ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Практический опыт взаимодействия с ГосСОПКА

АО «Перспективный мониторинг»

Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом РФ 12 декабря 2014 г. N К 1274)

Уполномоченный орган
ФСБ России

НКЦКИ

Национальный координационный центр по компьютерным инцидентам

Нормативные правовые акты

Методические документы ФСБ России

Как получить методические документы

Направить письменный запрос на имя Директора НКЦКИ по адресу:

107031, г. Москва, ул. Большая Лубянка, д. 1/3

Какие сведения необходимо отразить в запросе:

- информацию об организации
- цель получения документов
- сведения о лицензиях ФСБ России
- предполагаемую зону ответственности

187-ФЗ

Статья 9. Права и обязанности субъектов критической информационной инфраструктуры

Кому это обязательно?

Субъект критической информационной инфраструктуры **обязан** незамедлительно информировать о компьютерных инцидентах соответствующие федеральные органы исполнительной власти (НКЦКИ ГосСОПКА, Финцерт ЦБ РФ для финансовых организаций), а также реагировать на компьютерные инциденты в установленном порядке.

ГосСОПКА это не только КИИ

ОГВ

Могут быть подключены к ГосСОПКА

КИИ

Обязаны быть подключены к ГосСОПКА

Приказ ФСБ России № 367

от 24 июля 2018 г.

«Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»

Передаются сведения:

- О категорировании объекта
- О нарушении требований по обеспечению безопасности значимых объектов КИИ (по итогам проведения государственного контроля)
- Информация о компьютерных инцидентах, связанных с функционированием объектов КИИ
- Иная информация в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

Два способа предоставления информации в НКЦКИ:

- с использованием технической инфраструктуры НКЦКИ
- посредством электронной, факсимильной, почтовой и телефонной связи

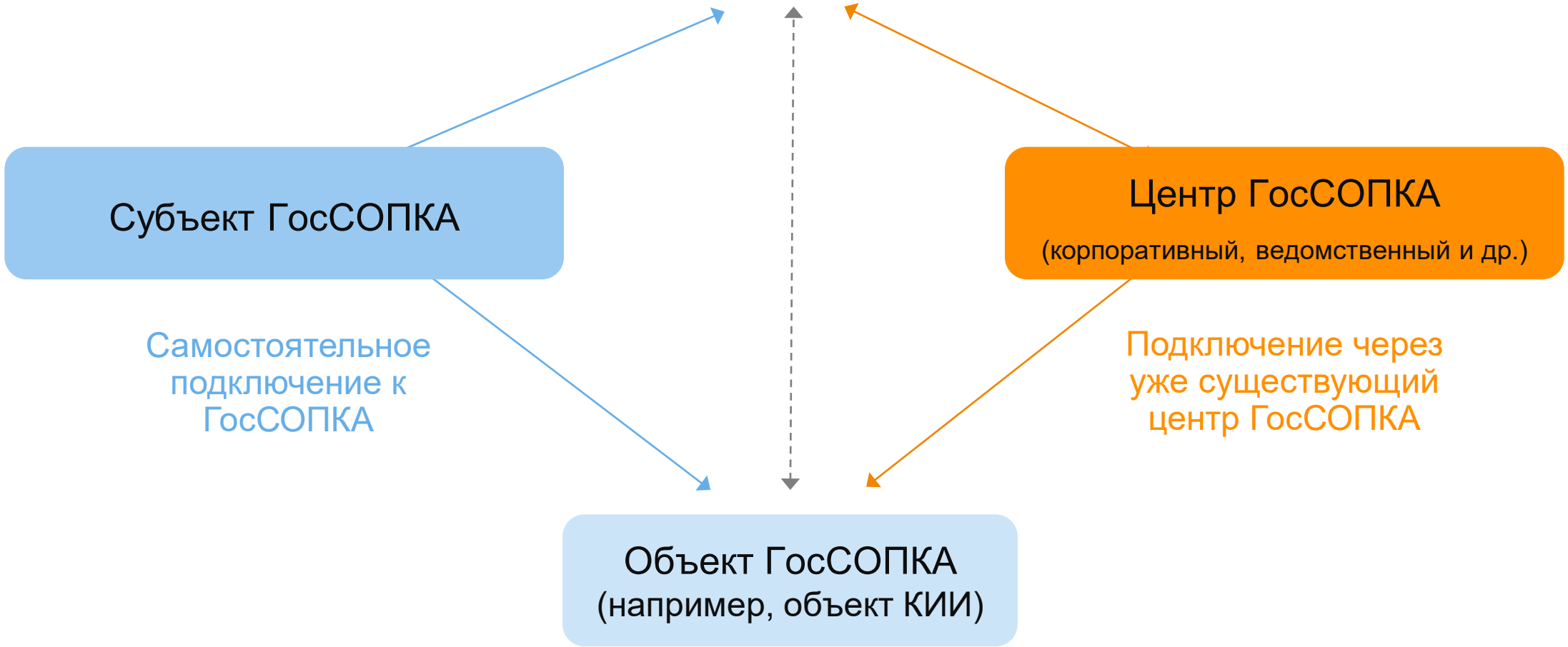
Автоматизированное взаимодействие с технической инфраструктурой НКЦКИ сильно экономит силы и время

