PT

Информационная
безопасность

# О компании

**РТ- Информационная безопасность занимается разработкой и внедрением решений в сфере информационной безопасности, позволяющих решать широкий спектр задач по защите информации. Наши сотрудники – эксперты с многолетним опытом работы в области ИБ. При разработке продуктов мы используем как собственную практику их использования в реальных инфраструктурах, так и лучшие мировые решения построения безопасных систем.**

Мы защищаем корпоративные сети, помогаем обнаруживать утечки конфиденциальной информации и расследовать сетевые инциденты ИБ.

**НАШИ ЛИЦЕНЗИИ И СЕРТИФИКАТЫ:**

- Лицензия на проведение работ, связанных с использованием сведений, составляющих государственную тайну (ФСБ России)
- Лицензия на осуществление мероприятий и (или) оказания услуг в области защиты государственной тайны (ФСТЭК России)
- Лицензия на проведение работ, связанных с созданием средств защиты информации (Минобороны России)
- Лицензия на проведение работ, связанных с созданием средств защиты информации (ФСТЭК России)
- Лицензия на деятельность по технической защите конфиденциальной информации (ФСТЭК России)
- Лицензия на деятельность по разработке и производству средств защиты конфиденциальной информации (ФСТЭК России)
- Лицензия на осуществление разработки, производства, распространения шифровальных средств (ФСБ России)
- Сертификат соответствия СМК

**RT Protect NTA - программно-аппаратный комплекс, позволяющий осуществлять анализ внутреннего и внешнего трафика компании, проводить обнаружение активности злоумышленников и контроль соблюдения политик информационной безопасности.**

**Комплекс является эффективным и удобным инструментом для анализа сетевых взаимодействий и контроля сетевой активности пользователей и ПО.**

## Клиенты

- Подразделения ИБ и IT
- Компании, заинтересованные в контроле интернет-активности своих сотрудников
- Интернет-провайдеры

**Комплекс RT Protect NTA подходит для компаний любого масштаба, имеет интуитивно понятный интерфейс, гибкие настройки и оптимальное ресурсопотребление.**

На оборудовании архитектуры x86-64 Комплекс позволяет без потерь обрабатывать сетевой поток на скорости до 20 Гбит/с (10 Гбит/с full-duplex).

Для анализа сетевых потоков на скорости до 2 Гбит/с **RT Protect NTA** требуются ресурсы, сопоставимые с недорогим ПК.

Один Комплекс одновременно позволяет обрабатывать сетевые потоки с нескольких независимых сетевых интерфейсов.

эльбрус

**RT Protect NTA** также работает на российском оборудовании архитектуры «Эльбрус».

**2,5 трлн руб.**

потери экономики России от кибератак в 2019 году

**10,52 млрд**

атак вредоносных программ зарегистрировала в 2018 году компания SonicWall

**На 61%**

выросло число утечек конфиденциальных данных в России 2023 года (по сравнению с аналогичным периодом 2022 года)

*данные Сбербанка, SonicWall, InfoWatch.

## Для чего нужен RT Protect NTA

- **Выявляет кибератаки на активы предприятия**
- **Классифицирует трафик по базе публичных сервисов**
- **Контролирует действия сотрудников в Интернете**
- **Собирает статистику и позволяет анализировать весь трафик в удобном формате отчетов**
- **Собирает доказательную базу и помогает расследовать инциденты ИБ**
- **Позволяет минимизировать финансовые и репутационные риски**

# Что умеет RT Protect NTA

**RT Protect NTA помогает эффективно контролировать сетевую активность организации, выявлять факты нарушения политик безопасности, отказы в работе сетевых сервисов и нарушения стандартного профиля сетевых взаимодействий.**

### Захват трафика

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

### Индексация и классификация трафика

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

### Запись трафика

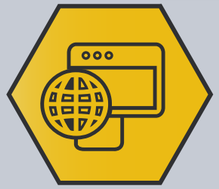
Гарантированная запись сетевого трафика на диск со скоростью до 20 Гбит/с и предоставление его для анализа.

### Мониторинг в реальном времени

Оперативный мониторинг состояния сети организации в графическом и табличном представлении.

