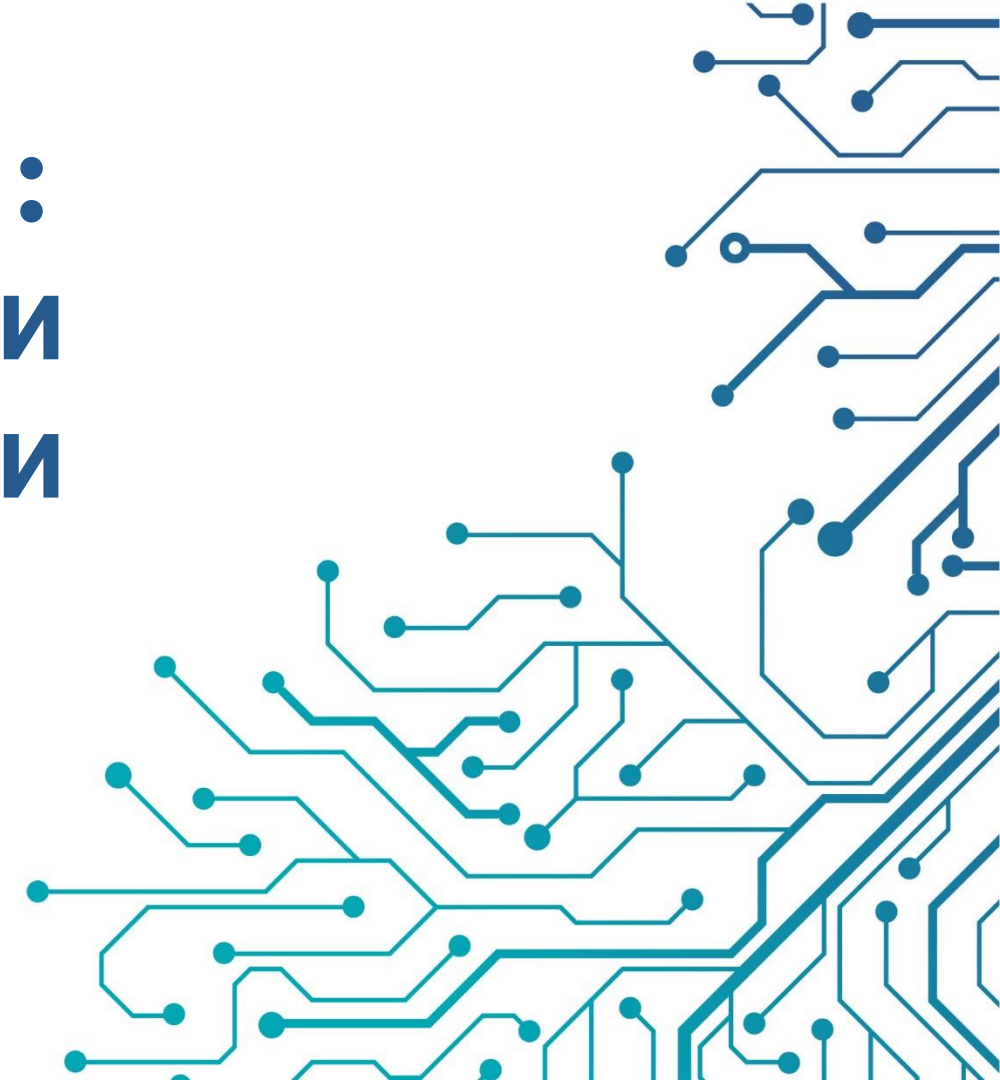
ViPNet IDS 3: новые функции и возможности

Светлана Старовойт
руководитель продуктового решения



infotecs

План вебинара

- Система ViPNet IDS 3
- Комплект поставки сертифицированной версии
- Реестры ПО и ПАК
- Новое в сертифицированной версии

