

# Новое в версии ViPNet TIAS 3.8

Светлана Старовойт  
руководитель продуктового направления



# План вебинара



- Система ViPNet IDS 3
- Решение ViPNet TDR
- Новое в версии ViPNet TIAS 3.8
- Планы развития

The logo for infotecs, featuring the word "infotecs" in a dark blue, lowercase sans-serif font. A red curved line is positioned above the letter "i".

infotecs

# ViPNet IDS 3

# Система обнаружения компьютерных атак (вторжений) ViPNet IDS 3



ViPNet IDS NS

Обязательный  
компонент



ViPNet TIAS

Не обязательные компоненты



ViPNet IDS MC



Система обнаружения  
компьютерных атак класс В



Система обнаружения вторжений  
уровня сети 4 класс

Требования доверия  
безопасности 4 уровня

# Сертифицированные версии продуктов



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

## СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ СЕРТИФИКАТ СООТВЕТСТВИЯ № СФ/СЗИ.0194

Идентификационный номер: 001  
Входит в действие с: 20.10.2020  
Истекает: 20.10.2025  
Настоящий сертификат удостоверяет, что:  
1. Система, обеспечивающая комплексную защиту информации от несанкционированного доступа (СЗИ), соответствует требованиям, установленным в документе СФ/СЗИ.0194, утвержденном приказом Федеральной службы безопасности Российской Федерации от 20.10.2020 № 001/001-2020-И/И.  
2. Сертификат о соответствии выдан на основании заявления изготовителя (ИЗ) и/или владельца (ВЛ) системы, обеспечивающей комплексную защиту информации от несанкционированного доступа (СЗИ), соответствующей требованиям, установленным в документе СФ/СЗИ.0194, утвержденном приказом Федеральной службы безопасности Российской Федерации от 20.10.2020 № 001/001-2020-И/И.  
3. Система, обеспечивающая комплексную защиту информации от несанкционированного доступа (СЗИ), соответствует требованиям, установленным в документе СФ/СЗИ.0194, утвержденном приказом Федеральной службы безопасности Российской Федерации от 20.10.2020 № 001/001-2020-И/И.  
4. Система, обеспечивающая комплексную защиту информации от несанкционированного доступа (СЗИ), соответствует требованиям, установленным в документе СФ/СЗИ.0194, утвержденном приказом Федеральной службы безопасности Российской Федерации от 20.10.2020 № 001/001-2020-И/И.

## Сертифицированные версии:

- ViPNet IDS NS 3.6.1 + 5 патчей обновления
- ViPNet TIAS 3.5.1 + 1 патч обновления
- ViPNet IDS MC 1.6 + 2 патча обновления

## СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ СЕРТИФИКАТ СООТВЕТСТВИЯ № 4329

Входит в действие с: 24 ноября 2020  
Истекает: 24 ноября 2025



## Завершается контроль изменений:

- ViPNet IDS NS 3.8
- ViPNet TIAS 3.7.1
- ViPNet IDS MC 1.8

Настоящий сертификат удостоверяет, что система обеспечения комплексной защиты информации от несанкционированного доступа (СЗИ), соответствующая требованиям, установленным в документе СФ/СЗИ.0194, утвержденном приказом Федеральной службы безопасности Российской Федерации от 20.10.2020 № 001/001-2020-И/И, соответствует требованиям, установленным в документе СФ/СЗИ.0194, утвержденном приказом Федеральной службы безопасности Российской Федерации от 20.10.2020 № 001/001-2020-И/И.

Идентификационный номер: 001  
Входит в действие с: 24 ноября 2020  
Истекает: 24 ноября 2025

### НАЧАЛЬНИК УПРАВЛЕНИЯ ФСТЭК РОССИИ



Д.Шенцов

The logo for infotecs, featuring a red curved line above the word "infotecs" in a dark blue, lowercase sans-serif font.

# VIPNet TDR

# ViPNet Threat Detection & Response

Решение по обнаружению и предотвращению компьютерных атак

Управление



ViPNet IDS MC

Анализ



ViPNet TIAS

Обнаружение



ViPNet IDS NS



ViPNet IDS HS

Обнаружение и  
предотвращение



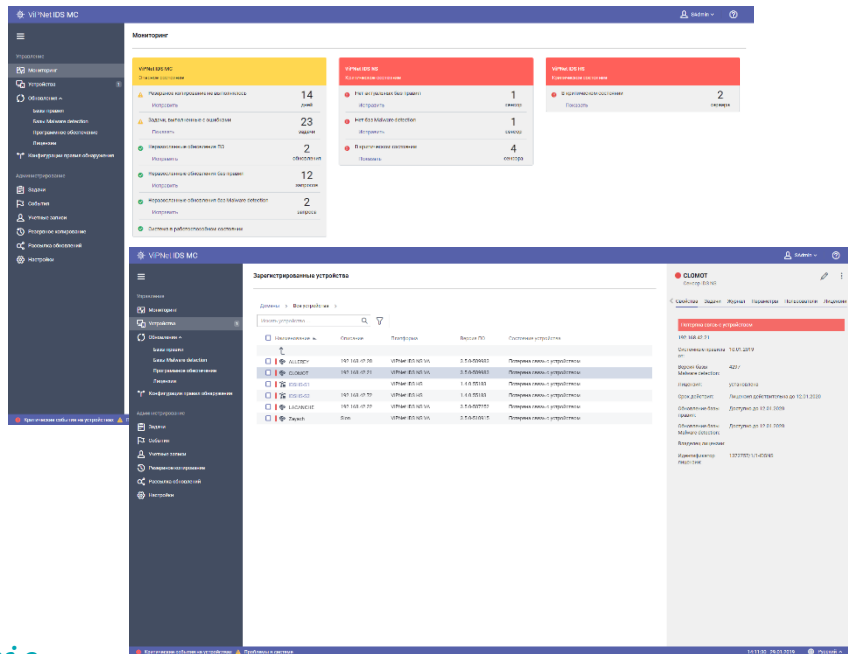
ViPNet  
xFirewall



ViPNet EndPoint  
Protection

# VIPNet IDS MC

- Ввод в эксплуатацию сенсоров IDS;
- управление инфраструктурой решения ViPNet TDR;
- управление конфигурациями правил на устройствах.
- обновление:
  - баз решающих правил
  - сигнатур вредоносного ПО
  - экспертных данных
  - программного обеспечения устройств
  - лицензий
- мониторинг состояния устройств

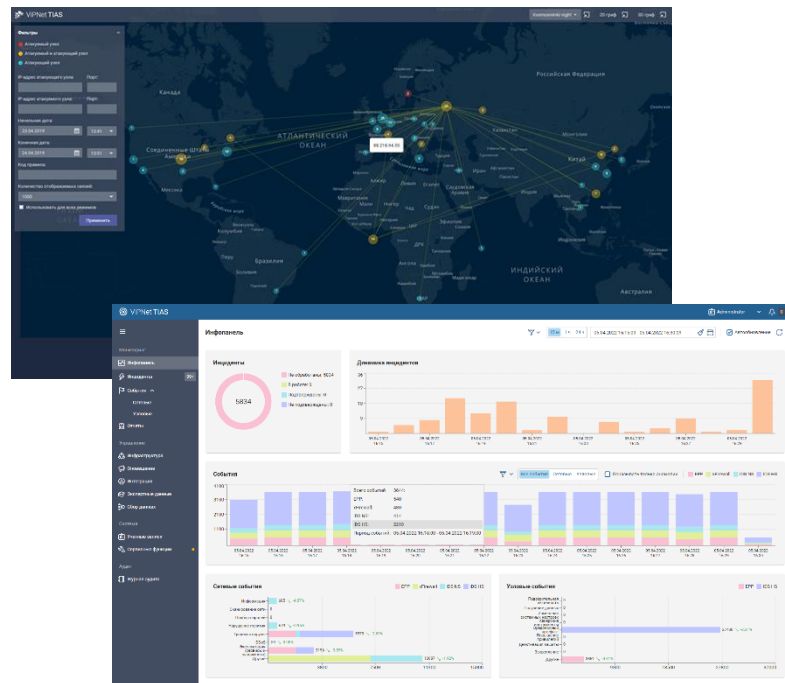


<https://infotecs.ru/webinars/archive/bystroe-razvorachivanie-i-vvod-v-ekspluatatsiyu-resheniya-vipnet-tdr.html>



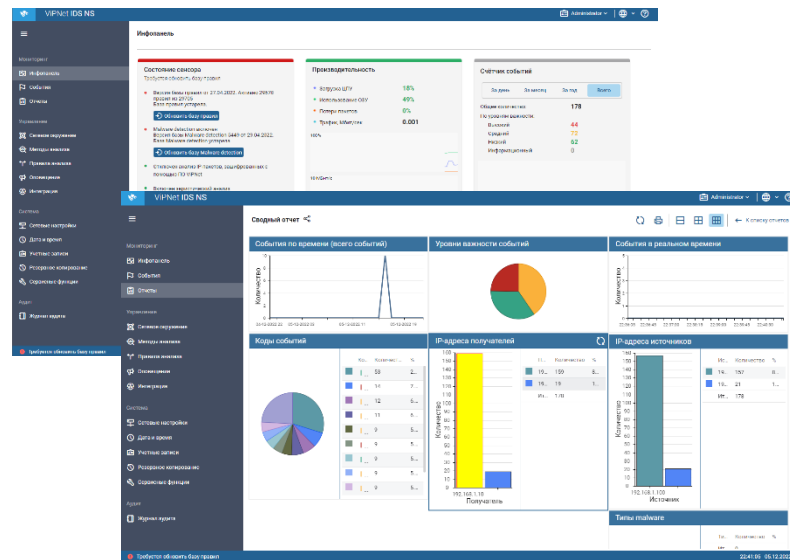
# VIPNet TIAS

- сбор и анализ событий ИБ, поступающих от источников;
- автоматическое выявление подозрений на инциденты ИБ;
- предоставление рекомендаций по реагированию на инцидент;
- формирование отчетов по событиям и инцидентам;
- предоставление возможностей для ручного анализа событий и проведения расследований по инцидентам.