### Ретроспективный анализ

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



### Интеграция с SIEM-системами

Экспорт событий ИБ в сторонние системы

### Анализаторы трафика

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

### Геолокация

Идентификация географической принадлежности сетевых адресов индексируемого трафика.

### Интеграция с внешними анализаторами трафика

Перенаправление трафика на внешние системы обнаружения вторжений: СОА «Аргус», Snort, Suricata.

### Идентификация протоколов

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

## Как это работает

# RT Protect NTA

**Интернет**

**Сетевой шлюз**

**Дампер**

Захватывает и сохраняет весь трафик сети.

**RAID-массив**

Хранит трафик с метаинформацией.

**Анализаторы**

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

**Управляющий сервер**

Централизованный мониторинг и управление всеми компонентами Комплекса.

**Консоль оператора**

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


**Локальная сеть**


**Индексатор**

Индексирует и классифицирует трафик, записывает метаинформацию в БД.

**База данных**

Хранит статистику трафика, события анализаторов и политики фильтрации трафика.

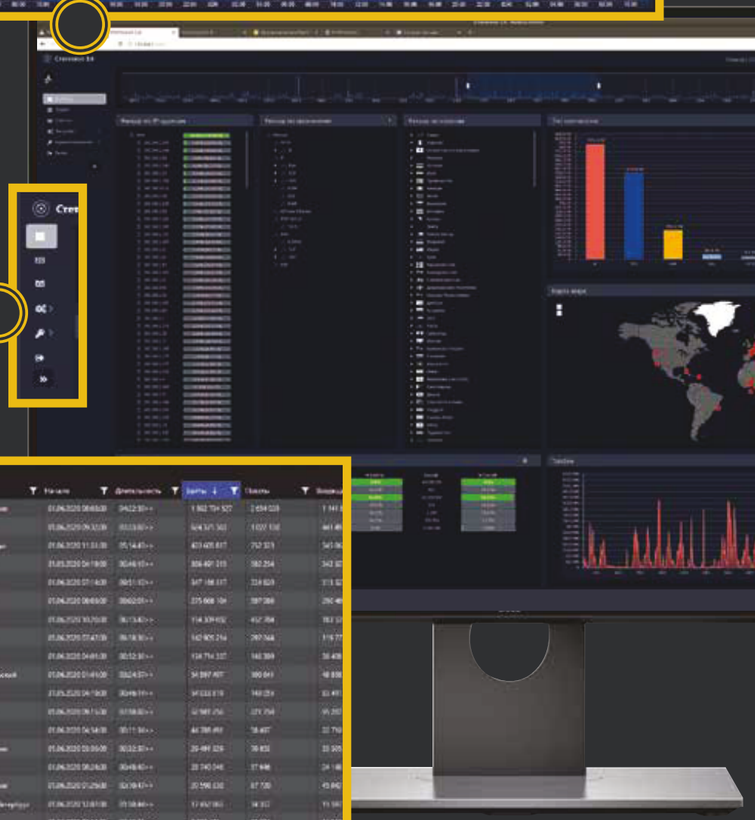
# Интерфейс оператора

## Выбор временного интервала

Удобный способ получить детализацию статистики трафика или событий ИБ за нужный интервал времени.

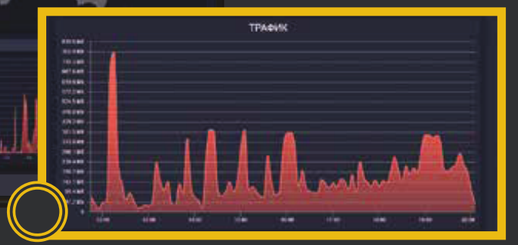
## Главное меню

Выбор режима отображения данных между агрегированными отчетами или детализированной информацией о трафике и событиях ИБ, также раздел управления Комплексом.