Система обнаружения компьютерных атак (вторжений) ViPNet IDS 3

ViPNet IDS NS

ViPNet TIAS

ViPNet IDS MC

Обязательный компонент

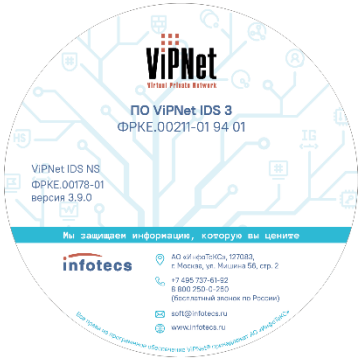
Не обязательные компоненты

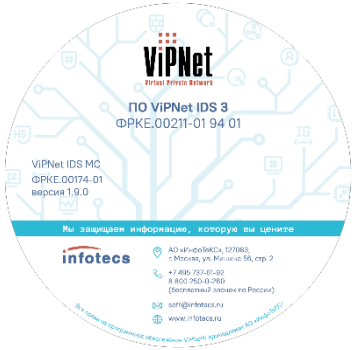
Система обнаружения вторжений уровня сети 4 класс

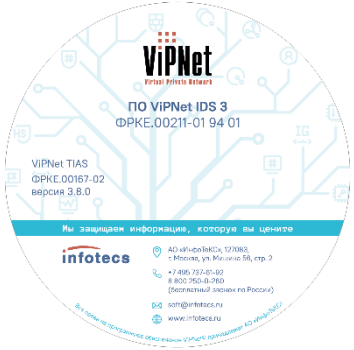
Требования доверия безопасности 4 уровня

Система обнаружения компьютерных атак класс В

Комплект поставки

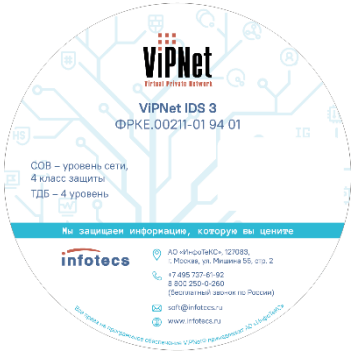




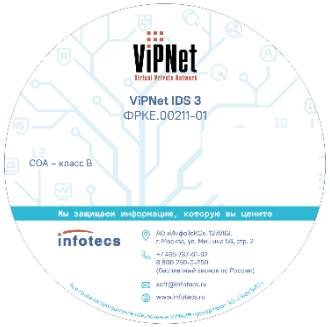


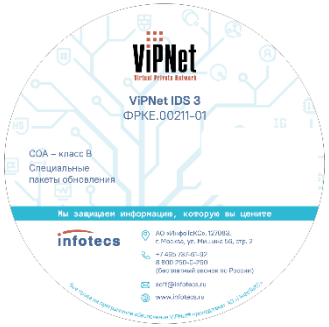
Полный комплект для первичной поставки и обновления!

Комплект ПО и документации на компоненты



Диск с документацией.
сертификация ФСТЭК





Диски с документацией и спец. ПО
сертификация ФСБ

Сертифицированные версии

Сертифицированные версии:

- ViPNet IDS NS 3.9
- ViPNet TIAS 3.8
- ViPNet IDS MC 1.8

Комплекты обновления:

- **ViPNet IDS NS:** 3.6.0-3.6.1; 3.6.1-3.8.0; 3.8.0-3.9.0
- **ViPNet TIAS:** 3.5.1-3.7.1. 3.8.0 – новая прошивка!
- **ViPNet IDS MC:** 1.8.0-1.9.0

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4329

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 24 ноября 2020 г.

Выдан: 24 ноября 2020 г.
Действителен до: 24 ноября 2025 г.

Настоящий сертификат удостоверяет, что **система обнаружения компьютерных атак (вторжений) ViPNet IDS 3**, разработанная и производимая АО «ИнфоТеКС», является системой обнаружения вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012).

