетевых протоколов, включая прикладной уровень приложений и сервисов.

## Геолокация

Идентификация географической принадлежности сетевых адресов индексируемого трафика.

PT
Информационная безопасность

# Схема работы RT Protect NTA

## Интернет

## Сетевой шлюз

Захватывает и сохраняет весь трафик сети.

## Дампер

Захватывает и сохраняет весь трафик сети.

## RAID-массив

## Индексатор

Индексирует и классифицирует трафик, записывает метаинформацию в БД.

Выявляют аномалии и атаки в автоматическом режиме с применением методов математической статистики и машинного обучения.

## Анализаторы

Централизованный мониторинг и управление всеми компонентами Комплекса.

## Управляющий сервер

## База данных

Хранит статистику трафика, события анализаторов и политики фильтрации трафика.

Интуитивно понятный web-интерфейс. Предоставляет данные для анализа трафика и выполнения расследований.

## Консоль оператора

## Локальная сеть

RT
Информационная безопасность

# RT link

**RT link** – корпоративная платформа коммуникации для взаимодействия между работниками организации, разработанная для Государственной корпорации «Ростех»

## Преимущества RT link:

- Конфиденциальность, защищенность и исключение утечки информации благодаря контейнеризации
- DLP, SIEM, Антивирус
- Оптимизация корпоративной коммуникации благодаря единой платформе
- Повышение уровня принятия решений линейными сотрудникам
- Наличие всех современных функций - аудио и видео звонки, голосовые сообщения, чат-боты, корпоративные каналы

Федерация

Аудио звонки

Видео конференции

Корпоративные каналы

Stealth режим

Отечественное решение

Голосовые сообщения

DLP

Чат боты

E2EE

Совместная работа

Защита данных

Магазин приложений

Active Directory

Роутинг

Круги доверия

PT
Информационная безопасность

# Технические возможности RT link

PT Информационная безопасность

## Защита данных

### Контейнеризация

- Зашифрованное хранение всех данных
- Удаление всех данных по команде с сервера
- Контроль системы функций

### DLP, SIEM, антивирус

- Интеграция с корпоративными DLP и SIEM
- Пред-проверка потоковым антивирусом

### Аутентификация пользователей

- Копоративная учетная запись в Active Directory
- Одноразовый пароль из СМС
- Личный пользовательских пароль

### Безопасность передачи данных

- 3 слоя шифрования данных
- Безопасные пуш-нотификации
- Запрет резервного копирования (iCloud, Google Drive, Яндекс.Диск и т.д.)

## Взаимодействие

### Гостевой доступ

- Гостевые учетные записи для внешних участников
- Создание корпоративного доверенного контура

### Режим конфиденциальности

- Открытие файлов строго внутри защищенного хранилища
- Запрет копирования, пересылки, сохранения сообщений и файлов
- Запрет скриншотов и записи экрана
- Таймер автоматического удаления сообщения
- Ограничение «Mobile only»

### Создание рабочих групп

- Мультисерверные видео и аудио звонки с демонстрацией экрана
- Мгновенный поиск контактов на серверах
- Полная интеграция с Active Directory, поиск по ФИО, должности, подразделению

## Инфраструктура

### Серверная инфраструктура

- Инфраструктура на 500 тыс. пользователей
- Соответствует требованием Tier 3
- Администрирование серверной инфраструктуры осуществляется командой экспертов PT-Информационная безопасность

# Федерация

## Эффективность коммуникации

- Возможность создать рабочую группу внутри компании и с внешними пользователями RT link
- Полная интеграция с Active Directory. Поиск коллег по ФИО, должности, подразделению и другими полям. В том числе на серверах, связанных доверенными отношениями (трастом)
- Ваши контакты на телефоне, зарегистрированные в RT link – сразу отобразятся в числе контактов RT link

