


ViPNet TIAS 3.5. Схемы подключения к ГосСОПКА и практические сценарии взаимодействия с НКЦКИ

менеджер продукта Старовойт Светлана

A decorative orange arc is located in the bottom right corner of the slide, partially overlapping the text area.



Подключение к ГосСОПКА

Структура ГосСОПКА



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



Объект КИИ

Подключение через корпоративный центр



Корпоративный центр
ГосСОПКА

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



- **Перечень информации**, предоставляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка предоставления информации в ГосСОПКА (Приказ № 367 от 24 июля 2018 года);
- **Порядок обмена информацией** о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации... (Приказ от 24 июля 2018 г. N 368);
- **Требования к средствам**, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (Приказ от 06.05.2019 №196)
- **Порядок информирования** ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации (Приказ ФСБ России от 19.06.2019 N 282)



Информация о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры:

- дата, время, место нахождения или географическое местоположение объекта критической информационной инфраструктуры, на котором произошел компьютерный инцидент;
- наличие причинно-следственной связи между компьютерным инцидентом и компьютерной атакой;
- связь с другими компьютерными инцидентами (при наличии);
- состав технических параметров компьютерного инцидента;
- последствия компьютерного инцидента.



определяет правила обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты

- При наличии подключения к технической инфраструктуре НКЦКИ уведомления и запросы направляются посредством использования данной инфраструктуры
- В случае отсутствия подключения к технической инфраструктуре НКЦКИ информирование осуществляется посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети "Интернет" по адресу: "<http://cert.gov.ru>";

Требования к средствам ГосСОПКА



К средствам ГосСОПКА относятся:

- технические, программные, программно-аппаратные и иные средства для обнаружения компьютерных атак (далее - **средства обнаружения**);
- технические, программные, программно-аппаратные и иные средства для предупреждения компьютерных атак (далее - **средства предупреждения**);
- технические, программные, программно-аппаратные и иные средства для ликвидации последствий компьютерных атак (далее - **средства ликвидации последствий**);
- технические, программные, программно-аппаратные и иные средства поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры (далее - **средства ППКА**);
- технические, программные, программно-аппаратные и иные средства обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак (далее - **средства обмена**);
- **криптографические средства** защиты информации, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.

Приказ № 196 от 6 мая 2019 года

Общие требования к средствам ГосСОПКА



Средства ГосСОПКА должны соответствовать следующим требованиям:

- должна быть исключена возможность удаленного управления со стороны лиц, не являющихся работниками субъекта КИИ или привлекаемыми работниками
- должна быть исключена возможность несанкционированной передачи обрабатываемой информации
- должны иметь возможность модернизации российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц.
- должны быть обеспечены гарантийной и технической поддержкой российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц
- Работа средств ГосСОПКА не должна приводить к нарушениям функционирования информационных систем
- В средствах ГосСОПКА должны быть реализованы функции безопасности в соответствии с главой VIII настоящих Требований.

Требования к средствам обнаружения



- сбор и первичная обработка событий, связанных с нарушением информационной безопасности (далее - события ИБ),
- автоматический анализ событий ИБ и выявление компьютерных инцидентов;
- повторный анализ ранее зарегистрированных событий ИБ и выявление на основе такого анализа не обнаруженных ранее компьютерных инцидентов.

Приказ № 196 от 6 мая 2019 года

Требования к средствам предупреждения



- сбор и обработка сведений об инфраструктуре контролируемых информационных ресурсов и справочной информации;
- сбор и обработка сведений об уязвимостях и недостатках в настройке программного обеспечения (далее - ПО), используемого в контролируемых информационных ресурсах;
- формирование рекомендаций по минимизации угроз безопасности информации;
- учет угроз безопасности информации

Приказ № 196 от 6 мая 2019 года

Требования к средствам ликвидации последствий



- учет и обработка компьютерных инцидентов;
- управление процессами реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак;
- взаимодействие с НКЦКИ посредством использования технической инфраструктуры НКЦКИ;
- информационно-аналитическое сопровождение пользователей

Приказ № 196 от 6 мая 2019 года

Требования к средствам поиска признаков компьютерных атак



- обнаружение признаков компьютерных атак в сети электросвязи по значениям служебных полей протоколов сетевого взаимодействия, а также осуществление сбора, накопления и статистической обработки результатов такого обнаружения;
- обнаружение в сети электросвязи признаков управления телекоммуникационным оборудованием;
- обнаружение изменений параметров настроек телекоммуникационного оборудования сети электросвязи;
- обнаружение изменений параметров настроек систем управления телекоммуникационным оборудованием и сетями электросвязи;
- хранение копий сетевого трафика, в котором были обнаружены признаки компьютерных атак в сети электросвязи и (или) признаки управления телекоммуникационным оборудованием, не менее шести месяцев;
- анализ и экспорт фрагментов копий сетевого трафика, в котором были обнаружены признаки компьютерных атак в сети электросвязи и (или) признаки управления телекоммуникационным оборудованием;