# VIPNet IDS NS

- анализ сетевого трафика с помощью баз решающих правил, сигнатур вредоносного ПО и эвристических методов и выявление событий ИБ;
- хранение событий, пакетов и сессий;
- передача событий во внешние системы;
- передача во внешние системы статистики Netflow;
- пользовательские правила анализа.



# VIPNet IDS HS

- анализ сетевого трафика проходящего через узел;
- выявление подозрительной активности внутри ОС:
  - файловая активность,
  - изменения в реестре,
  - неизвестные процессы.
- выявление подозрительной активности пользователей;
- выявление вредоносного ПО.

Дата, время	Описание	Приоритет	Идентификатор	Устройство	Группа
20.12.2022 15:02:04	Запрос/получение данных для или из файла в процессе	1	200758	WEN784R0P-2	Запросы на подключение
20.12.2022 15:02:04	Сетевой вход в систему	2	600039	WEN784R0P-2	Запросы на подключение
20.12.2022 15:02:05	Сетевой вход в систему	2	500039	WEN784R0P-2	Запросы на подключение
20.12.2022 15:02:05	Сетевой вход в систему	4	600030	WEN784R0P-2	Запросы на подключение
20.12.2022 15:04:45	Неизвестные изменения в процессе файла	1	400030	WEN784R0P-2	Запросы на подключение
20.12.2022 15:05:23	Изменение типа запроса службы (выполн.)	2	100034	WEN784R0P-2	Запросы на подключение
20.12.2022 15:05:42	Удаление задачи планировщика	1	400070	WEN784R0P-2	Запросы на подключение
20.12.2022 15:05:42	Добавление ролевого члена в группу/роль через группу планировщика	1	400029	WEN784R0P-2	Запросы на подключение
20.12.2022 15:05:52	Запрос/получение данных из файла в Temp	2	200035	WEN784R0P-2	Запросы на подключение
20.12.2022 15:05:52	Запрос/получение данных для или из файла в процессе	2	200758	WEN784R0P-2	Запросы на подключение
20.12.2022 15:05:52	Изменение системных служб (выполн.)	14	700030	WEN784R0P-2	Запросы на подключение
20.12.2022 15:05:42	Получение данных о процессе файла	1	400030	WEN784R0P-2	Запросы на подключение
20.12.2022 15:05:27	Изменение типа запроса службы (выполн.)	2	100034	WEN784R0P-2	Запросы на подключение
20.12.2022 15:04:47	Удаление задачи планировщика	1	400070	WEN784R0P-2	Запросы на подключение
20.12.2022 15:05:57	Добавление ролевого члена в группу/роль через группу планировщика	1	600039	WEN784R0P-2	Запросы на подключение
20.12.2022 15:05:47	Запрос/получение данных из файла в Temp	2	200035	WEN784R0P-2	Запросы на подключение
20.12.2022 15:05:47	Запрос/получение данных для или из файла в процессе	2	200758	WEN784R0P-2	Запросы на подключение
20.12.2022 15:05:47	Получение данных о процессе файла	1	400030	WEN784R0P-2	Запросы на подключение
20.12.2022 15:05:47	Изменение системных служб (выполн.)	14	700030	WEN784R0P-2	Запросы на подключение

# VIPNet xFirewall

- выявление подозрительной активности в сетевом трафике с помощью:
  - правил IPS;
  - эвристического и поведенческого анализа;
- блокирование компьютерных атак и подозрительных действий с помощью:
  - фильтров межсетевого экрана;
  - правил IPS + DPI;
  - фильтров контроля приложений.

### Параметры сетевого фильтра

Название:

Состояние:  Включено

Действие:  Блокировать трафик  
 Пропускать трафик  
 Отклонять трафик, с ответом:

Признаки трафика, по группам

- Прикладные протоколы (1)
  - Microsoft Exchange
- Пользователи (1)
  - Ivanov

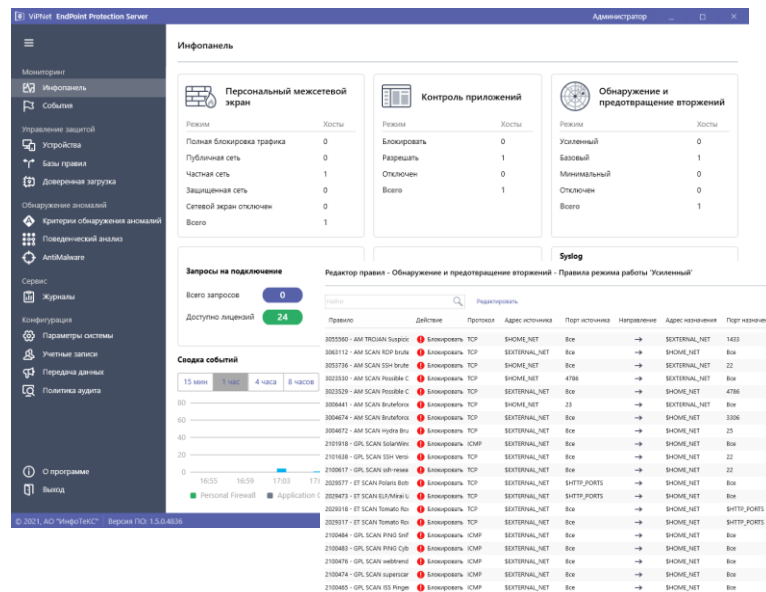
Добавить

- Пользователей
- Приложения
- Протоколы
- Источники
- Назначения
- Расписания

Сетевой фильтр применяется всегда для любого приложения, транспортного протокола, источника и назначения.

# ViPNet Endpoint Protection

- выявление подозрительной активности на конечных рабочих станциях с помощью:
  - правил системы обнаружения и предотвращения вторжений;
  - эвристического анализа Anti-malware;
  - обнаружения аномального поведения системных утилит;
- блокирование компьютерных атак и подозрительных действий с помощью:
  - фильтров Межсетевое экрана
  - списков ПО для Черного и Белого списка
  - правил HIPS



# ViPNet TIAS 3.8

# Новое в версии ViPNet TIAS 3.8



---

## Основные улучшения и новые возможности

### Пользовательские метаправила

возможность написания собственных правил анализа событий и выявления инцидентов

### Дообучение модели

возможность дообучения модели машинного обучения как на новых экспертных данных, так и на размеченных данных пользователей

### Улучшения UX

адаптация web-интерфейса под разные разрешения экранов и повышение удобства работы в ранее реализованных сценариях

# Пользовательские метаправила



# Управление метаправилами

## Экспертные данные

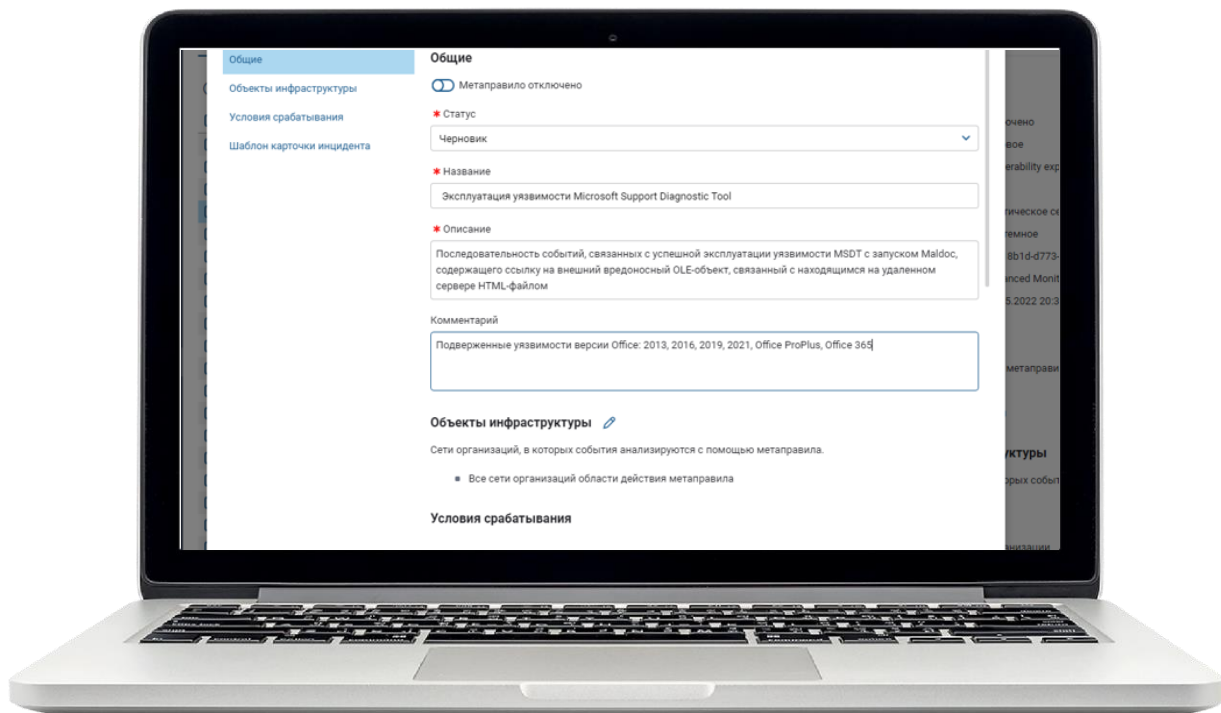
Метаправила анализа событий | Сетевые и узловые правила | Модель машинного обучения | Отчеты сканеров уязвимостей | Обновление экспертных данных