## Безопасность

- Полный контроль потоков данных
- Усиленное шифрование

## Гостевой контур

- Временные аккаунты для внешних участников проектных групп

РТ
Информационная безопасность

# Эффект от использования RT link

### Отказ от сторонних приложений

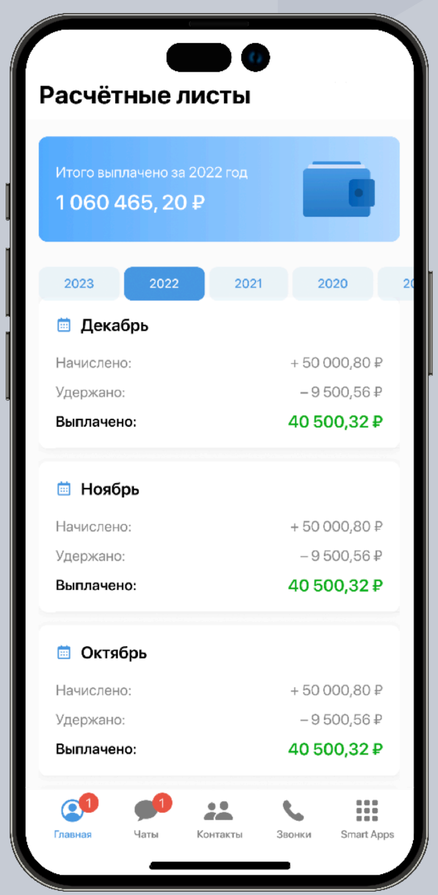
Нет необходимости переписываться в одном приложении, видеоконференцию проводить в другом, а документы отправлять по почте. Все функции есть в одном месте

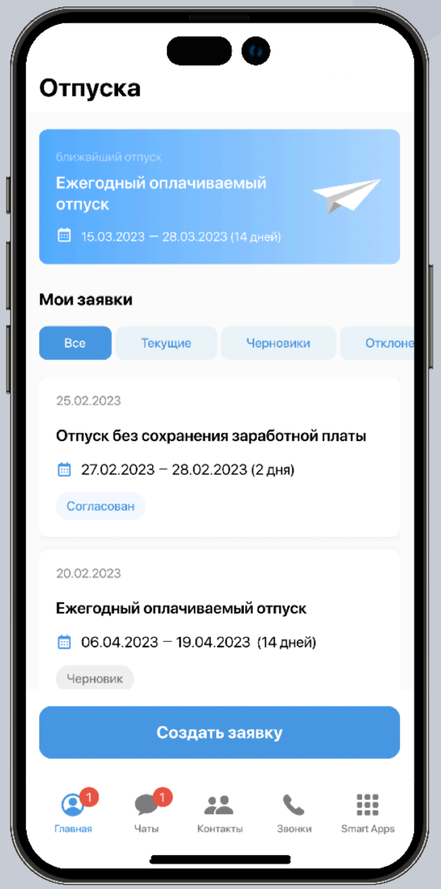
### Уменьшение трудозатрат

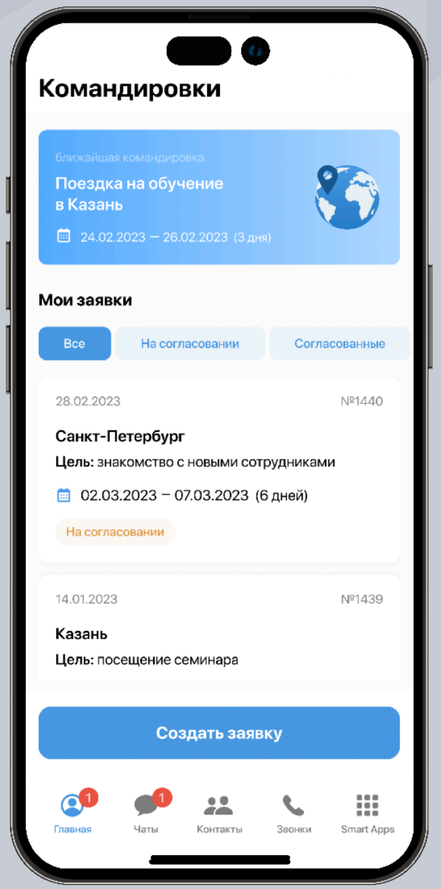
Благодаря интеграции с различными системами и чат-ботами кадровые трудозатраты значительно уменьшатся. Например, заказ кадровой справки, согласование командировки и авансового отчета можно осуществить самостоятельно