Технические аспекты

Что делать

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ



Что делать?

В случае самостоятельного подключения к ГосСОПКА

- ✓ Обеспечить взаимодействие с 8Ц ФСБ России
- ✓ Выполнить организационные и технические требования в соответствии с нормативными правовыми актами и методическими рекомендациями
- ✓ Развернуть специализированные системы взаимодействия с технической инфраструктурой НКЦКИ (для значимых КИИ обязательно, остальным опционально).

В случае подключения через сторонний корпоративный сегмент

- ✓ Заключить соглашение с корпоративным центром
- ✓ Уведомить НКЦКИ о включении своих информационных ресурсов в зону ответственности корпоративного центра.

Какие функции выполняют центры ГосСОПКА

Глобально:

1. Сбор сведений о контролируемой инфраструктуре.
2. Непрерывный мониторинг и выявление КА и инцидентов.
3. Информирование, реагирование, расследование.
4. Передача сведений в НКЦКИ.

Персонал

Первая линия	Вторая линия	Третья линия
Взаимодействие с пользователями	Помощь в расследовании и установлении причин инцидентов	Подготовка и улучшение нормативной базы, описание сценариев выявленных инцидентов
Анализ событий и обнаружение компьютерных атак и инцидентов	Координация действий при реагировании на инциденты ИБ	Разработка сигнатурных правил и правил корреляции
Регистрация инцидентов ИБ и оповещение заинтересованных лиц	Анализ уязвимостей, анализ защищенности, тестирование на проникновение	Углубленный анализ Инцидентов ИБ, сбор доказательной базы

Специалисты 1 линии

Специалист по взаимодействию с персоналом и пользователями

- Прием сообщений персонала и пользователей
- Подготовка информации для предоставления в НКЦКИ
- Взаимодействие с НКЦКИ

Специалист по обнаружению компьютерных атак и инцидентов

- Анализ событий информационной безопасности
- Регистрация компьютерных атак и инцидентов

Специалист по обслуживанию средств центра ГосСОПКА

- Обеспечение функционирования средств, размещаемых в центре ГосСОПКА, а также дополнительных средств защиты информационных систем

Специалисты 2 линии

Специалист по оценке защищенности

- Проведение инвентаризации информационных ресурсов
- Выявление уязвимостей
- Сбор и анализ выявленных уязвимостей и угроз
- Установление соответствия требований по информационной безопасности принимаемым мерам

Специалист по ликвидации последствий компьютерных инцидентов

- Координация действий при реагировании на компьютерные инциденты и приведение в штатный режим работы
- Взаимодействие с НКЦКИ

