



техно infotecs  
2021 Фест

ТЕХНИЧЕСКИЙ  
ФЕСТИВАЛЬ

# MDR-сервисы на базе решения ViPNet TDR

Светлана Старовойт

# Что такое MDR?

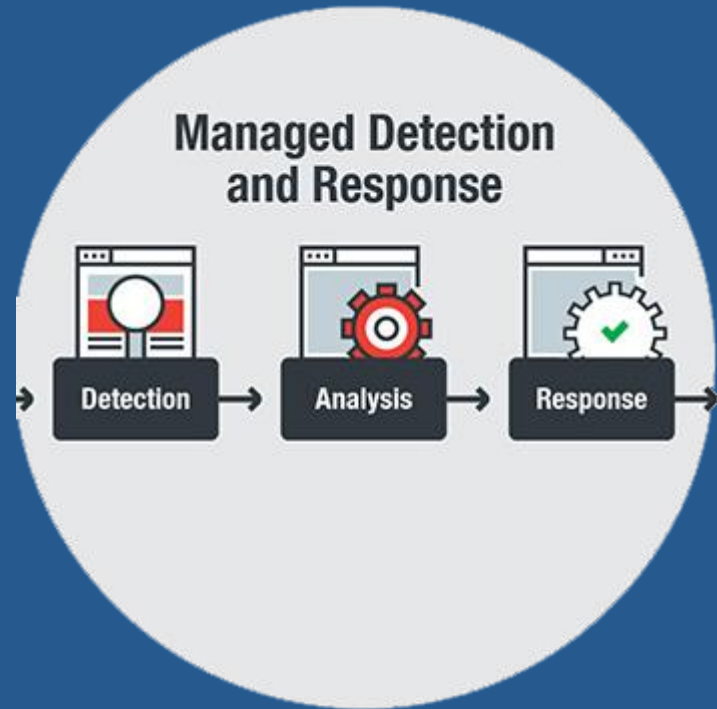


- **Управляемое обнаружение и реагирование (MDR)** — это служба кибербезопасности, которая сочетает в себе технологии и человеческий опыт для поиска, мониторинга и реагирования на угрозы.
- **Основное преимущество MDR** заключается в том, что он помогает быстро выявлять и ограничивать влияние угроз без необходимости в дополнительном персонале.  
*(с) 2021 Managed Detection and Response (MDR) Services Buyers Guide*

Прогноз Gartner: к 2025 году 50% организаций будут использовать сервисы MDR

# Как работает MDR?

- Приоритизация и анализ событий;
- Threat Hunting;
- Проведение расследования;
- Реагирование;
- Устранение последствий.



# Что отличает MDR Security от других решений?

SEARCH

SCANNING

SEARCH  
SCANNING

# MDR vs EDR



## EDR:

- Отслеживает и сохраняет поведение и события на конечных точках;
- Может автоматически блокировать известную угрозу;
- Нет полной картины для выявления сложных угроз;
- EDR – часть MDR.

# MDR vs MSSP



## MSSP:

- Являются предшественниками MDR;
- Включают более широкий спектр ИБ-услуг (управление активами, обновлениями, уязвимостями);
- Обычно не реагируют на угрозы активно;
- Клиенты MSSP должны привлекать дополнительных консультантов для выявления и расследования сложных угроз.

# MDR vs SIEM

## Причины неудовлетворенности системой SIEM © IDC



Все SIEM объединяет то, что их клиенты сталкиваются с трудностями в понимании результатов работы SIEM. 45% пользователей SIEM говорят, что им не хватает собственных знаний для полноценного использования своего решения SIEM. SIEM также могут быть дорогими и ресурсоемкими.