Сертификат выдан на основании технического заключения от 30.09.2020, оформленного по результатам сертификационных испытаний испытательной лабораторией МОУ «ИИФ» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 27.10.2020, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «ИнфоТеКС»
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

НАЧАЛЬНИК 2 УПРАВЛЕНИЯ ФСТЭК РОССИИ

Д.Шевцов

Варианты исполнения

	IDS NS	ViPNet TIAS	ViPNet IDS MC
Новые АП	IDS NS100 Q1	TIAS 1000 Q2	-
	IDS NS100 Q2	TIAS 2000 Q3	
	IDS NS1000 Q3	TIAS 5000 Q2	
	IDS NS2000 Q4	TIAS 10000 Q1	
	IDS 10000 Q1		
Поддержка АП	IDS NS100 N1	1000 Q1	-
	IDS NS100 X1	TIAS 2000 Q2	
	IDS NS1000 Q1	TIAS 5000 Q1	
	IDS NS1000 Q2		
	IDS NS2000 Q1		
	IDS NS2000 Q2		
	IDS NS2000 Q3		
Среды виртуализации	Microsoft Hyper-V	Microsoft Hyper-V	Microsoft Hyper-V
	VMware ESXi	VMware ESXi	VMware ESXi
	Oracle VM VirtualBox	VMware Workstation Pro	VMware Workstation Pro
	Workstation Pro	Oracle VM VirtualBox	Oracle VM VirtualBox
		Proxmox VE	Oracle Virtual Server
		ПК СВ «Брест»	Proxmox VE

Реестры

Единый реестр российских программ:

- **ViPNet IDS NS**
  (* Программное обеспечение относится к сфере искусственного интеллекта)
- **ViPNet TIAS**
  (* Программное обеспечение относится к сфере искусственного интеллекта)
- **ViPNet IDS**

03.14 Средства обнаружения и/или предотвращения вторжений (атак)
03.02 Средства управления событиями информационной безопасности
03.15 Средства обнаружения угроз и расследования сетевых инцидентов

Реестр российской радиоэлектронной продукции:

- ПАК ViPNet IDS NS
- ПАК ViPNet TIAS

Подтверждение производства продукции на территории РФ

ViPNet IDS 3

ПРЕИМУЩЕСТВА

Использование алгоритмов машинного обучения

Ввод в эксплуатацию за несколько дней

Ежедневно обновляемые собственные базы правил и сигнатур вредоносного ПО

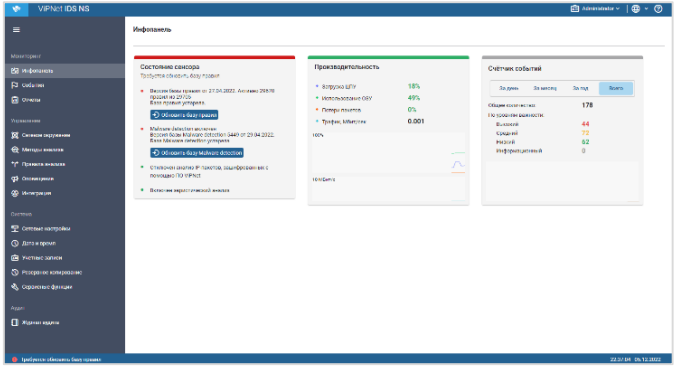
Подключение к ГосСОПКА

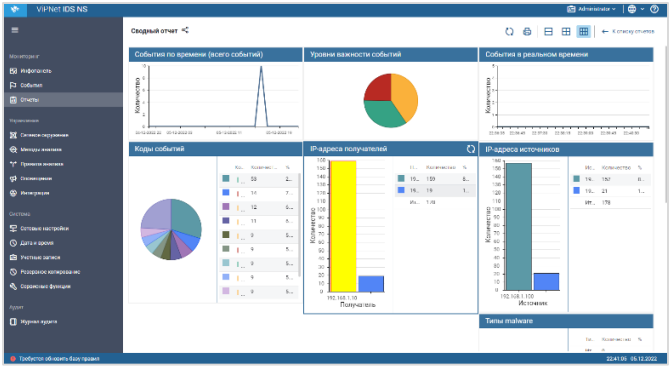
Компоненты системы

Управление	ViPNet IDS MC
Анализ	ViPNet TIAS
Обнаружение	ViPNet IDS NS

ViPNet IDS NS

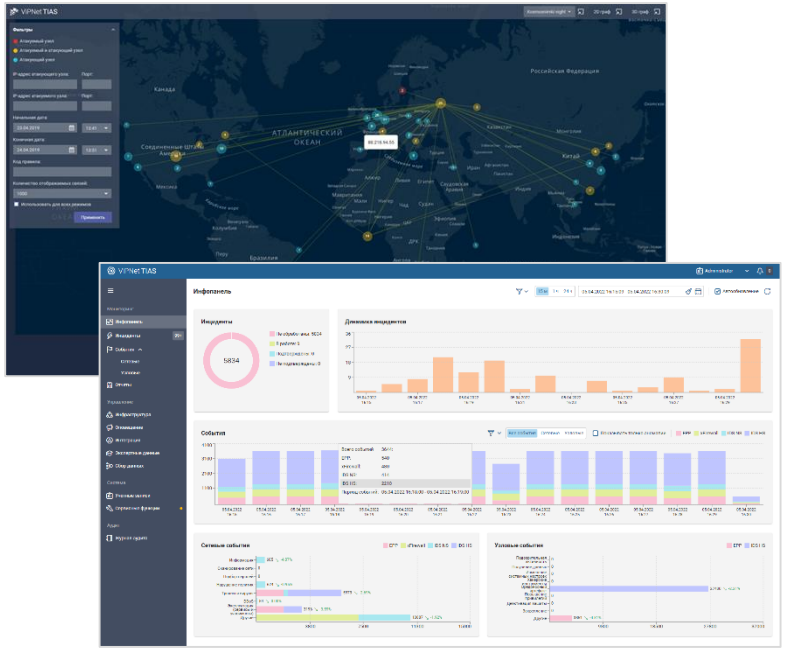
- анализ сетевого трафика с помощью баз решающих правил, сигнатур вредоносного ПО и эвристических методов и выявление событий ИБ
- хранение событий, пакетов и сессий
- передача событий во внешние системы
- передача во внешние системы статистики Netflow
- пользовательские правила анализа





ViPNet TIAS

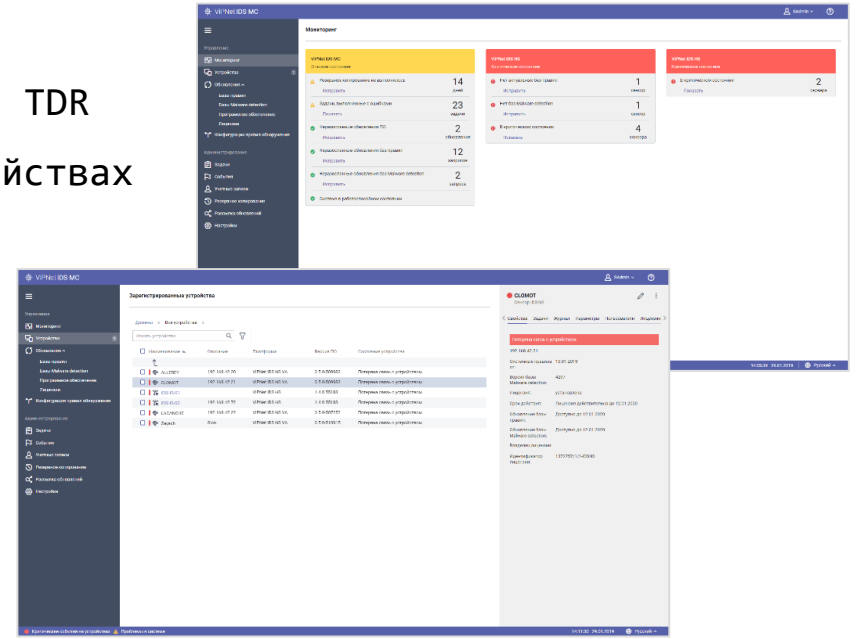
- сбор и анализ событий ИБ, поступающих от источников
- автоматическое выявление подозрений на инциденты ИБ
- предоставление рекомендаций по реагированию на инцидент
- формирование отчетов по событиям и инцидентам