Требования к средствам обмена и криптографическим средствам защиты информации



- Средства обмена должны обеспечивать передачу, прием и целостность при передаче и приеме информации, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.
- Криптографические средства защиты информации, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, **должны быть сертифицированы в системе сертификации средств криптографической защиты информации.**

Средства ГосСОПКА

Средство ГосСОПКА	Продукты и сервисы
Средства обнаружения	Продукты ИнфоТеКС: <ul style="list-style-type: none">• ViPNet IDS NS• ViPNet IDS HS• ViPNet TIAS Сервисы ПМ: лог-коллектор для сбора и анализа событий с других источников и для ретроспективного анализа
Средства предупреждения	Сервисы ПМ: <ul style="list-style-type: none">• Управление уязвимостями• Учет угроз
Средства ликвидации последствий	ViPNet TIAS: <ul style="list-style-type: none">• Учет и обработка КА• Взаимодействие с НКЦКИ Сервис ПМ: <ul style="list-style-type: none">• Управление процессами реагирования• Взаимодействие с НКЦКИ• Информационно-аналитическое сопровождение пользователей
Средства ППКА	COA ViPNet IDS NS * для IT-сетей
СКЗИ	<ul style="list-style-type: none">• ViPNet Coordinator• ViPNet Client

VIPNet TIAS
Administrator ▼ 0

Мониторинг

- Инфопанель ▲
- Сетевая активность
- Уловая активность
- Инциденты 27
- События ▲
- Сетевые
- Уловые
- Отчеты
- Управление
- Инфраструктура
- Оповещение
- Интеграция
- Экспертные данные
- Система
- Учетные записи
- Лицензия
- Сбор и отображение данных
- Аудит
- Журнал аудита

Сетевая активность 15 м 60 м 24 ч 📅 19.08.2019 00:00 - 31.08.2019 23:45 🔄 Автообновление 🔄

Динамика событий

Информация	Сканирование сети	Подбор паролей	Нарушение политик	Трояны и вирусы	DDoS	Эксплуатация (сервисы и уязвимости)
IDS NS: 335705	IDS NS: 147687	IDS NS: 2896	IDS NS: 2339897	IDS NS: 43719	IDS NS: 37998	IDS NS: 46522
IDS HS: 1	IDS HS: 0	IDS HS: 0	IDS HS: 1	IDS HS: 0	IDS HS: 0	IDS HS: 10
Всего: 335706	Всего: 147687	Всего: 2896	Всего: 2339898	Всего: 43719	Всего: 37998	Всего: 46532
Изменение: ↗ >10000%	Изменение: —	Изменение: —	Изменение: —	Изменение: —	Изменение: —	Изменение: —

Другие

IDS NS: 12345000
IDS HS: 69657
Всего: 12414657
Изменение: —

События ■ События IDS NS ■ События IDS HS

Инциденты Всего: 23 | 📄 Не обработаны: 21 📄 В работе: 0 📄 Подтверждены: 2 📄 Не подтверждены: 0

17:47:44 11.09.2019

Реагирование

VIPNet TIAS Administrator 1

Инциденты

15 м 60 м 24 ч 19.08.2019 00:00 - 31.08.2019 23:45 Автообновление

Количество инцидентов: 29

Статус	Тип ин...	Польз...	Дата и время	Рейтинг	Пораж...	Тип угр...	Наимен...	Описание
Не обрабо...	Сетевой		22.08.2019 11:37:31	8	10.0.7.243		Классифика...	
Не обрабо...	Сетевой		22.08.2019 11:11:28	10	10.0.7.243		Классифика...	
Не обрабо...	Сетевой		22.08.2019 10:27:04	9	10.0.7.248		Классифика...	
Не обрабо...	Сетевой		22.08.2019 09:00:18	10	91.244.183...	Нарушение ...	Загрузка вр...	Зафиксирована загрузка вр...
Не обрабо...	Сетевой		22.08.2019 08:19:49	10	10.0.3.235		Классифика...	
Не обрабо...	Сетевой		22.08.2019 03:31:57	10	91.244.183...	Нарушение ...	Загрузка вр...	Зафиксирована загрузка вр...
Не обрабо...	Сетевой		22.08.2019 03:27:51	10	11.0.3.98		Классифика...	
Не обрабо...	Сетевой		21.08.2019 19:37:59	10	10.0.7.243		Классифика...	
Не обрабо...	Сетевой		21.08.2019 19:03:36	7	91.244.183...	Иное	Множество...	Выявлены многочисленные...
Не обрабо...	Сетевой		21.08.2019 19:03:20	7	10.0.7.93	Иное	Множество...	Выявлены многочисленные...
Не обрабо...	Сетевой		21.08.2019 18:15:33	10	10.0.7.241		Классифика...	
Не обрабо...	Сетевой		21.08.2019 18:05:43	9	10.0.7.243		Классифика...	
Не обрабо...	Сетевой		21.08.2019 18:03:26	10	10.0.8.26		Классифика...	
Не обрабо...	Сетевой		21.08.2019 14:25:12	10	10.0.8.125		Классифика...	
Не обрабо...	Сетевой		21.08.2019 13:59:52	10	91.244.183...	Нарушение ...	Загрузка вр...	Зафиксирована загрузка вр...
Не обрабо...	Сетевой		21.08.2019 12:41:08	10	10.0.7.249		Классифика...	
Подтверж...	Сетевой	Administra...	21.08.2019 09:43:46	10	172.16.1.1		Классифика...	