Специалист по установлению причин компьютерных инцидентов

- Установление причин компьютерных инцидентов
- Анализ последствий инцидентов и подготовка перечня компьютерных инцидентов
- Взаимодействие с НКЦКИ

Специалисты 3 линии

Аналитик-методист

- Анализ информации, предоставляемой специалистами 1-й и 2-й линий
- Выявление и анализ угроз информационной безопасности
- Прогнозирование развития угроз
- Разработка рекомендаций по доработке нормативных и методических документов

Технический эксперт

- Экспертная поддержка в соответствии со специализацией (ВПО, настройка средств защиты, применение специализированных технических средств, оценка защищенности и т.п.)
- Формирование предложений по повышению уровня защищенности

Специалист

- Нормативно-правовое и методическое сопровождение деятельности центра ГосСОПКА

Руководитель

Управление деятельностью центра ГосСОПКА
Взаимодействие с НКЦКИ

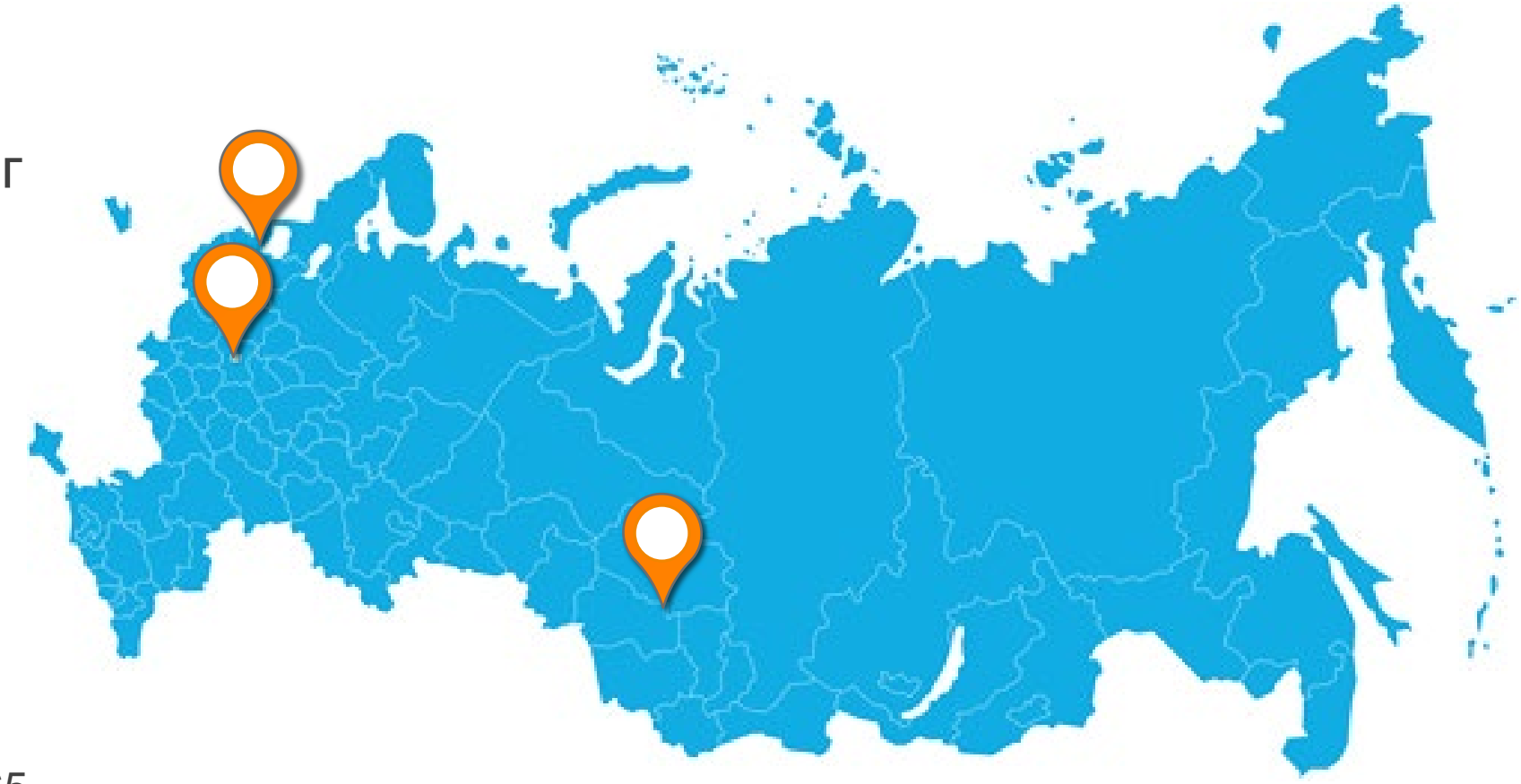
Как это работает у нас?