https://infotecs.ru/webinars/archive/demonstratsiya-vozmozhnostey-resheniya-tdr-v-usloviyakh-provedeniya-setevoy-ataki.html

ViPNet IDS MC

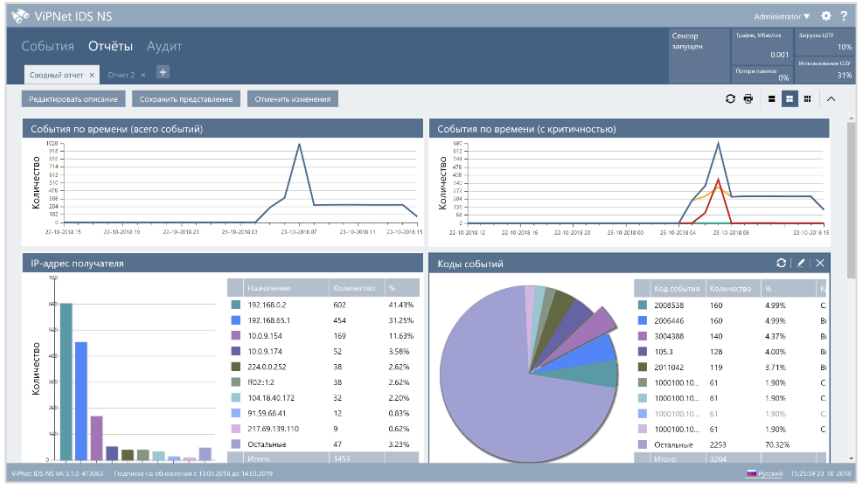
- ввод в эксплуатацию сенсоров IDS
- управление инфраструктурой решения ViPNet TDR
- управление конфигурациями правил на устройствах
- обновление:
  - баз решающих правил
  - сигнатур вредоносного ПО
  - экспертных данных
  - программного обеспечения устройств
  - лицензий
- мониторинг состояния устройств