192.168.1.2

Связанные события

Дата и время	Правило	IP-адрес источни...	IP-адрес получат...	Пакет
22.08.2019 03:31:39	Malware: EICAR test file	213.211.198.62:80	91.244.183.252:35378	

Загрузка вредоносного файла

Высокий уровень важности

Статус инцидента: Не обработан [Взглянуть в работу](#)

Тип инцидента: Сетевой
Рейтинг: 10
Дата и время: 22.08.2019 03:31:57

Пораженные узлы (1): ip: 91.244.183.252 mac: 00:50:56:b8:6e:86

Рекомендации

- Отключить пораженный актив от вычислительной сети
- Провести интервьюирование владельца
- Осуществить антивирусную проверку
- Осуществить ручной поиск "нелегального" (установленного без желания пользователя) ПО
- Передать обнаруженное вредоносное ПО в ЦМ для анализа
- Удалить обнаруженное вредоносное ПО

16.05.02 10.09.2019

VIPNet TIAS
Administrator

- Мониторинг
- Инфопанель
- Сетевая активность
- Узловая активность
- Инциденты
- События
- Сетевые
- Узловые
- Отчеты
- Управление
- Инфраструктура
- Оповещение
- Интеграция
- Экспертные данные
- Система
- Учетные записи
- Лицензия
- Сбор и отображение данных
- Аудит
- Журнал аудита

Узловые события

Узел: 10X64HSSERVER31 IP адрес: 127.0.0.1 Правило: Отключение задачи планировщика Уровень важности: Критичный, Высоки

Категории источников угроз на узле

Системная активность

Имя агента	Имя правила	Количество событий	Дата и время	IP-адрес агента
10X64HSSERVER31	Отключение задачи планировщика	1	25.08.2019 06:20:27	127.0.0.1
<p>Идентификатор сообщения: 156469068707954080 Идентификатор сенсора: 5F103c5a-7e4e-484c-a87b-08a0cc8fadab</p> <p>Имя агента: 10X64HSSERVER31 Идентификатор правила: 402043</p> <p>Имя правила: Отключение задачи планировщика Критичность события: Высокий</p> <p>Количество событий: 1 Дата и время: 25.08.2019 06:20:27</p> <p>Признак аномалии: Признаки аномалии отсутствуют Категория угрозы: Подозрительная активность</p> <p>Псевдоним службы: Имя службы:</p> <p>Полный путь к образу службы: Учетная запись службы:</p> <p>Тип службы: Тип запуска службы:</p> <p>Имя задачи: Полный путь к образу задачи:</p> <p>Активная учетная запись пользователя: Домен активной учетной записи пользователя:</p> <p>Sid активной учетной записи пользователя: Тип запуска (старое значение):</p> <p>IP агента: 5db97c5d-f4b3-40e3-8b2b-a119a0dc3190 IP-адрес агента: 127.0.0.1</p> <p>Название организации: Своа организация Идентификатор организации: f4f1bd50-a879-df1f-e3ef-f1586493dd62</p>				
10X64HSSERVER31	Отключение задачи планировщика	1	24.08.2019 04:45:01	127.0.0.1
10X64HSSERVER31	Отключение задачи планировщика	1	23.08.2019 06:11:24	127.0.0.1
10X64HSSERVER31	Отключение задачи планировщика	1	22.08.2019 08:07:40	127.0.0.1