География площадок Центра мониторинга АО «ПМ»

Санкт- Петербург

Москва

Новосибирск



Круглосуточно 24/7/365

Центр мониторинга АО «ПМ»

2014
год запуска

28 200
подключенных узлов

>30
операторов, исследователей, аналитиков и инженеров

<30 мин.
реагирование на инцидент ИБ

>12 000
собственных сигнатур атак для IDS

С 2017 года Центр ГосСОПКА класса А

СБОР СОБЫТИЙ

Сетевые IDS

Хостовые IDS

DNS, DHCP, AV,
VPN, FW, Mail...

АНАЛИЗ И ВЫЯВЛЕНИЕ

TIAS

LogCollector

ОБОГАЩЕНИЕ И РЕАГИРОВАНИЕ

Фиды угроз
и уязвимостей

TI Platform

Incident
Management

ТИ НКЦКИ

Карточка инцидента

В РАБОТЕ У КЛИЕНТА | Попытки эксплуатации уязвимости CVE-2021-4

Создан: 2023-07-07 17:27:02
Изменен: 2023-07-07 17:34:21
Просмотрен заказчиком: 2023-07-20 16:07:52
Закрыт: -

ОТПРАВЛЕН ЗАКАЗЧИКУ | УДАЛИТЬ

Общая информация

Попытки эксплуатации уязвимости

Уровень важности: ВЫСОКИЙ

Описание

Фиксируем сканирование защищаемой сети на наличие уязвимости CVE-2021-44228 от узла 95.214.55.244 (Польша, ASN: 201814) , зафиксированного во множестве черных списков вредоносной активности в сети Интернет. Уровень критичности 10/10, вектор: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H.

Адрес получателя защищаемой сети -

Log4j — библиотека журналирования (логирования) Java-программ.

Местоположение

Сегменты

Сенсоры: IDS 1000 10.0.26.14...