### Подбор персонала

Выстраивание корпоративной культуры, обучение и адаптация персонала в одном месте. Персональные чаты для общения с кандидатами, групповые чаты для рекрутеров и обсуждения резюме




РТ
Информационная безопасность

# RT Protect Awareness

**RT Protect Awareness**
– платформа по повышению осведомлённости сотрудников в сфере информационной безопасности

**RT Protect Awareness** в легкой и понятной форме повышает осведомленность работников в сфере информационной безопасности и цифровой гигиены. При помощи имитации фишинговых рассылок у компании есть возможность проверить степень уязвимости работников к действиям злоумышленника.

PT
Информационная безопасность

# RT Protect Awareness

## По каким причинам происходит взлом инфраструктуры компании?

**01.** Большинство работников не знают основ цифровой гигиены, поэтому халатно относятся к информационной безопасности при использовании личных и корпоративных устройств.

**02.** У компании отсутствует возможность контролировать уровень знаний своих работников.

**03.** В компаниях отсутствует инструмент, с помощью которого можно проверить действия работников в ситуациях, приближенных к реальной атаке.

**04.** У руководителей нет подробной аналитики по уровню подготовки работников и степени их уязвимости к действиям злоумышленников.

# Что включает в себя?

RT
Информационная безопасность

Набор курсов

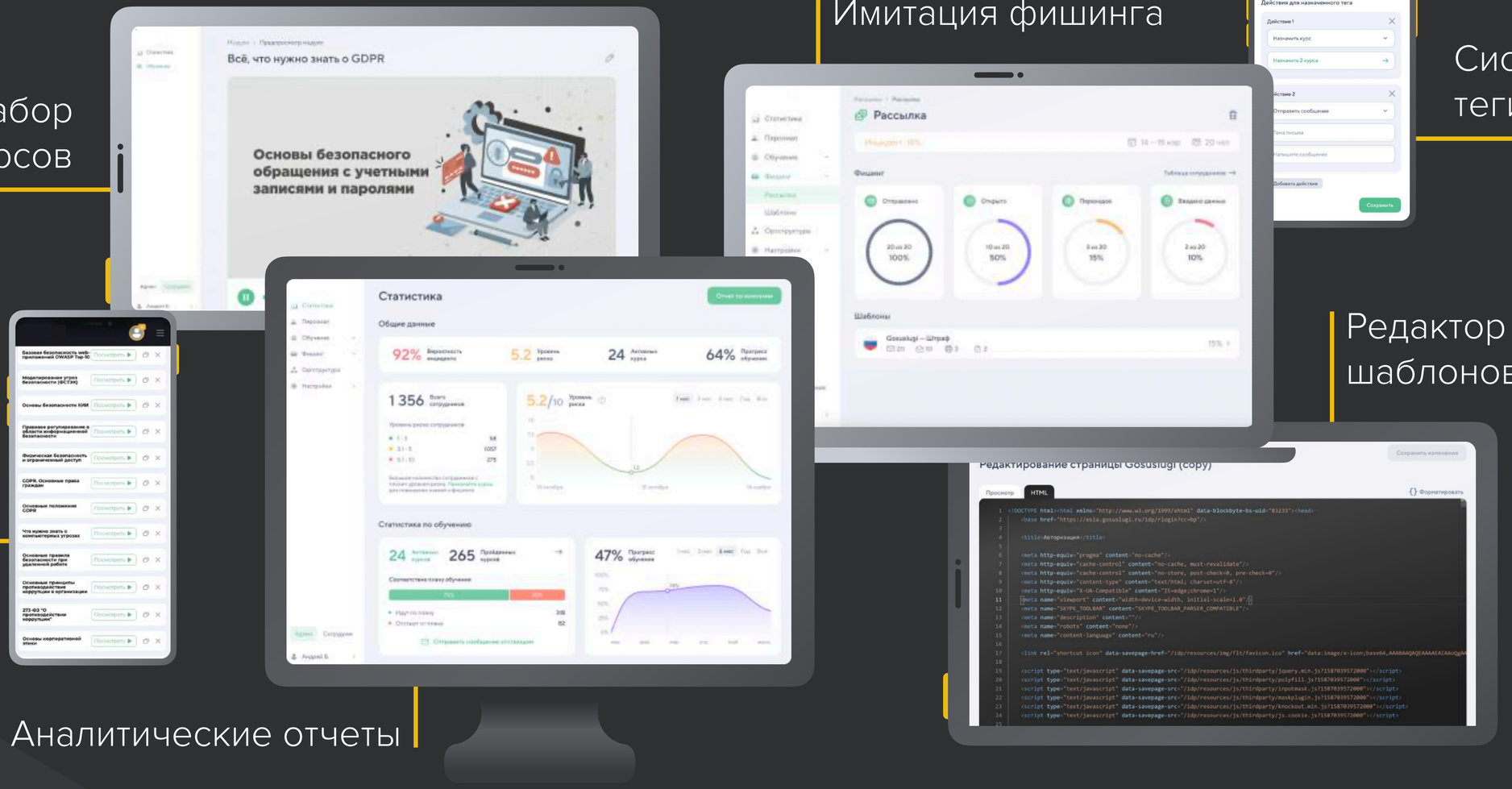
Авторские курсы

Аналитические отчеты

Имитация фишинга

Система тегирования

Редактор шаблонов



# Аудит ИБ

**Аудит ИБ**
– оценка состояния ИТ-инфраструктуры организации