(c) 2021 Managed Detection and Response (MDR) Services Buyers Guide





# Бизнес-факторы внедрения MDR

# Драйвер №1: Нужны сложные дорогие инструменты

## Old School Versus New School Security Products

### Old School Rule Based

SIEM broad scope monitoring

Intrusion detection and prevention

Database and File audit, DLP

Identity access management

Antivirus and anti-malware protection

### New School Analytics

UEBA broad scope analytics

Network traffic analytics

Data and File access and exfiltration analytics

Identity analytics

Advanced analytics for endpoint

Add advanced analytics

Add platform features

Gartner

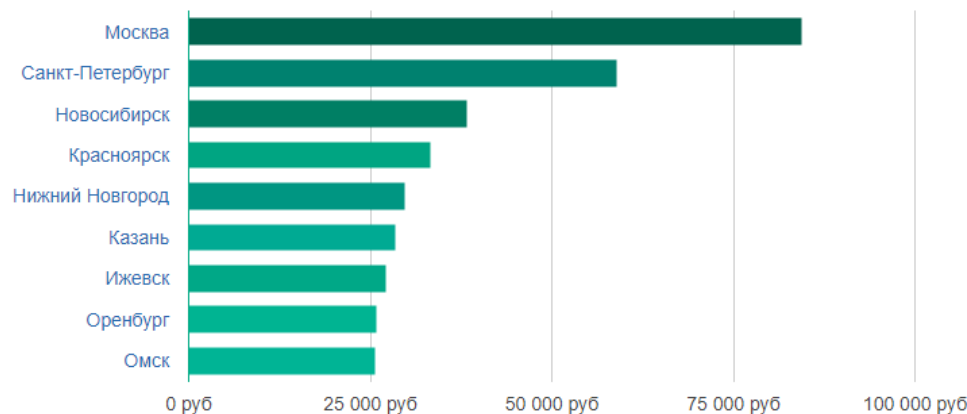
Использование  
устаревших  
инструментов

# Драйвер №2: Персонал/ресурсы

*Сегодня у большинства организаций есть инструменты безопасности в своем стеке, которыми у них нет времени управлять*

*(с) 2021 Managed Detection and Response (MDR) Services Buyers Guide*

Уровень заработной платы: Специалист по информационной безопасности



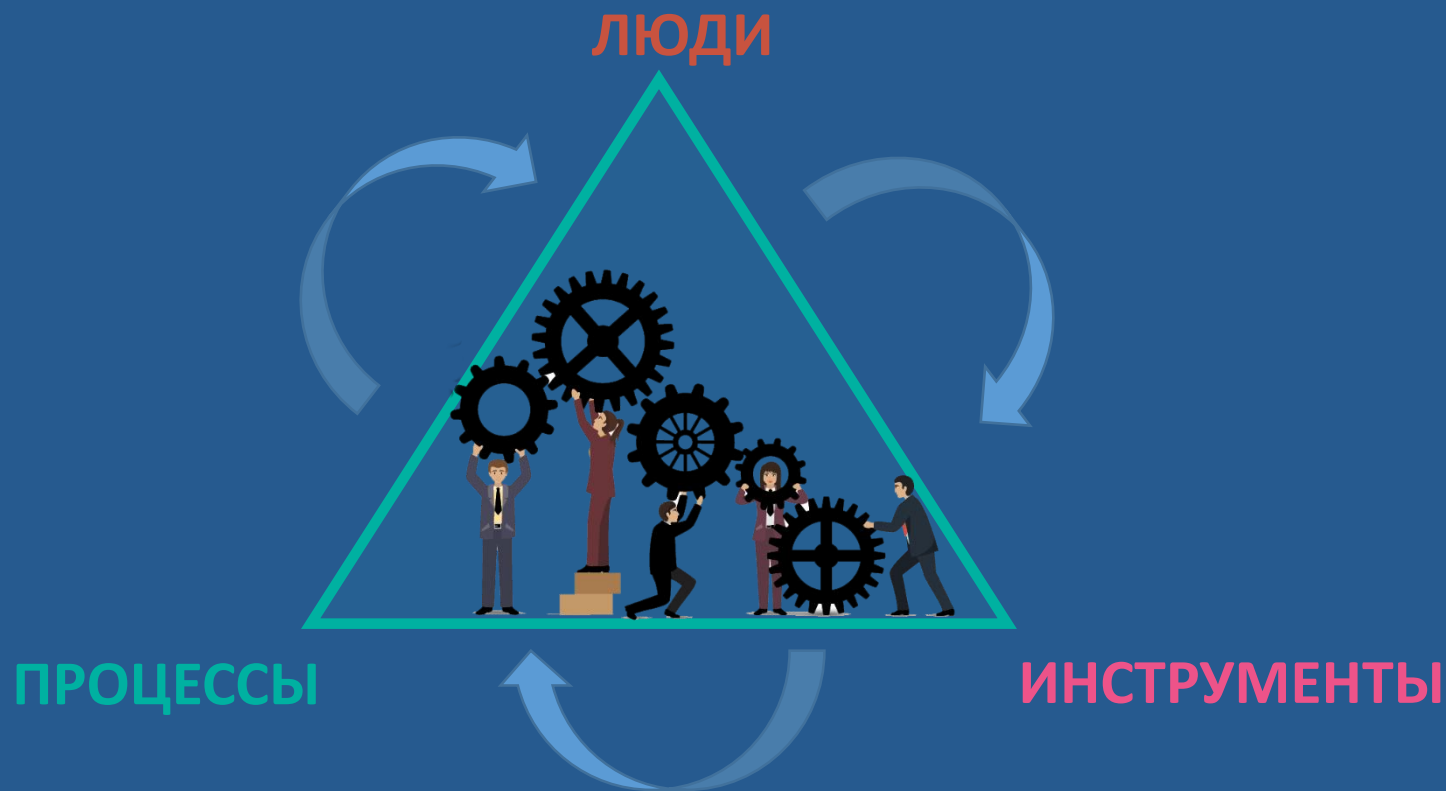
Нехватка квалифицированных кадров в области кибербезопасности и дефицит экспертизы — отчетливая тенденция на рынке ИБ, с которой нам часто приходится сталкиваться. Особенно это касается регионов, где нехватка знаний в области кибербезопасности приводит к существенному отставанию специалистов от глобального развития киберугроз