Пользователи

Автор: Паньков Денис

Оператор: Паньков Денис

ЛИНИЯ: 1 | ПЕРЕДАТЬ 2 ЛИНИИ

НКЦКИ

Регистрационный номер

Статус: Принято решение

Выявлен: 2023-07-07 17:39:35

Обновлен: 2023-07-07 18:37:05

ОТКРЫТЬ УВЕДОМЛЕНИЕ

Работы

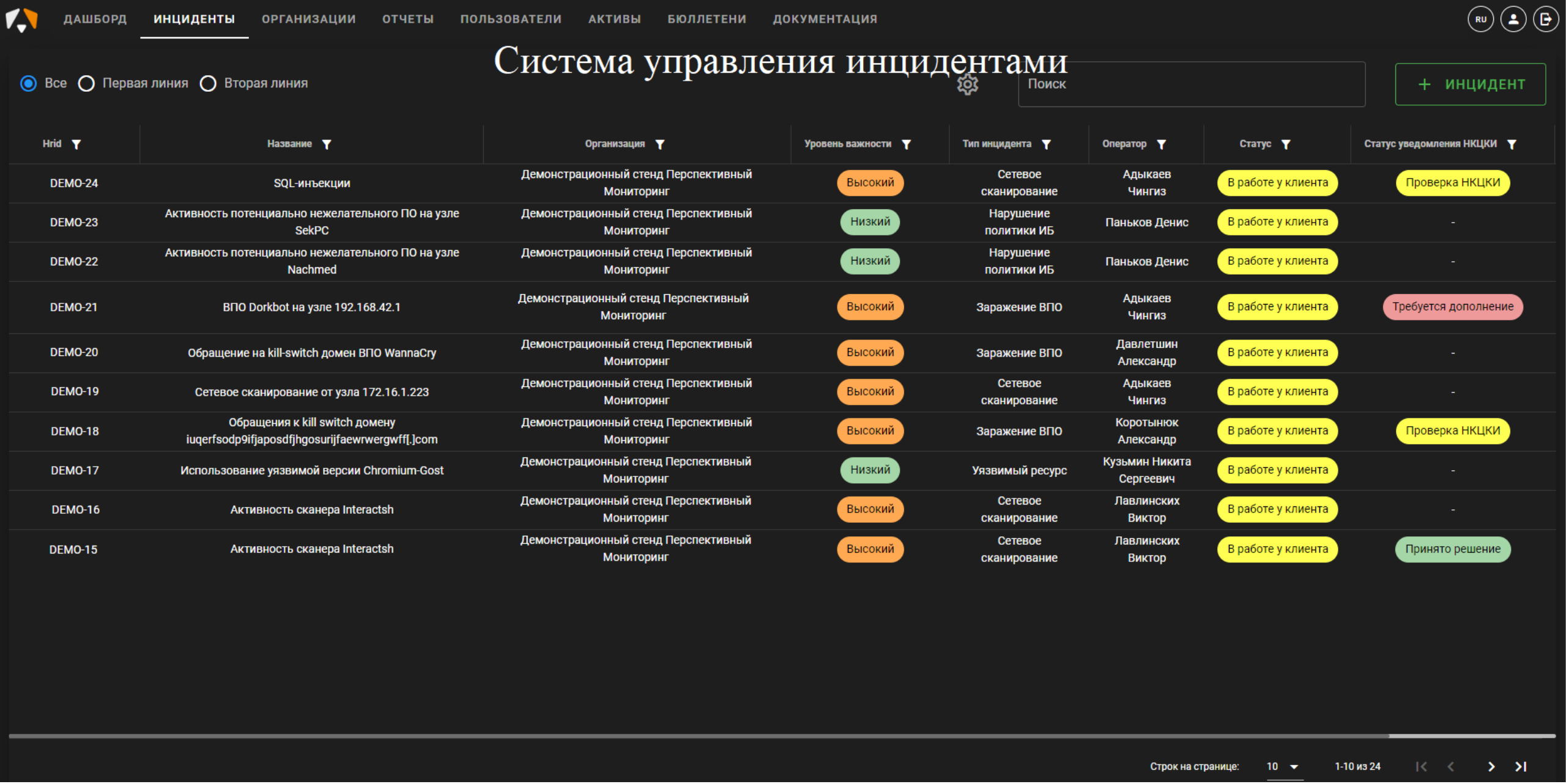
РЕКОМЕНДАЦИИ | ПРЕДПРИНЯТЫЕ ДЕЙСТВИЯ

- Паньков Денис: Заблокировать адрес источника 95.214.55.244
- Паньков Денис: Установить обновление безопасности Apache Log4j2
- Паньков Денис: Для обнаружения уязвимой версии log4j можно восп
- Паньков Денис: В случае невозможности обновления удалить класс .
- Паньков Денис: Проверить активные подключения к узлу на предмет