Создать метаправило | Загрузить пользовательские метаправила | Скачать таблицу

940 метаправило

Критическое сетевое событие	Состояние	Статус	Тип	Источник	Область действия	Родительское метаправило	Дата изменения
Критическое сетевое событие							
Критическое сетевое событие							
Повторяющееся сетевое событие	<input type="checkbox"/>	Готовое	Контроль доступа по GeoIP	Пользовательское	Все организации	1e9c0db3-71c4-4b7d-816a-3...	02.12.2022 16:20:06
Последовательность событий	<input type="checkbox"/>	Готовое	Контроль доступа по GeoIP	Пользовательское	Все организации	auth_not_from_us	02.12.2022 16:20:06
Набор событий	<input type="checkbox"/>	Готовое	Контроль доступа по GeoIP	Пользовательское	Все организации	auth_not_from_us	02.12.2022 16:20:06
Контроль доступа по GeoIP	<input type="checkbox"/>	Готовое	Набор событий	Пользовательское	Все организации	06a3d605-16ff-4b0d-a22f-9d...	02.12.2022 16:20:06
<input type="checkbox"/> Authorized logon from outside the South Africa copy 3	<input type="checkbox"/>	Готовое	Контроль доступа по GeoIP	Пользовательское	Все организации	auth_not_from_za	02.12.2022 16:20:06
<input type="checkbox"/> Authorized logon from outside the South Africa copy 2	<input type="checkbox"/>	Готовое	Контроль доступа по GeoIP	Пользовательское	Все организации	auth_not_from_za	02.12.2022 16:20:06
<input type="checkbox"/> Account compromise copy 4	<input type="checkbox"/>	Готовое	Набор событий	Пользовательское	Все организации	comprometation_creds	02.12.2022 16:20:06
<input type="checkbox"/> Account compromise copy 3	<input type="checkbox"/>	Готовое	Набор событий	Пользовательское	Все организации	comprometation_creds	02.12.2022 16:20:06
<input type="checkbox"/> Authorized logon from outside the South Africa copy 1	<input type="checkbox"/>	Готовое	Контроль доступа по GeoIP	Пользовательское	Все организации	auth_not_from_za	02.12.2022 16:20:06
<input type="checkbox"/> Account compromise	<input checked="" type="checkbox"/>	Готовое	Набор событий	Системное	Все организации		02.12.2022 16:20:06
<input type="checkbox"/> Scanning with possible penetration to the system	<input checked="" type="checkbox"/>	Готовое	Последовательность событий	Системное	Все организации		02.12.2022 16:20:06
<input type="checkbox"/> Adding a host to botnet	<input checked="" type="checkbox"/>	Готовое	Набор событий	Системное	Все организации		02.12.2022 16:20:06
<input type="checkbox"/> Successful ProxyLogon vulnerability exploitation	<input checked="" type="checkbox"/>	Готовое	Набор событий	Системное	Все организации		02.12.2022 16:20:06
<input type="checkbox"/> Activity of Trojan-Downloader.MSWord.Agent.mu	<input checked="" type="checkbox"/>	Готовое	Набор событий	Системное	Все организации		02.12.2022 16:20:06
<input type="checkbox"/> Signs of the Dridex Trojan download	<input checked="" type="checkbox"/>	Готовое	Набор событий	Системное	Все организации		02.12.2022 16:20:06
<input type="checkbox"/> Downloading malware related to IcedID	<input checked="" type="checkbox"/>	Готовое	Набор событий	Системное	Все организации		02.12.2022 16:20:06
<input type="checkbox"/> Code execution in Thecus N4800Eco NAS Server Control Panel	<input checked="" type="checkbox"/>	Готовое	Набор событий	Системное	Все организации		02.12.2022 16:20:06
<input type="checkbox"/> Exploit of the remote execution vulnerability in the Moodle spellchecker plugin 3.10	<input checked="" type="checkbox"/>	Готовое	Набор событий	Системное	Все организации		02.12.2022 16:20:06
<input type="checkbox"/> Attempt to inject a code aimed at loading and executing a malicious script	<input checked="" type="checkbox"/>	Готовое	Набор событий	Системное	Все организации		02.12.2022 16:20:06
<input type="checkbox"/> Meterpreter activity	<input checked="" type="checkbox"/>	Готовое	Набор событий	Системное	Все организации		02.12.2022 16:20:06
<input type="checkbox"/> Authorized logon from outside the South Africa	<input type="checkbox"/>	Готовое	Контроль доступа по GeoIP	Системное	Все организации		02.12.2022 16:20:06
<input type="checkbox"/> Authorized logon from outside the United States	<input type="checkbox"/>	Готовое	Контроль доступа по GeoIP	Системное	Все организации		02.12.2022 16:20:06
<input type="checkbox"/> Authorized logon from outside the Turkey	<input type="checkbox"/>	Готовое	Контроль доступа по GeoIP	Системное	Все организации		02.12.2022 16:20:06

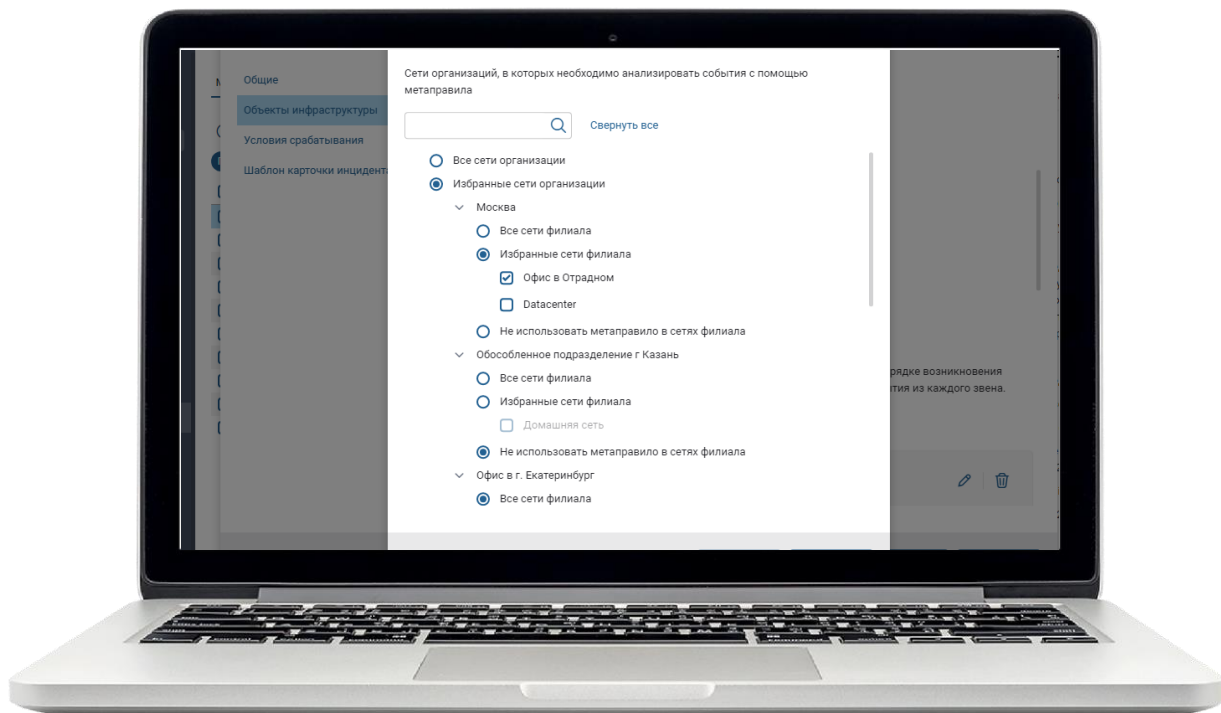
# Создание нового метаправила



## Шаблоны метаправил:

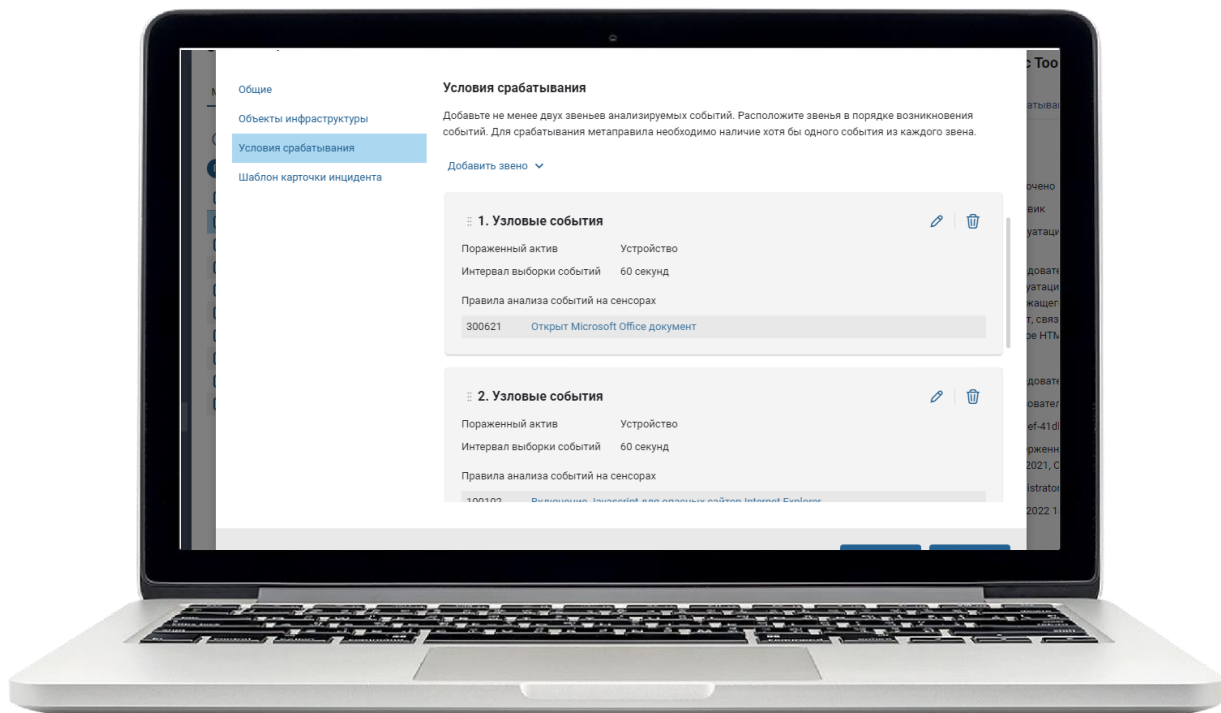
- критическое сетевое событие;
- критическое узловое событие;
- повторяющееся сетевое событие;
- последовательность событий;
- набор событий;
- контроль доступа по GeoIP.