# Драйвер №3: Неконтролируемый рост предупреждений от средств безопасности

Еще одна проблема – управление огромным количеством предупреждений от всех этих новых систем безопасности. Это не новая проблема, но она растет на порядки по мере увеличения количества конечных точек, в том числе IoT, BYOD, удаленных сотрудников, подключенных партнеров по цепочке поставок и гибридных сетей.

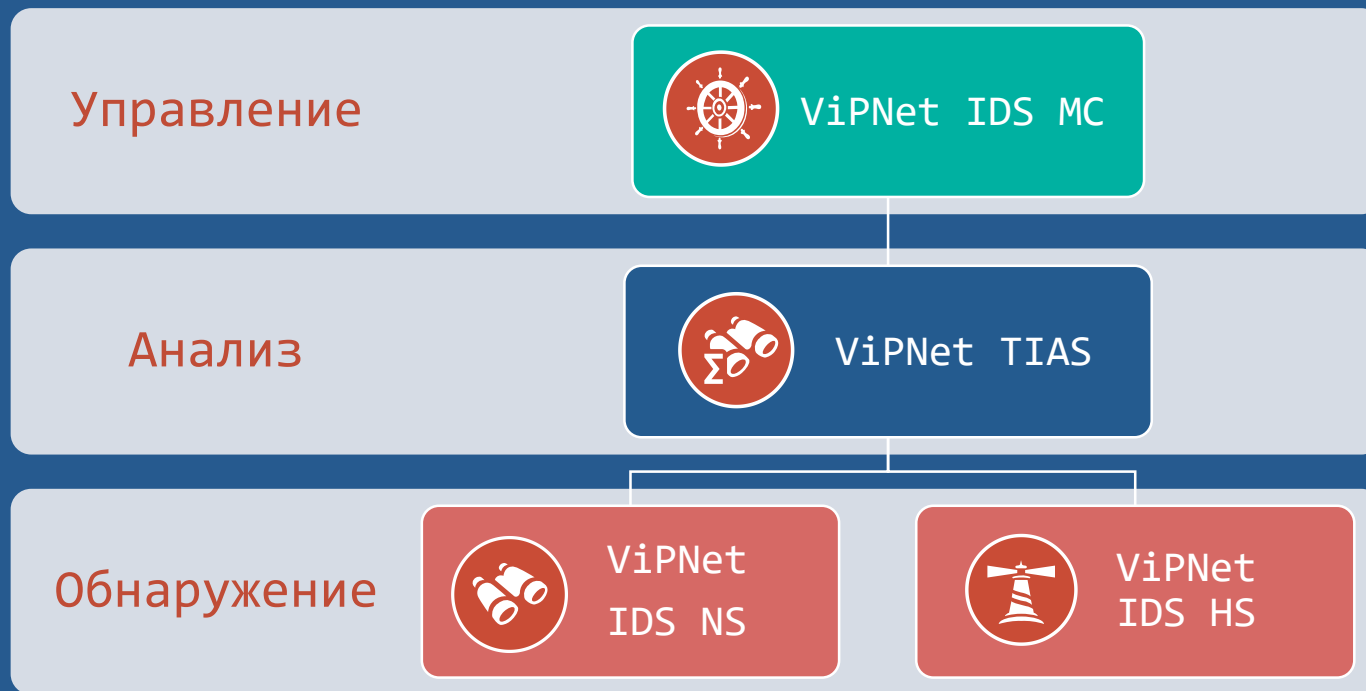
(с) 2021 Managed Detection and Response (MDR) Services Buyers Guide