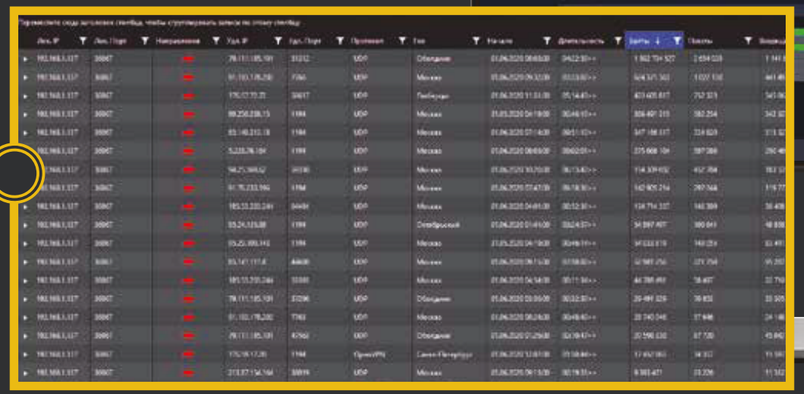
## Протоколы

Статистика наиболее используемых протоколов.




## Трафик

Интенсивность трафика за выбранный интервал времени с фильтрацией по IP-адресам, протоколам и геолокации.



## Подробные отчеты

Получение детальной информации по сетевым сессиям и событиям ИБ. Возможность фильтрации и экспорта.

## Сценарии использования

Выполнение анализа в реальном времени и ретроспективно.

## Сетевой трафик

Представление сетевой активности с удобным механизмом фильтрации.

## События ИБ

Единая система отчетов по событиям ИБ от различных анализаторов.

# Преимущества Комплекса

**RT Protect NTA полезен для большинства компаний и имеет ряд преимуществ по сравнению с другими решениями.**

## Плюсы решения RT Protect NTA

### Уникальный развивающийся функционал

Реализована плагинная архитектура, позволяющая гибко расширять базовую функциональность анализаторов Комплекса. Применяются методы математической статистики, сигнатурного анализа и машинного обучения (ML).

### Простота внедрения и масштабируемость

Простая процедура развертывания не требует изменения сетевой инфраструктуры. Для анализа потоков на скорости 1 Гбит/с достаточно обычного персонального компьютера, а для анализа каналов до 10 Гбит/с нет необходимости в дорогом серверном оборудовании.

### Эргономика

Интуитивно понятный интерфейс позволяет легко начать работу с Комплексом по решению задач мониторинга сети.

### Импортозамещение

Российская разработка. Поддержка отечественной платформы «Эльбрус». Возможность применения в государственных органах РФ.

### Гибкая ценовая политика

Аппаратные и программные компоненты подбираются с учетом скорости сетевых потоков, времени хранения данных и планируемых к использованию анализаторов.

### Интеграционные возможности

Интеграция с существующими системами анализа трафика (IDS/IPS) и системами управлениями событиями и информацией о безопасности.

### Поддержка

Оказание поддержки и сопровождения на всех этапах эксплуатации Комплекса, от внедрения Комплекса до расследования инцидентов ИБ.

## Технические характеристики

Мы поставляем **RT Protect NTA** в виде комплексного решения: сервер с предустановленным программным обеспечением. Это позволяет гарантировать соответствие всем техническим требованиям и правильную настройку параметров, а значит, надежную работу всего Комплекса.

Типовое решение представляет собой сервер с предустановленным ПО **RT Protect NTA** и при необходимости ответвитель сетевого трафика (TAP) для безопасного внедрения в действующую сеть.

Также в комплект типового решения включено более 20 анализаторов контроля пороговых значений, анализа по белым/черным спискам (IP, DNS, геолокация), базам «плохих» IP, DNS и сервисов.

## Характеристики

| | |
|---|---|
| Скорость канала | **20 Гбит/с** |
| Количество сессий в секунду | **<100 000** |
| Форм-фактор | **Сервер 1U-4U** |
| Длительность хранения данных | **От нескольких дней до нескольких лет** |

## Клиенты

Кредитно-финансовые организации

Государственные структуры и ведомства

Телекоммуникационные компании

IT-интеграторы

## Партнеры

ООО «ЦСС»

ЦЕНТР СПЕЦИАЛЬНОЙ СИСТЕМОТЕХНИКИ

High-Tech Bridge

HIGH-TECH BRIDGE
WEB SECURITY COMPANY

АО «МЦСТ»

эльбрус

# 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