# Назначение метаправил на объекты инфраструктуры



Назначение  
метаправил на любой  
уровень  
инфраструктуры с  
точностью до подсети

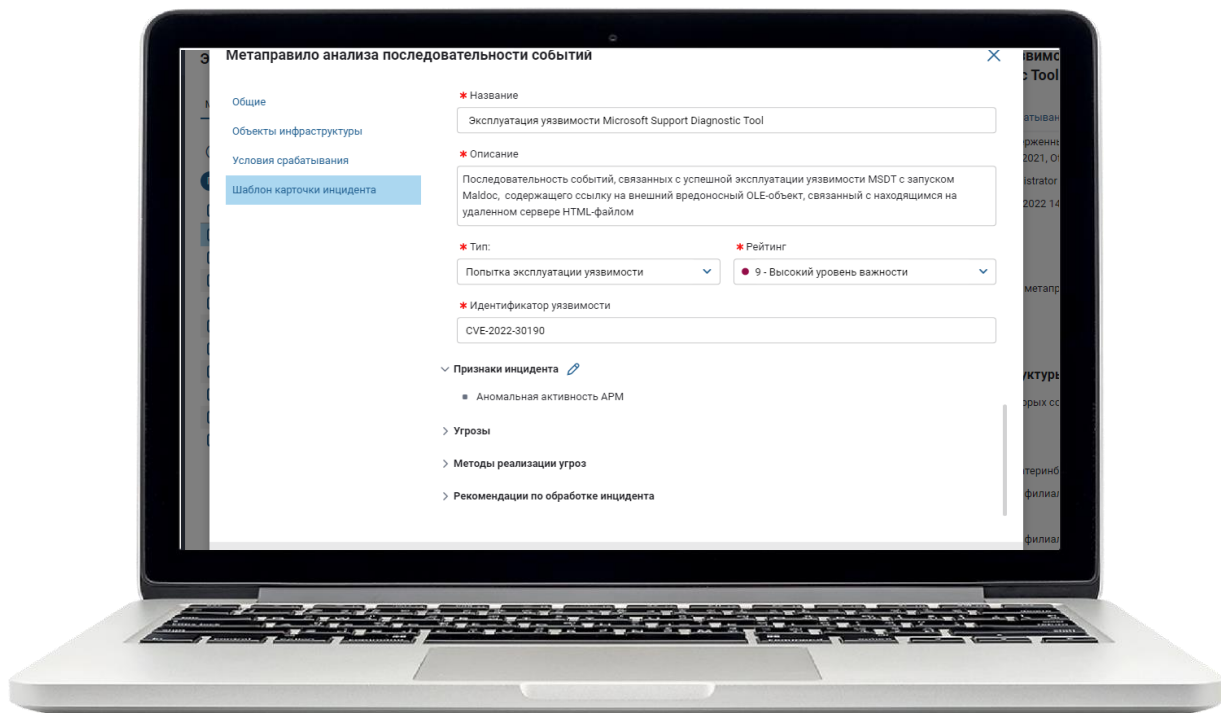
# Условия срабатывания правила



## Выбор условий:

- направление атаки;
- интервал выборки событий;
- порядок следования событий;
- сетевые и узловые правила.

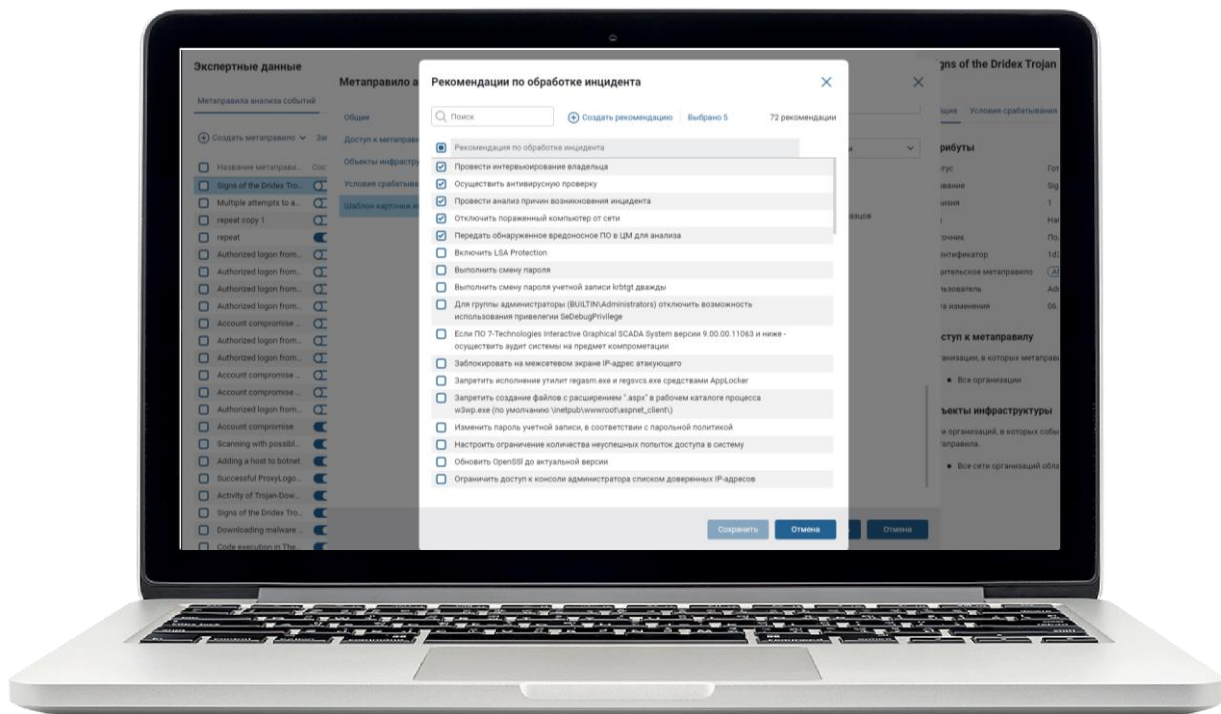
# Шаблон карточки инцидента



## Шаблон инцидента:

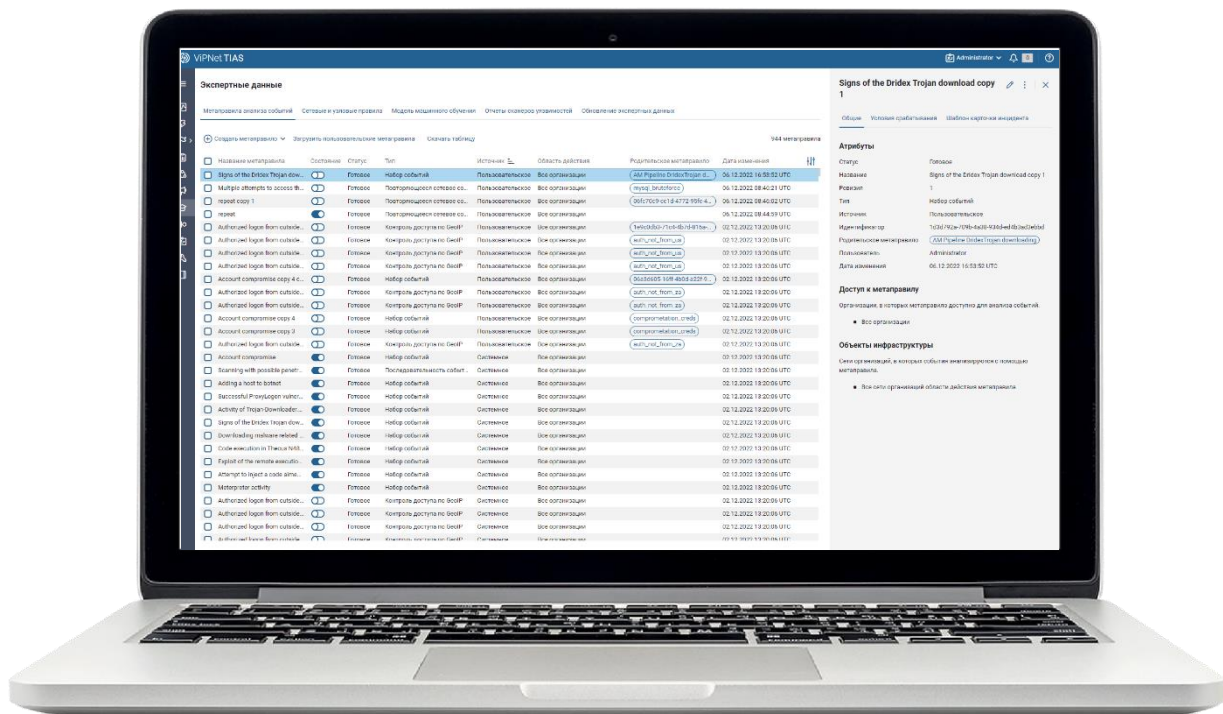
- название;
- описание;
- тип инцидента;
- рейтинг;
- идентификатор уязвимости;
- признаки инцидента;
- угрозы;
- методы реализации угроз;
- рекомендации по обработке.