# MDR ЭТО...



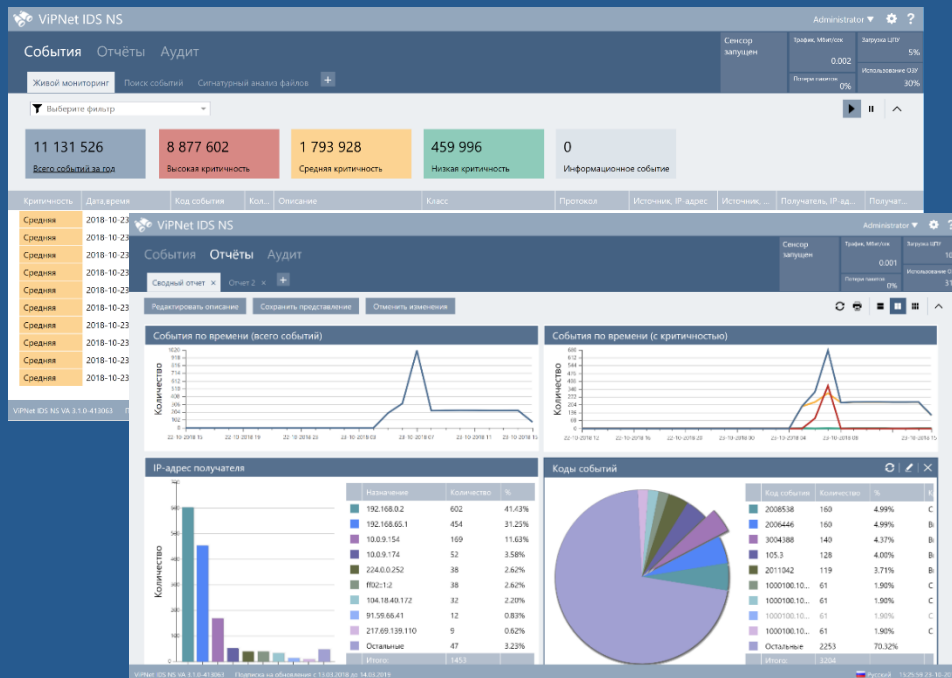
# Решение ViPNet TDR

# Состав решения ViPNet TDR



# VIPNet IDS NS

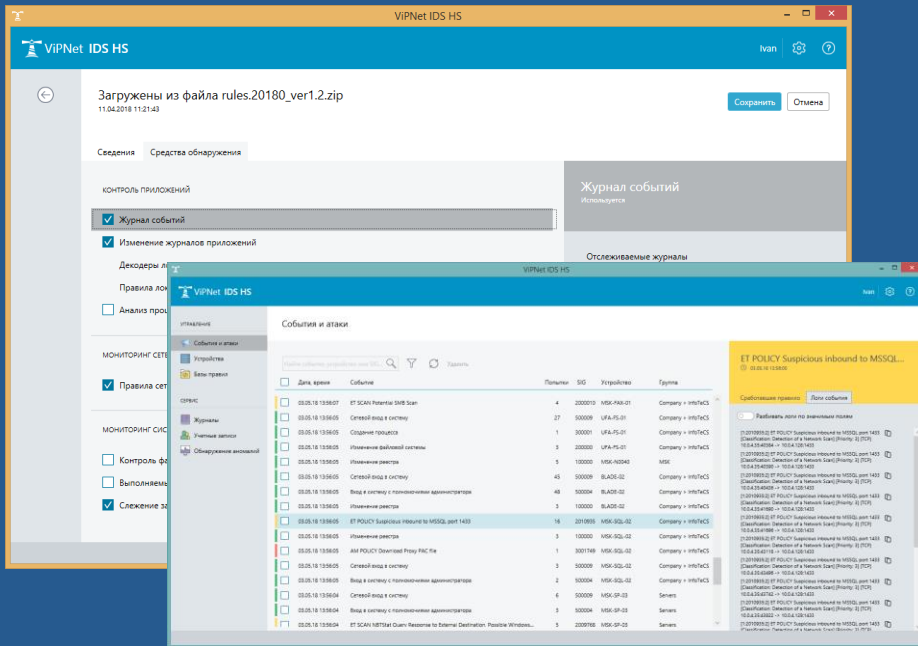
- обнаруживать события ИБ в трафике;
- оповещать о событиях;
- хранить события;
- работать с событиями;
- управлять правилами и настройкой сигнатур.