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

Новое в версиях

ViPNet IDS NS



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

Поддержка записи сессий

- регулирование времени записи сессии
- запись сессии с определенного IP

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

ViPNet TIAS

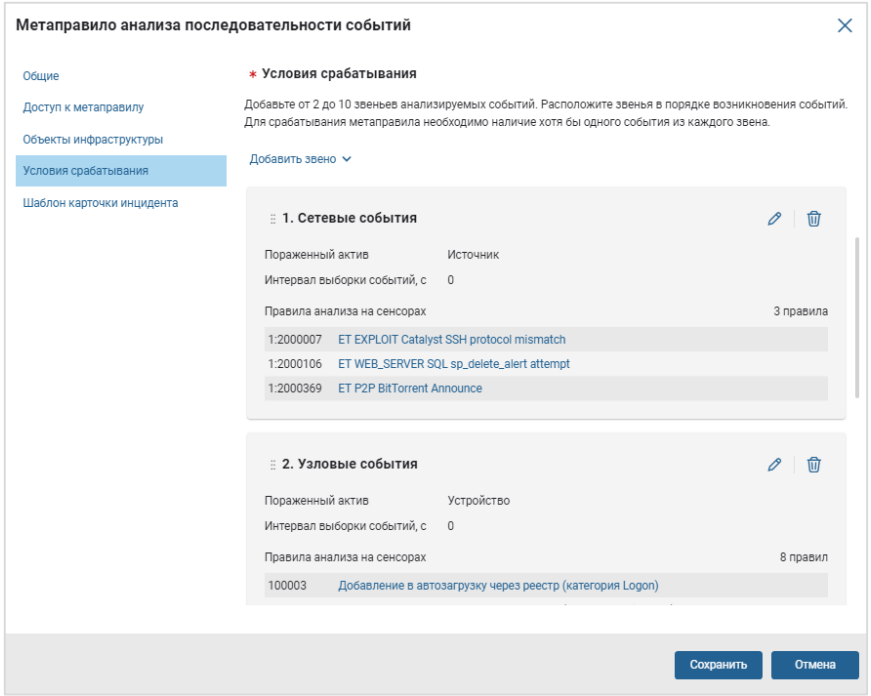
Основные улучшения и новые возможности

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

Новый источник событий
Прием и обработка событий ИБ, от шлюза безопасности ViPNet Coordinator HW 5

Пользовательские метаправила

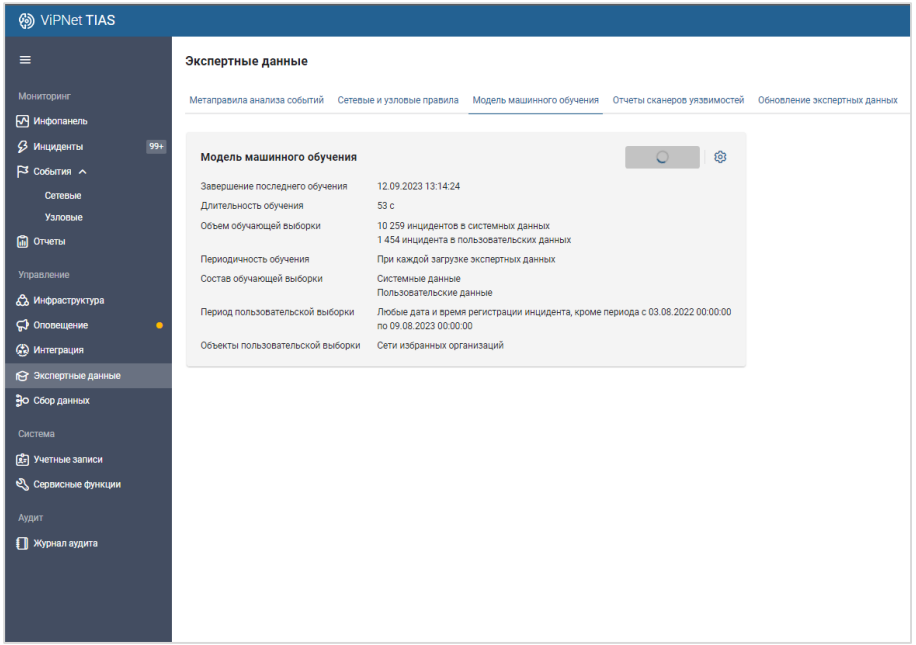


6 алгоритмов анализа событий:

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

анализ событий, сработавших на пользовательские правила IDS

назначение метаправил на любой уровень инфраструктуры



Дообучение модели

- обучение модели на пользовательских и системных данных
- снижение false positive rate при выявлении инцидентов

ViPNet IDS MC

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

21 09 2023 МОСКВА

ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

ТЕХНО infotecs ФЕСТ

ТЕХНО infotecs 2023 ФЕСТ

- Расскажу о планах развития решения
- Покажу новые версии продуктов
- Покажу на мастер-классах работу алгоритмов машинного обучения TIAS и IDS NS
- Покажу на реальном кейсе как создавать собственные правила анализа событий

Регистрируйтесь на сайте!

ТЕХНО infotecs ФЕСТ 2023

infotecs

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363