# Рекомендации по обработке инцидента



Выберите набор рекомендаций из представленного списка или добавьте свои

# Работа с правилами



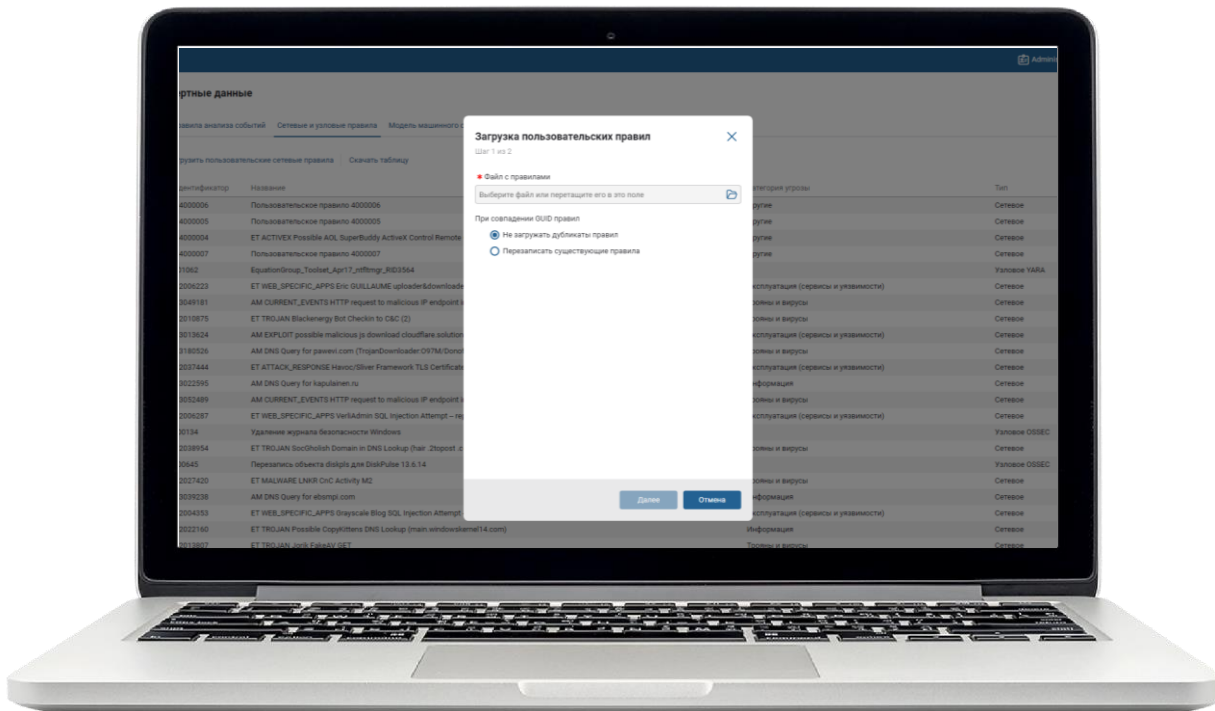
Для ввода правила в действие необходимо:

- назначить область действия правила;
- перевести из статуса «черновик» в статус «готовое»;
- включить правило

# Пользовательские правила IDS NS



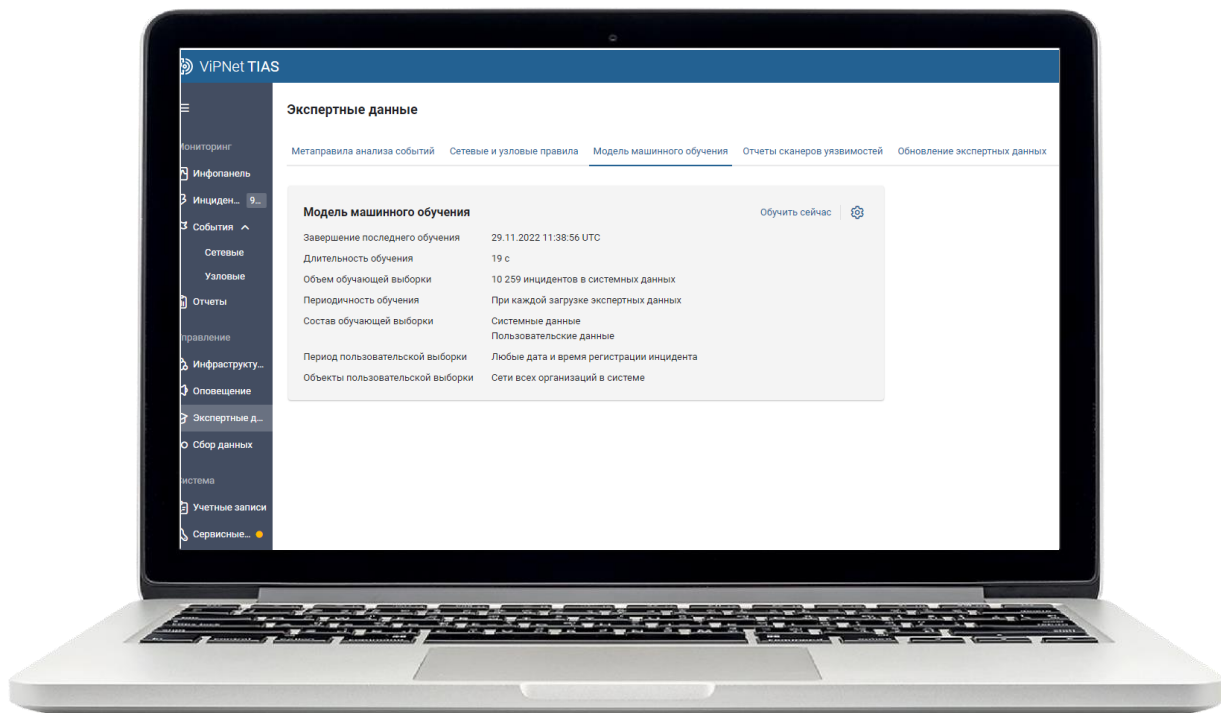
Для выявления инцидентов на основе событий, сработавших на пользовательские правила, необходимо загрузить пользовательскую БП в TIAS.





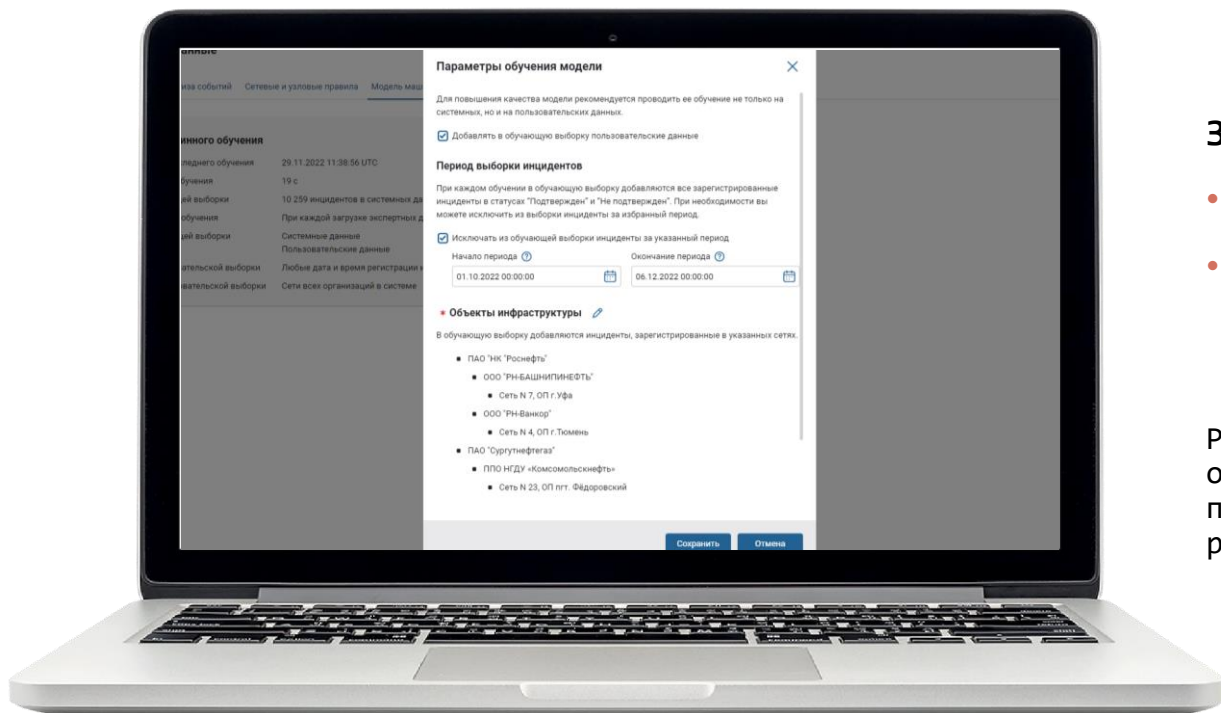
# Дообучение математической модели принятия решений

# Статистика обучения модели



- время завершения последнего обучения;
- длительность последнего обучения;
- объем обучающей выборки;
- периодичность обучения;
- состав обучающей выборки