# VIPNet IDS HS

- **выявлять** подозрительную активность внутри ОС:
  - файловая активность,
  - изменения в реестре,
  - неизвестные процессы.
- **определять** атаки, которые «не видит» сетевой сенсор;
- **обнаруживать** атаки после расшифровки входящего трафика.



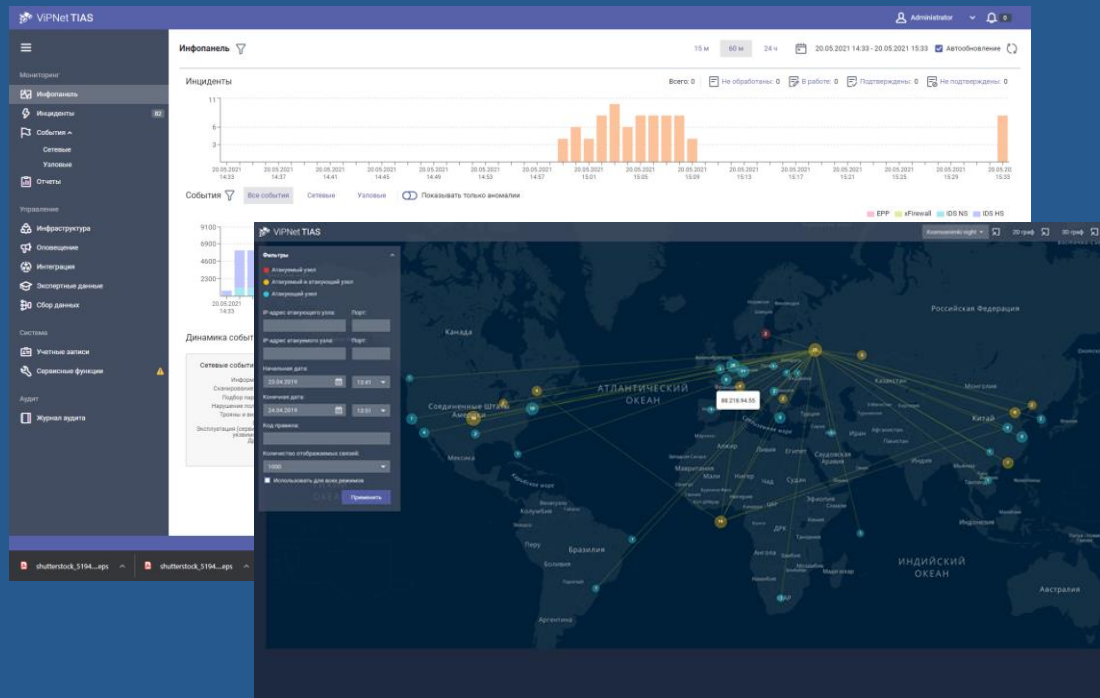
# VIPNet IDS MC

- настраивать структуру и параметры сенсоров;
- управлять конфигурациями правил;
- мониторить работоспособность сенсоров;
- обновлять:
  - базы решающих правил;
  - базы сигнатур вредоносного ПО;
  - экспертные данные.