СОБЫТИЯ + | ИСТОРИЯ | КОММЕНТАРИИ | ФАЙЛЫ + | ЗАТРОНУТЫЕ АКТИВЫ + | IOCS +

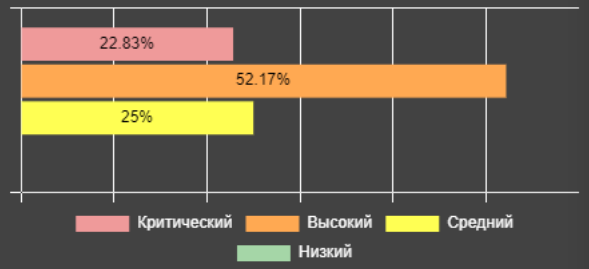
ViPNet_IDS

Дата	Сенсор	Sid	Узел	Источник	Получатель	Событие	Объект	Домен	Действия
2023-07-07 16:46:37	IDS 1000 10.0.26.147	2034755		95.214.55.244		ET EXPLOIT Apache Obfuscated log...			
2023-07-07 16:46:37	IDS 1000 10.0.26.147	3195137		95.214.55.244		AM EXPLOIT Apache Log4j2 JNDI R...			
2023-07-07 16:46:37	IDS 1000 10.0.26.147	3195052		95.214.55.244		AM EXPLOIT Possible Apache Log4j...			
2023-07-07 16:46:37	IDS 1000 10.0.26.147	3195047		95.214.55.244		AM EXPLOIT Possible Apache Log4j...			
2023-07-07 16:46:37	IDS 1000 10.0.26.147	3195137		95.214.55.244		AM EXPLOIT Apache Log4j2 JNDI R...			
2023-07-07 16:46:37	IDS 1000 10.0.26.147	3195047		95.214.55.244		AM EXPLOIT Possible Apache Log4j...			


ДАШБОРД
ИНЦИДЕНТЫ
ОРГАНИЗАЦИИ
ОТЧЕТЫ
ПОЛЬЗОВАТЕЛИ
АКТИВЫ
БЮЛЛЕТЕНИ
ДОКУМЕНТАЦИЯ
RU
Система управления инцидентами
Все
Первая линия
Вторая линия
Поиск
+ ИНЦИДЕНТ
Hrid
Название
Организация
Уровень важности
Тип инцидента
Оператор
Статус
Статус уведомления НКЦКИ
DEMO-24
SQL-инъекции
Демонстрационный стенд Перспективный Мониторинг
Высокий
Сетевое сканирование
Адыкаев Чингиз
В работе у клиента
Проверка НКЦКИ
DEMO-23
Активность потенциально нежелательного ПО на узле SekPC
Демонстрационный стенд Перспективный Мониторинг
Низкий
Нарушение политики ИБ
Паньков Денис
В работе у клиента
-
DEMO-22
Активность потенциально нежелательного ПО на узле Nachmed
Демонстрационный стенд Перспективный Мониторинг
Низкий
Нарушение политики ИБ
Паньков Денис
В работе у клиента
-
DEMO-21
ВПО Dorkbot на узле 192.168.42.1
Демонстрационный стенд Перспективный Мониторинг
Высокий
Заражение ВПО
Адыкаев Чингиз
В работе у клиента
Требуется дополнение
DEMO-20
Обращение на kill-switch домен ВПО WannaCry
Демонстрационный стенд Перспективный Мониторинг
Высокий
Заражение ВПО
Давлетшин Александр
В работе у клиента
-
DEMO-19
Сетевое сканирование от узла 172.16.1.223
Демонстрационный стенд Перспективный Мониторинг
Высокий
Сетевое сканирование
Адыкаев Чингиз
В работе у клиента
-
DEMO-18
Обращения к kill switch домену iuqerfsodp9ifjaposdfjhgosurijfaewrwergwff[.]com
Демонстрационный стенд Перспективный Мониторинг
Высокий
Заражение ВПО
Коротынюк Александр
В работе у клиента
Проверка НКЦКИ
DEMO-17
Использование уязвимой версии Chromium-Gost
Демонстрационный стенд Перспективный Мониторинг
Низкий
Уязвимый ресурс
Кузьмин Никита Сергеевич
В работе у клиента
-
DEMO-16
Активность сканера Interactsh
Демонстрационный стенд Перспективный Мониторинг
Высокий
Сетевое сканирование
Лавлинских Виктор
В работе у клиента
-
DEMO-15
Активность сканера Interactsh
Демонстрационный стенд Перспективный Мониторинг
Высокий
Сетевое сканирование
Лавлинских Виктор
В работе у клиента
Принято решение
Строк на странице:
10
1-10 из 24