# Параметры обучения модели



## Задайте:

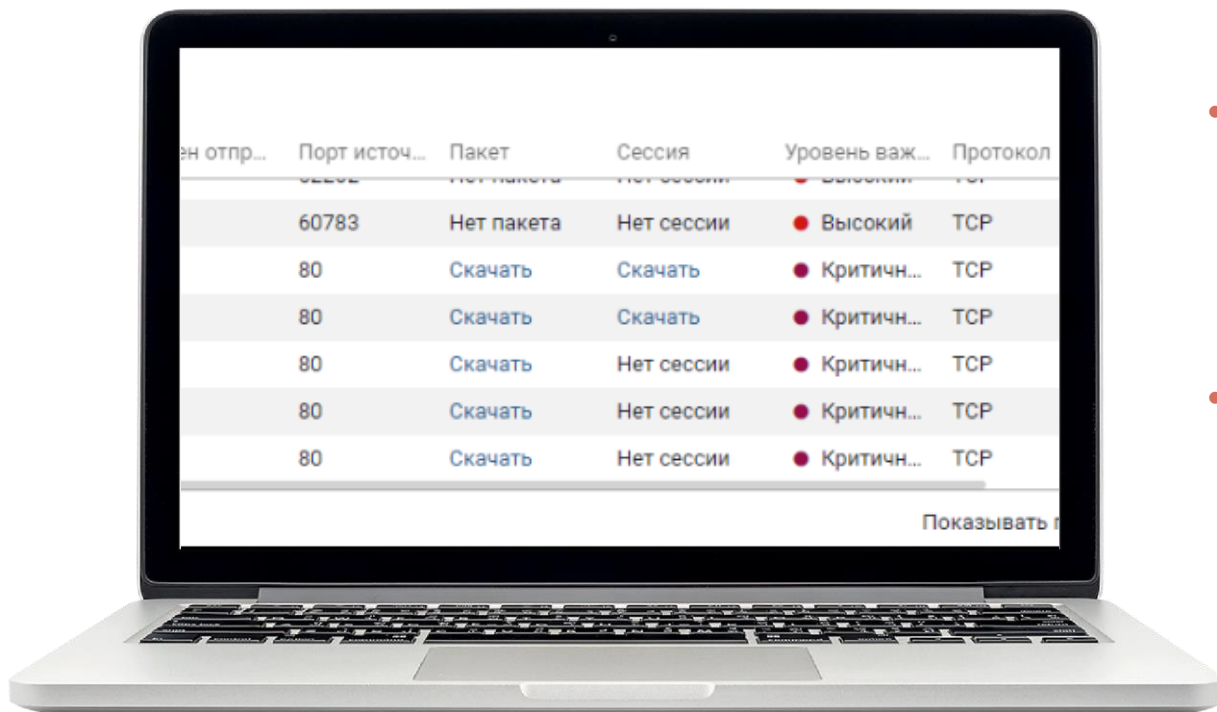
- Периодичность обучения
- Состав обучающей выборки



Рекомендуем добавлять в обучающую выборку пользовательские данные при размеченных статусах инцидентов

# Улучшения пользовательских сценариев

# Передача записи сессии из IDS NS в TIAS



- Отображение статуса наличия пакета и сессии для скачивания по каждому событию
- Возможность скачивания с IDS NS как одного сетевого пакета, так и записанной сессии;

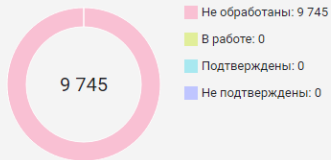
# Главная инфопанель

- Мониторинг
- Инфопанель
- Инциденты 99+
- События
- Сетевые
- Узловые
- Отчеты
- Управление
- Инфраструктура
- Оповещение
- Интеграция
- Экспертные данные
- Сбор данных
- Система
- Учетные записи
- Сервисные функции
- Аудит
- Журнал аудита

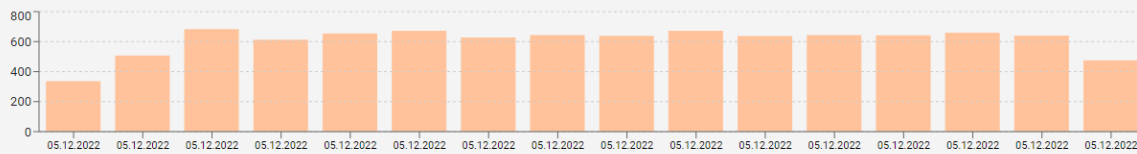
## Инфопанель

Инфраструктура 15 М 1 ч 24 ч 05.12.2022 17:44:42 - 05.12.2022 17:59:42 Автообновление