The screenshot displays the VIPNet IDS MC management console. The top section, titled 'Мониторинг' (Monitoring), shows a summary of sensor status with three cards: 'VIPNet IDS' (14 sensors), 'VIPNet IDS' (1 sensor), and 'VIPNet IDS' (2 sensors). Below this is a table of sensor configurations with columns for name, status, and last update. The bottom section, titled 'Зарегистрированные устройства' (Registered devices), shows a table of devices with columns for IP, MAC, name, and status. The table lists several devices, including 'Алиса', 'Боб', 'Вася', and 'Гриша', with their respective IP and MAC addresses and status 'Получены данные с устройства' (Data received from device).

# VIPNet TIAS

- анализировать события от сенсоров VIPNet IDS;
- выявлять инциденты;
- оповещать об инцидентах;
- проводить расследования;
- давать рекомендации;
- формировать отчеты.



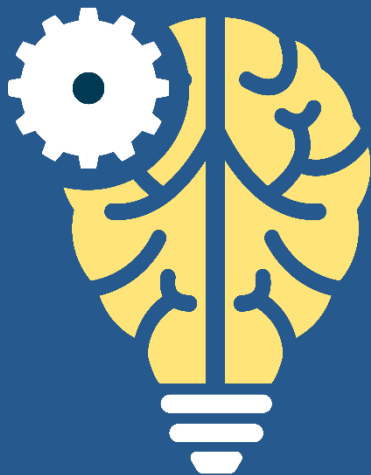
# Как это работает?



# Отличительные особенности



# Machine Learning



- математическая модель принятия решений;
- алгоритмы машинного обучения;
- ежемесячное переобучение;
- выявление атак нулевого дня.

# Threat Intelligence



- индикаторы атак и компрометации;
- ТТП – тактики, техники, процедуры;
- информационный обмен:
  - СОПКА,
  - ФСТЭК,
  - RU-CERT.
- опыт клиентов – верифицированная и обезличенная информация.

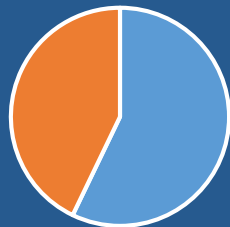
# Обновление правил и экспертных данных

Правила IDS NS



AM ET Всего: 27000

Правила IDS HS



AM ET Всего: 14000

Правила TIAS



AM Всего: 1015

- Ежедневное обновление правил;
- Ежемесячное переобучение математической модели.



# Облачный сервис на базе решения

## сервис-провайдер



ViPNet TIAS



ViPNet IDS MC



ViPNet IDS HS Server

## организация 1



ViPNet IDS NS



ViPNet IDS HS Agents

## организация 2



ViPNet IDS HS Agents

## организация 3



ViPNet IDS NS



ViPNet IDS NS

- мастер подключения организации;
- активация и настройка сенсоров из IDS MC;
- мульти-арендный доступ;
- учет лицензий по организациям.

# Внедрение решения

сервис-провайдер



ViPNet TIAS

10 часов



ViPNet IDS MC



ViPNet IDS HS Server

организация 1



ViPNet IDS NS



ViPNet IDS HS Agents

60 минут

5-15 минут



# Перспективный мониторинг

- Центр мониторинга компьютерных атак
- Разработка правил snort IDS
- Threat Hunting
- Внедрение процедур безопасной разработки ПО
- Расследование компьютерных инцидентов
- Анализ защищённости и пентесты
- Подключение к ГосСОПКА



RESCUE TEAM

более **30**  
операторов,  
исследователей,  
аналитиков

И еще более 40  
организаций подключались  
на мониторинг за последние  
3 года.





**367** человек обучено на курсе  
«Администрирование IDS и TIAS»



**16** ВУЗов имеют лаборатории,  
оснащенные ViPNet IDS и TIAS

# Минутка патриотизма



# Мониторинг информационной безопасности средств и систем информатизации

Наименование оборудования	Технические и (или) функциональные характеристики
22. Средства (системы) контроля (анализа) защищенности информационных систем	Автоматизированная инвентаризация ресурсов информационных систем (сбор информации об узлах информационных систем и об используемом в них программном обеспечении), выявление уязвимостей (кода, конфигурации и архитектуры) в них, анализ и управление выявленными уязвимостями с учетом угроз.  Должны иметь сертификаты соответствия ФСТЭК России.
24. Средства управления информацией об угрозах безопасности информации	Автоматизированный сбор и анализ информации, поступающей из различных источников, об угрозах безопасности информации.  Должны иметь формуляры, оформленные разработчиками (производителями) данных средств. В случае невозможности оформления формуляров разработчиками (производителями) данных средств (свободнораспространяемое программное обеспечение) формуляры оформляются лицензиатами (соискателями лицензии).
25. Средства управления событиями безопасности информации	Автоматизированный сбор, анализ и корреляция данных о событиях безопасности информации, регистрируемых компонентами информационных систем, идентификация по заданным индикаторам типовых инцидентов информационной безопасности и их локализация.  Должны иметь сертификаты соответствия ФСТЭК России.