**Аудит информационной безопасности** — мероприятия по оценке текущего состояния защиты объекта оценки (ИТ-инфраструктура, объект информатизации, информационная система и пр.) на соответствие требованиям законодательства РФ в области защиты информации, а также выявления уязвимостей и потенциальных угроз информационной безопасности.

## Когда необходим аудит?

**01.** Отсутствие знаний о текущем состоянии защиты объекта информатизации и порядке обработки информации.

**02.** Низкая осведомленность об организационных и технических мерах защиты информации.

**03.** Отсутствие или не актуальность организационно-распорядительных документов в области ИБ.

**04.** Отсутствие понимания процессов обеспечения ИБ.

**05.** Неэффективный выбор решений, не соответствующих рискам ИБ, снижение эффективности модулей защиты.

**06.** Отсутствие стратегии ИБ.

**07.** Непродуктивная деятельность работников подразделения ИБ.

**08.** Отсутствие возможности эффективной оценки рисков ИБ в составе операционных рисков компании.

# Технология

1
Утверждение методов анализа состояния защиты информации.
2
Проведение интервью с работниками с использованием стандартизованных опросных листов.
3
Документирование системы и анализ рисков.
4
Анализ организационно-распорядительной документации по обеспечению ИБ.
5
Оценка процессов обеспечения ИБ в организации, квалификации работников и др.
6
Оценка актуальности физических механизмов безопасности.
7
Формирование отчета и списка рекомендаций по проведенным работам.

# Нам доверяют

Ростех
РТ-Энергоэффективность

РТ
Развитие бизнеса

Ростех
Техприемка

Ростех

KAMAZ

ОАК
Объединенная авиастроительная корпорация

ОДК

КБП

СИБЕР

Нацимбио

Высокоточные комплексы

УВЗ

НОВИКОМБАНК

# Контакты

**Адрес:** 117587, г. Москва,
Варшавское шоссе,
дом 118, корпус 1

**Tel.:** +7 (499) 390-79-05

**E-mail:** info@rt-ib.ru

**Сайт:** rt-ib.ru

РТ
Информационная безопасность

PT

Информационная
безопасность