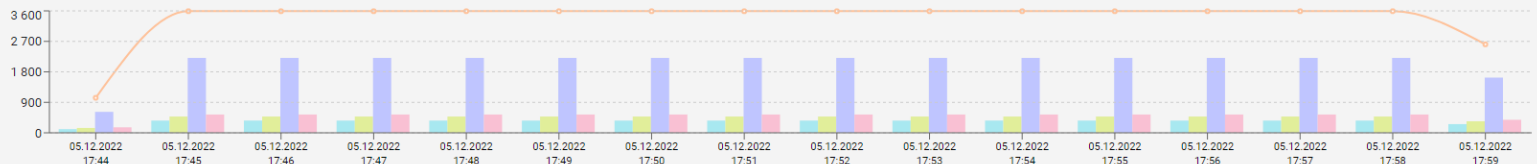
### Инциденты



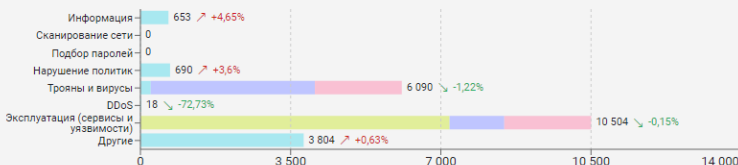
### Динамика инцидентов



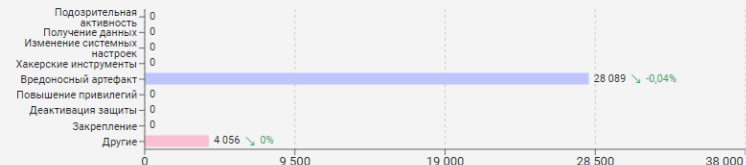
### События



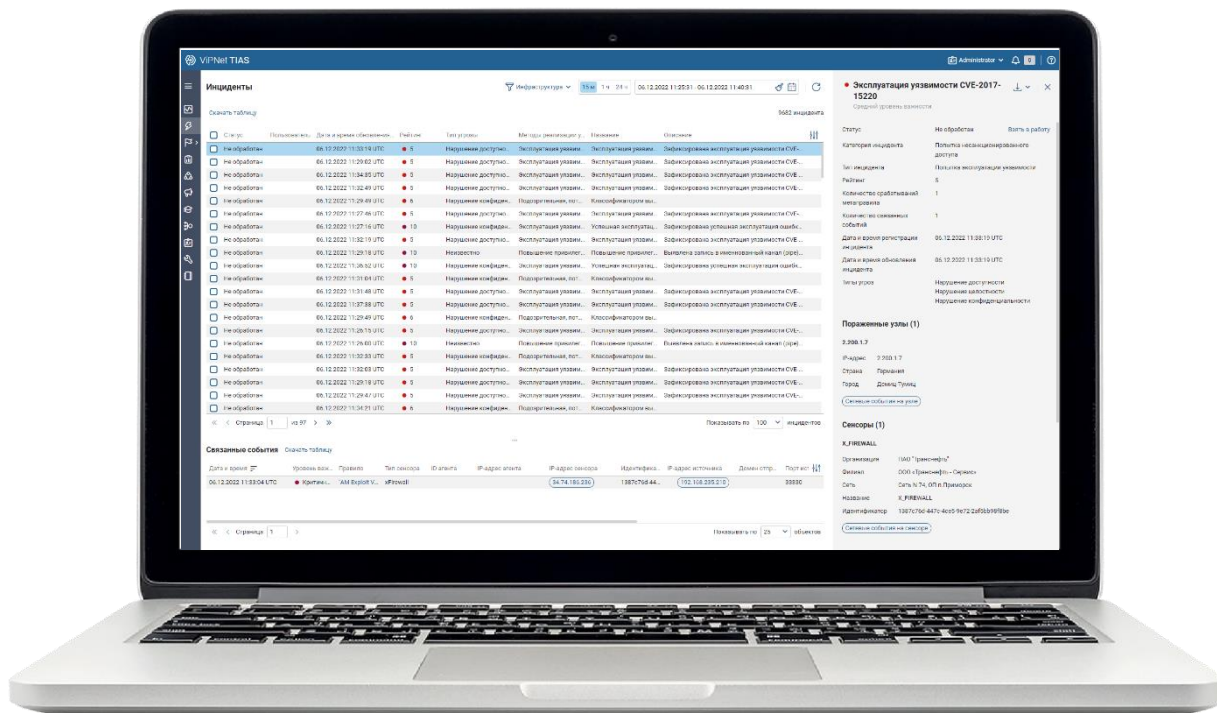
### Сетевые события



### Узловые события



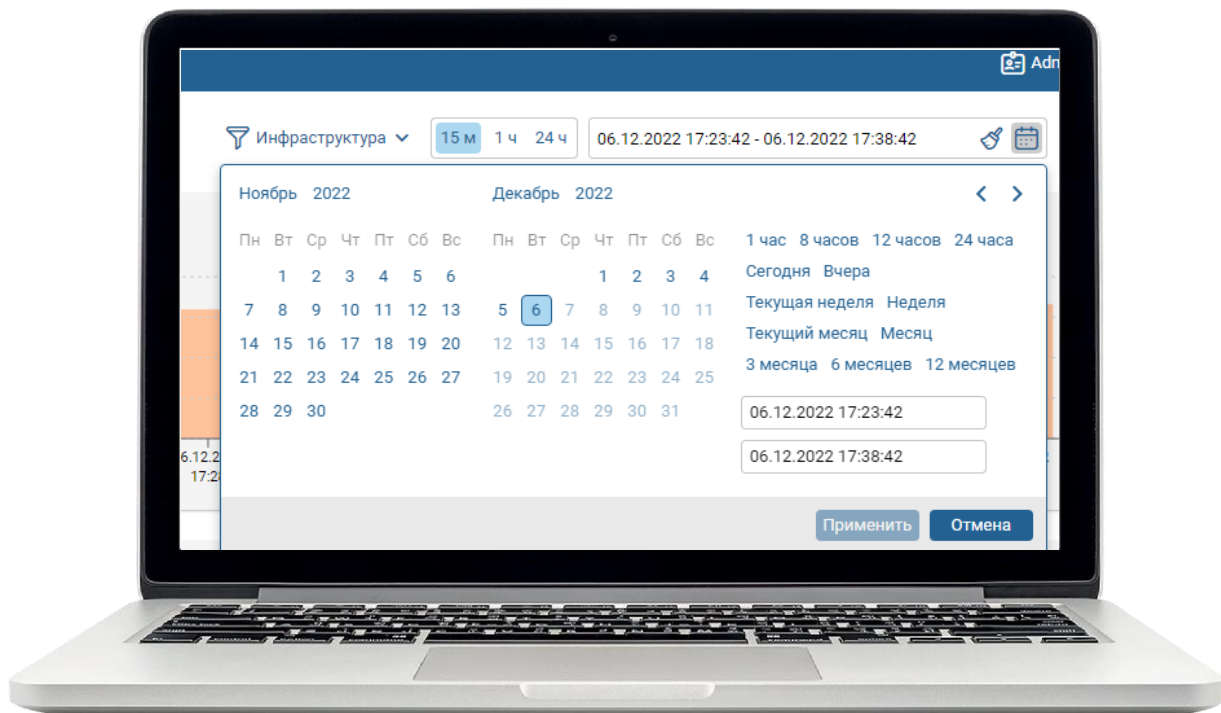
# Настройка размеров отображаемых областей



- Динамическая подстройка размеров отображаемых областей в зависимости от размера окна.
- Ручная настройка размеров фреймов



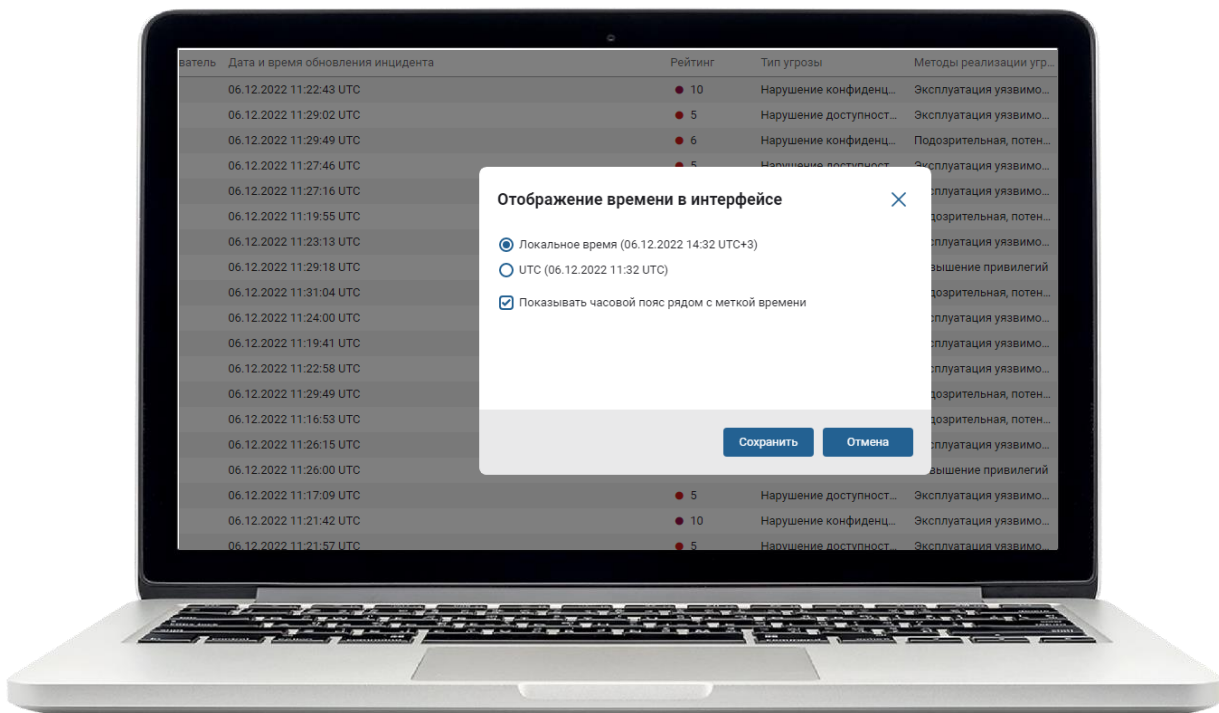
# Задание глобального фильтра отображения данных



Задавайте время отображения в глобальном фильтре в один клик

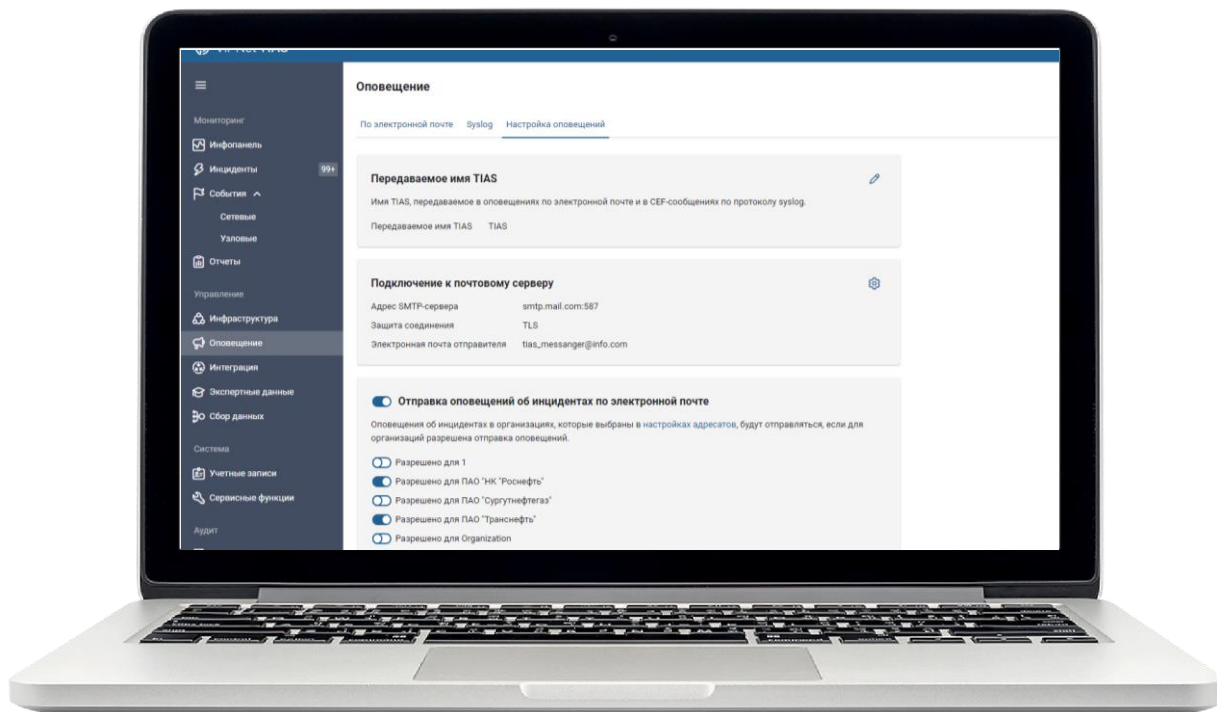


# Синхронизация и отображение времени



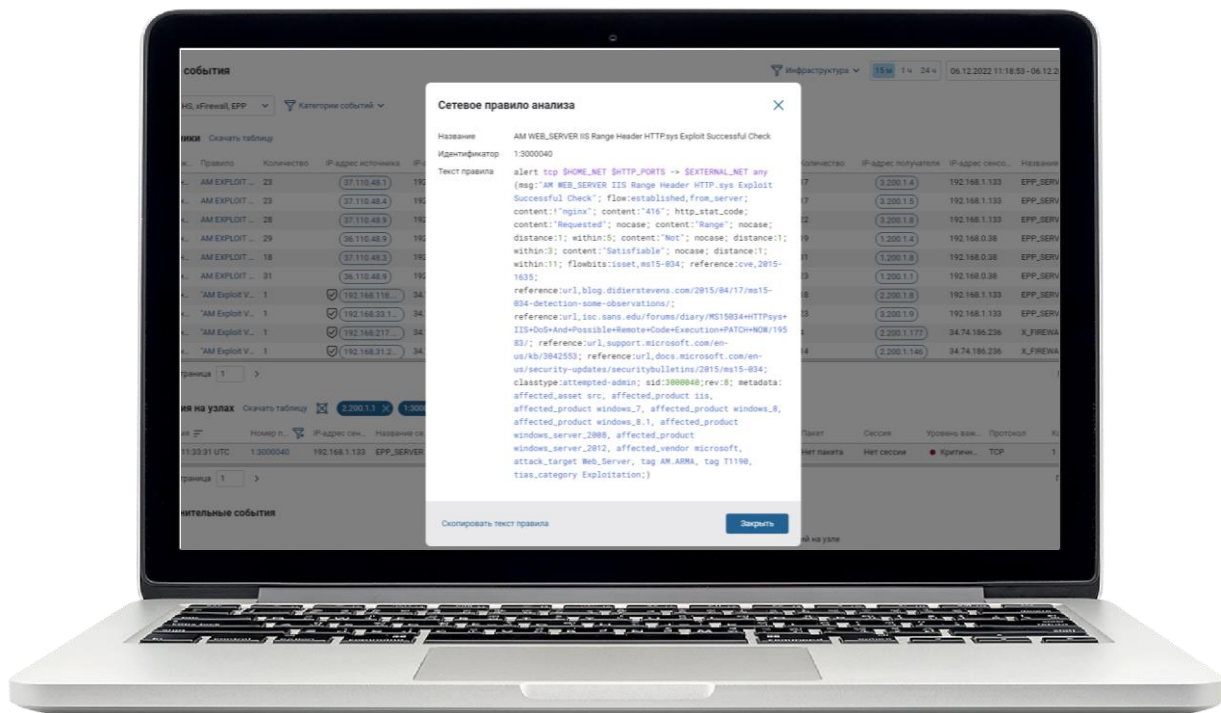
- Отображение в интерфейсе локального времени или времени в формате UTC;
- Синхронизация времени с IDS MC