*Положение о лицензировании деятельности по технической защите конфиденциальной информации, утвержденное постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79  
Перечень утвержден директором ФСТЭК России 19 апреля 2017 г.*



# Мониторинг информационной безопасности средств и систем информатизации

Наименование оборудования

Технические и (или) функциональные характеристики

26.	Средства управления инцидентами информационной безопасности	<p>Автоматизированная регистрация информации об инцидентах информационной безопасности информационных систем, предоставление рекомендаций по реагированию на них, формирование и модификация шаблонов инцидентов информационной безопасности, в том числе рекомендаций по реагированию на них.</p> <p>Должны иметь формуляры, оформленные разработчиками (производителями) данных средств. В случае невозможности оформления формуляров разработчиками (производителями) данных средств (свободнораспространяемое программное обеспечение) формуляры оформляются лицензиатами (соискателями лицензии).</p>
27.	Средства защиты каналов передачи данных	<p>Должны обеспечивать конфиденциальность и целостность данных, передаваемых по каналам связи между информационной системой, используемой для управления информационной безопасностью, и информационными системами, в отношении которых осуществляется мониторинг.</p> <p>Должны иметь сертификаты соответствия ФСБ России.</p>
28.	Системы защиты информации информационных систем, используемых для мониторинга информационной безопасности	<p>Системы защиты информации информационных систем, используемых для оказания услуг по мониторингу информационной безопасности информационных систем, должны соответствовать Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. N 17, применительно к первому классу защищенности государственных информационных систем.</p>

# ГосСОПКА



# Приказ ФСБ России №282 от 19.06.2019



- Информация о компьютерном инциденте, связанном с функционированием значимого объекта критической информационной инфраструктуры, направляется субъектом критической информационной инфраструктуры в НКЦКИ **в срок не позднее 3 часов** с момента обнаружения компьютерного инцидента, а в отношении иных объектов критической информационной инфраструктуры – **в срок не позднее 24 часов** с момента его обнаружения.
- Информирование осуществляется путем направления информации в Национальный координационный центр по компьютерным инцидентам в соответствии с определенными НКЦКИ форматами.

# Перечень мероприятий

## Класс В

- Взаимодействие с НКЦКИ;
- Разработка регламентирующих документов;
- Эксплуатация средств ГосСОПКА;
- Прием сообщений об инцидентах;
- Регистрация атак и инцидентов;
- Анализ событий ИБ;
- Инвентаризация.

## Класс Б

- Анализ угроз ИБ;
- Составление и актуализация перечня угроз;
- Выявление уязвимостей;
- Подготовка предложений по повышению уровня защищенности;
- Составление перечня инцидентов.

## Класс А

- Ликвидация последствий;
- Анализ результатов ликвидации последствий.

# Варианты подключения

## Самостоятельное подключение



Субъект  
ГосСОПКА

- Заключение соглашения с 8Ц ФСБ России;
- Выполнить организационные и технологические требования к центру ГосСОПКА;
- Обеспечить взаимодействие с технической инфраструктурой НКЦКИ.



## Подключение через корпоративный центр



Корпоративный центр  
ГосСОПКА

- Заключение соглашения с корпоративным (ведомственным) центром ГосСОПКА;
- Уведомить НКЦКИ о включении своих ресурсов в зону ответственности центра.