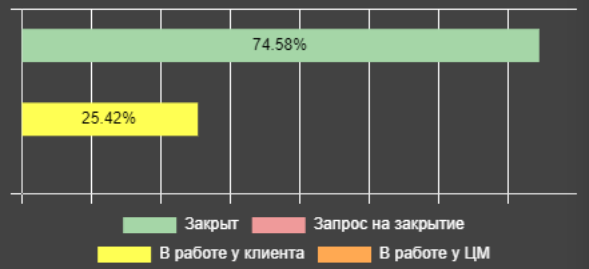
Организации | Период: Квартал | ПРИМЕНИТЬ

Статистика по уровню важности



Статистика по типам инцидентов

Статистика по статусу



Всего инцидентов за период

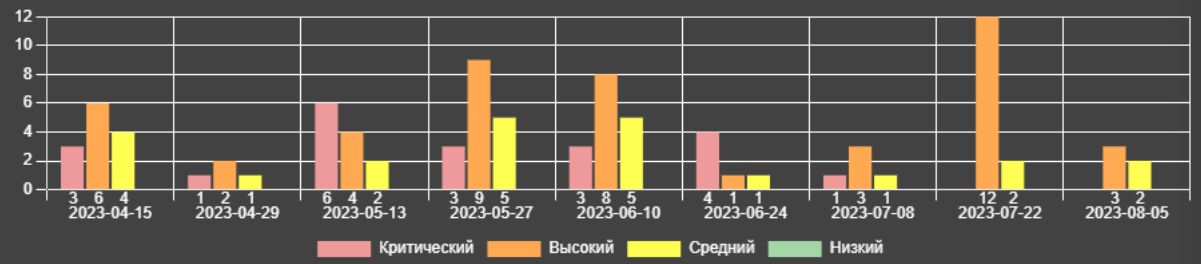
92

Процент соответствия SLA

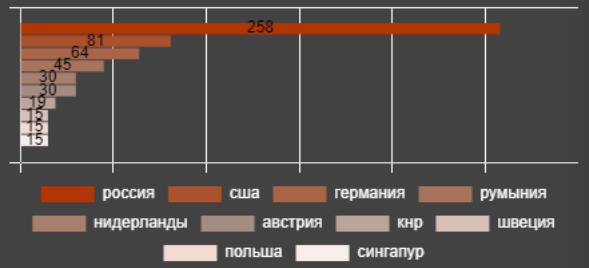
97.28%

ПОДРОБНОСТИ

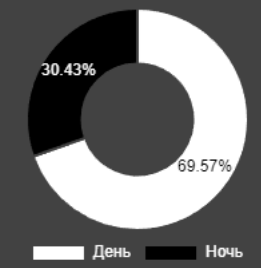
Статистика по уровню важности за период



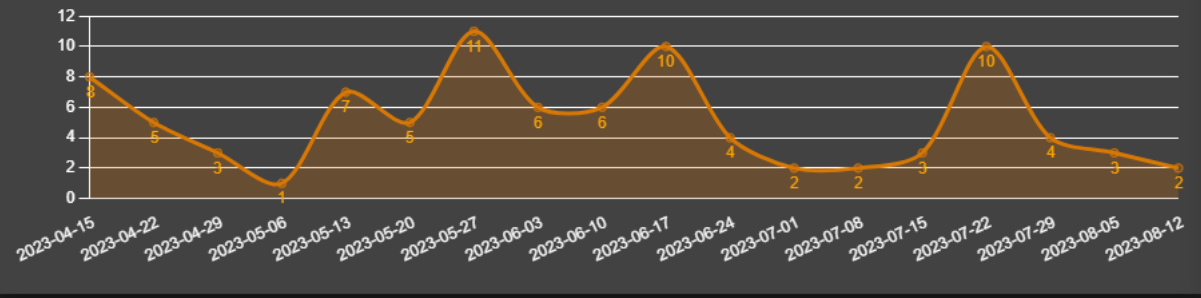
Топ 10 атакующих стран



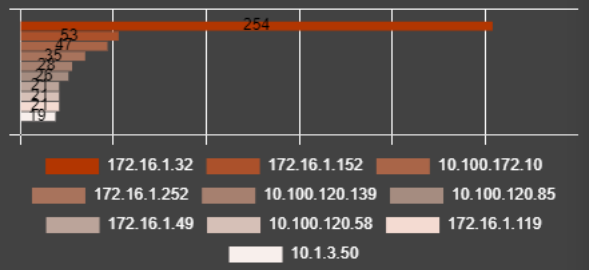
Статистика по времени суток



Динамика регистрации инцидентов



Топ 10 атакуемых узлов сети



Распределение по геокоординатам

Ответственность

ГОСУДАРСТВЕННАЯ ДУМА
ФЕДЕРАЛЬНОГО СОБРАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Новости Структура Фото и видео Сервисы | Деятельность: Законодательная Представительная Международная

Принят закон о штрафах за нарушения при защите критической IT-инфраструктуры

http://publication.pravo.gov.ru/Document/View/0001202004010048

КоАП РФ Статья 13.12.1.

КоАП РФ Статья 19.7.15.

КоАП РФ Статья 13.12.1. Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

1. за нарушение **требований** к созданию и обеспечению функционирования систем безопасности значимых объектов КИИ —
от 10 тыс. до 50 тыс. рублей для должностных лиц,
от 50 тыс. до 100 тыс. рублей для юр.лиц;

2. за нарушение **порядка** информирования, реагирования, принятия мер.. об инцидентах на объектах ЗОКИИ—
от 10 тыс. до 50 тыс. рублей для должностных лиц,