# Настройка оповещений



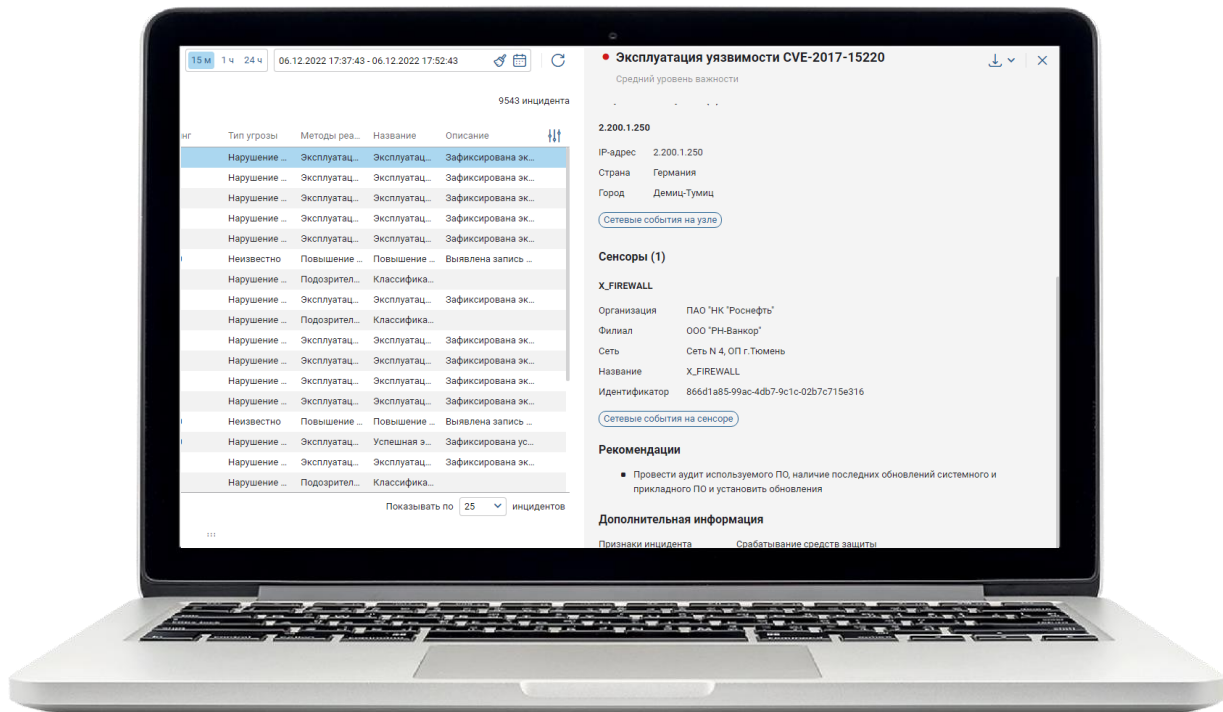
Настройка имени  
TIAS, передаваемого  
во внешние системы

# Разметка правила



Отображение текста  
правила с цветовой  
разметкой

# Отображение информации об инфраструктуре в карточке инцидента



- Отображение информации о принадлежности пораженных активов инфраструктуре в карточке инцидента;
- Передача всех параметров инцидента по syslog

# Улучшения в IDS MC и IDS NS



---

## Основные улучшения и новые возможности

### Централизованное обновление пользовательских БРП

загрузка с IDS NS и отправка на другие сенсоры пользовательской базы решающих правил

**Подключение работающего TIAS к IDS MC**  
передача с TIAS в IDS MC информации об инфраструктуре и подключенных устройствах

### Обмен информацией об инфраструктуре между IDS MC

Инфраструктура, заведенная в IDS MC сервис-провайдера передается в IDS MC заказчика

## Исполнения IDS NS:

### ПАК:

- ПАК ViPNet IDS NS100 X2;
- ПАК ViPNet IDS NS1000 Q3;
- ПАК ViPNet IDS NS2000 Q4;
- ПАК ViPNet IDS NS10000 Q1;

### ПО:

- ViPNet IDS NS VA 100;
- ViPNet IDS NS VA 500;
- ViPNet IDS NS VA 1000;
- ViPNet IDS NS VA 2000;
- ViPNet IDS NS VA 5000;

## **Поддержка записи сессий на низкопроизводительных платформах**

- регулирование времени записи сессии
- запись сессии с определенного IP

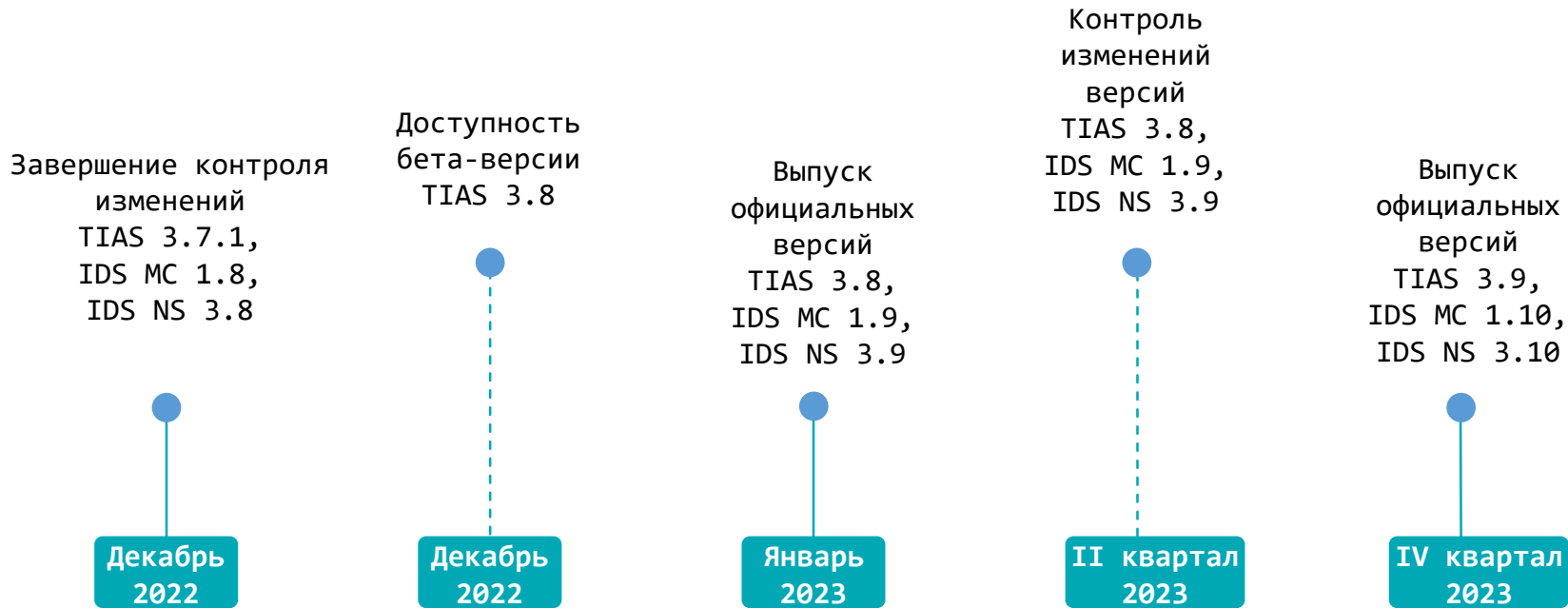
## **Математическая модель анализа Netflow** новый эвристический способ анализа аномалий в сетевом трафике

## **Выгрузка пользовательских БРП** возможность выгрузки пользовательских БРП для передачи в TIAS и IDS MC

# Планы развития



# Таймлайн выпуска версий продуктов





---

## Новые возможности и улучшения

**Ретроспективный анализ событий в TIAS**  
возможность поиска инцидентов в событиях, сохраненных в базе TIAS

### Интеграция с ViPNet Prime

IDS MC и TIAS

**Создание карточки инцидента вручную**  
Возможность самостоятельно заводить инциденты на основании событий в TIAS

### Улучшение работы моделей TIAS и IDS NC

- новые алгоритмы работы модели TIAS;
- расширенный анализ Netflow в IDS NS



Спасибо за внимание!

Светлана Старовойт

Руководитель направления развития  
продуктов

e-mail: [starovoytsg@infotecs.ru](mailto:starovoytsg@infotecs.ru)

---

Подписывайтесь на наши соцсети

---



[vk.com/infotecs\\_news](https://vk.com/infotecs_news)



[t.me/infotecs\\_official](https://t.me/infotecs_official)



[rutube.ru/channel/24686363](https://rutube.ru/channel/24686363)