Объект КИИ

# Карточка инцидента в формате НКЦКИ

### Параметры инцидента

Основные сведения

Информация об атакованной информационной системе

Информация об атакованных узлах

Индикаторы компрометации

Дополнительная информация об инциденте

Меры по реагированию

Связь с другими инцидентами

**\* Класс события информационной безопасности:**  
Компьютерный инцидент

**\* Категория:**  
Внедрение вредоносного программного обеспечения (Malware)

**\* Тип:**  
Внедрение в информационный ресурс модулей вредоносного программного обеспечения

Идентификатор: incidentGS-f34030ef-358a-445c-8567-25985ce 6d68a  
Регистрационный номер:

**\* Степень конфиденциальности сведений об инциденте:**  
White

Наименование организации-отправителя сведений об инциденте

**Оценка последствий**

**\* Нарушение конфиденциальности:** Высокая степень

**\* Нарушение целостности:** Высокая степень

**\* Нарушение доступности:** Высокая степень

Иная форма нарушения:

Для отправки заполните все обязательные поля.

Сохранить и отправить в НКЦКИ Сохранить Отмена

### Классификатором выявлено подозрительное событие

Высокий уровень важности

#### Параметры инцидента НКЦКИ

Статус инцидента: Подтвержден

Способ передачи в НКЦКИ: Не отправлен

Дата и время отправки: Не отправлен

Категория инцидента (НКЦКИ): Отправлен по телефону

Тип инцидента (НКЦКИ): Отправлен по электронной почте

Тип инцидента: Отправлен на электронную почту НКЦКИ через TIAS

Пользователь: Отправлен по факсимильной почте

Дата и время: Отправлен с использованием

Пораженные узлы (1): Личного кабинета НКЦКИ

страна: США  
Город: Не определен

Рейтинг: 10

IP-адрес сенсора: 123.123.123.123

Идентификатор сенсора: 123456789

Название сенсора: Сенсор 12345

Метод реализации угрозы: -

Наименование: Классификатором выявлено подозрительное событие

Метод обнаружения: Звистический

Идентификатор инцидента: 123456789

Симптомы: Аномальная сетевая активность АРМ

**Рекомендации**

- Отключить пораженный актив от вычислительной сети

### Классификатором выявлено подозрительное событие

Высокий уровень важности

#### Параметры инцидента НКЦКИ

Статус инцидента: Подтвержден

Способ передачи в НКЦКИ: Отправлен по телефону

Дата и время отправки: 02.10.2019 07:05:21

Категория инцидента (НКЦКИ):

Тип инцидента: 02.10.2019 07:05:21

Тип инцидента: Формат 00:00:00

Пользователь:

Дата и время: Сохранить Закрыть

Пораженные узлы (1): Личного кабинета НКЦКИ

страна: США  
Город: Не определен

Рейтинг: 10

IP-адрес сенсора: 123.123.123.123

Идентификатор сенсора: 123456789

Название сенсора: Сенсор 12345

Метод реализации угрозы: -

Наименование: Классификатором выявлено подозрительное событие

Метод обнаружения: Звистический

Идентификатор инцидента: 123456789

Симптомы: Аномальная сетевая активность АРМ

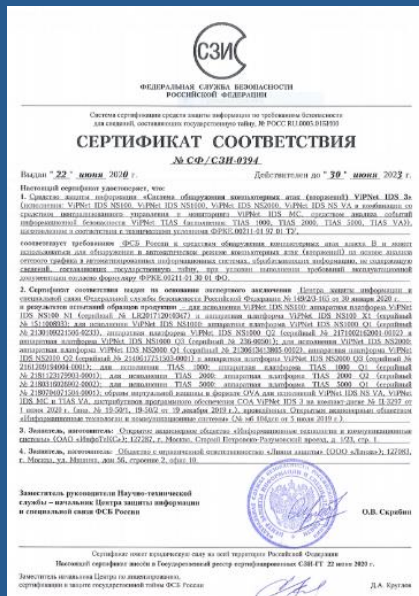
**Рекомендации**

- Отключить пораженный актив от вычислительной сети

# Сертификаты

ФСБ России  
СОА класса В  
Система IDS 3 в составе:

- ПAK ViPNet IDS NS
- ПО ViPNet IDS MC
- ПAK ViPNet



ФСТЭК России  
СОВ 4 класс, ТДБ 4  
уровень  
Система IDS 3 в составе:

- ПО ViPNet IDS NS
- ПО ViPNet IDS MC
- ПО ViPNet TIAS



ТЕХНО infotecs  
2021 Фест

Спасибо  
за внимание!

Подписывайтесь на наши соцсети



@infotecs.ru



@vpninfotecs



@InfoTeCS\_Moscow