от 100 тыс. до 500 тыс. рублей для юр.лиц;

3. за нарушение **порядка** обмена информацией об инцидентах между субъектами КИИ и уполн. органами иностранными государств —
от 20 тыс. до 50 тыс. рублей для должностных лиц,
от 100 тыс. до 500 тыс. рублей для юр.лиц.

КоАП РФ Статья 19.7.15. Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

1. Непредставление или нарушение **сроков** представления во ФСТЭК России, сведений о результатах присвоения объекту КИИ категории значимости, либо об отсутствии необходимости присвоения
   от 10 до 50 тыс. руб. на должностных лиц;
   от 50 до 100 тыс. руб. на юридических лиц

2. Непредставление или нарушение **порядка** либо сроков представления в ГосСОПКА
   от 10 до 50 тыс. руб. на должностных лиц;
   от 100 до 500 тыс. руб. на юридических лиц

УК РФ Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

1. Создание, распространение и (или) использование компьютерных программ.. предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты .. (до 5 лет)
2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре.. (до 5 лет)
3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре (ИТКС, ИС, АСУ) (до 6 лет)
4. Деяния, предусмотренные частью первой, второй или третьей настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения.. (до 8 лет)
5. Деяния, предусмотренные частью первой, второй, третьей или четвертой настоящей статьи, если они повлекли тяжкие последствия.. (до 10 лет)

Спасибо за внимание!

И подключайтесь к ГосСОПКА

«Перспективный мониторинг»