<< < Страница 1 >

17:53:40 11.09.2019

Сбор доказательной базы

VIPNet TIAS Administrator 19.08.2019 00:00 - 31.08.2019 23:45 Автообновление

Сетевые события

15 м 60 м 24 ч 19.08.2019 00:00 - 31.08.2019 23:45 Автообновление

События IDS NS События IDS HS

Источники **DDoS** Получатели **DDoS**

Урове..	Правило	Ко..	IP-адр..	IP-адр..	Прото..	Номер..	Категор..
Высокий	AM SNMP Atte...	21439	20.0.2.1...	10.0.21.111	UDP	1:3006120	DDoS
Высокий	AM SNMP Atte...	7978	43.226...		UDP	1:3006120	DDoS
Высокий	AM SNMP Atte...	1703	43.226...		UDP	1:3006120	DDoS
Высокий	AM SNMP Atte...	1371	218.64...		UDP	1:3006120	DDoS
Высокий	AM SNMP Atte...	1051	218.64...		UDP	1:3006120	DDoS
Высокий	AM SNMP Atte...	1018	43.226...		UDP	1:3006120	DDoS
Высокий	AM SNMP Atte...	769	185.251...		UDP	1:3006120	DDoS
Высокий	AM CURRENT...	404	20.0.2.88	10.0.21.111	ICMP	1:3001647	DDoS
Высокий	AM SNMP Atte...	252	47.111...		UDP	1:3006120	DDoS
Высокий	AM SNMP Atte...	237	45.239...		UDP	1:3006120	DDoS

Урове..	Правило	Ко..	IP-адр..	IP-адр..	Прото..	Номер..	Категор..
Высокий	AM SNMP Atte...	21439	10.0.3.2...	10.0.21.111	UDP	1:3006120	DDoS
Высокий	AM SNMP Atte...	15690	91.244...		UDP	1:3006120	DDoS
Высокий	AM CURRENT...	272	10.0.3.9	10.0.21.111	ICMP	1:3001647	DDoS
Высокий	AM CURRENT...	132	10.0.3.5	10.0.21.111	ICMP	1:3001647	DDoS
Высокий	ET DOS Possib...	31	91.244...	10.0.21.111	UDP	1:2017919	DDoS
Высокий	ET DOS Possib...	29	91.219...		UDP	1:2017919	DDoS
Высокий	ET DOS Possib...	29	91.219...		UDP	1:2017919	DDoS
Высокий	ET DOS Possib...	28	91.219...		UDP	1:2017919	DDoS
Высокий	ET DOS Possib...	28	91.219...		UDP	1:2017919	DDoS
Высокий	ET DOS Possib...	27	81.30.1...		UDP	1:2017919	DDoS

События на узлах

Дата и время	Номер правила	IP-адрес сенс...	IP-адрес получ...	Порт п...	IP-адрес источ...	Порт и...	Пакет	Уровень важн...	Протоко...	Колич..	Правило
28.08.2019 16:18:59	119:22	10.0.21.111	10.0.4.245	3128		0	↓	Средний	TCP	1288	HI CHUNK SIZE MISMATCH
28.08.2019 16:18:56	1:2027865	10.0.21.111	10.0.21.111	53	10.0.18.133	49249	↓	Высокий	UDP	1	ET INFO Observed DNS Query to cl...
28.08.2019 16:18:56	1:2027189	10.0.21.111	10.0.7.247	445	10.0.4.223	49441	↓ Пакет	Высокий	TCP	1	ET NETBIOS DCERPC DCOM Execut...
28.08.2019 16:18:56	1:2027189	10.0.21.111	10.0.7.247	445	10.0.4.223	49441	↓	Высокий	TCP	1	ET NETBIOS DCERPC DCOM Execut...
28.08.2019 16:18:56	1:2027865	10.0.21.111	10.0.26.100	53	10.0.18.122	16369	↓	Высокий	UDP	1	ET INFO Observed DNS Query to cl...
28.08.2019 16:18:55	119:22	10.0.21.111	185.12.29.2	8088	10.0.14.165	0	↓	Средний	TCP	15	HI CHUNK SIZE MISMATCH
28.08.2019 16:18:55	119:22	10.0.21.111	10.0.25.3	8080		0	↓	Средний	TCP	601	HI CHUNK SIZE MISMATCH
28.08.2019 16:18:53	119:22	10.0.21.111	185.12.29.2	8088	91.244.183.5	44947	↓	Средний	TCP	1	HI CHUNK SIZE MISMATCH
28.08.2019 16:18:53	119:22	10.0.21.111	185.12.29.2	8088	91.244.183.5	33767	↓	Средний	TCP	1	HI CHUNK SIZE MISMATCH
28.08.2019 16:18:53	119:22	10.0.21.111	10.0.4.212	80	10.0.9.2	58351	↓	Средний	TCP	1	HI CLIENT CONSECUTIVE SMALL C...
28.08.2019 16:18:51	1:3005617	10.0.21.111	10.0.7.250	445	10.0.4.96	50372	↓	Критичный	TCP	1	AM Exloit Possible SAP (BU) FAI W...

Дополнительные события

17:52:11 11.09.2019

Порядок информирования

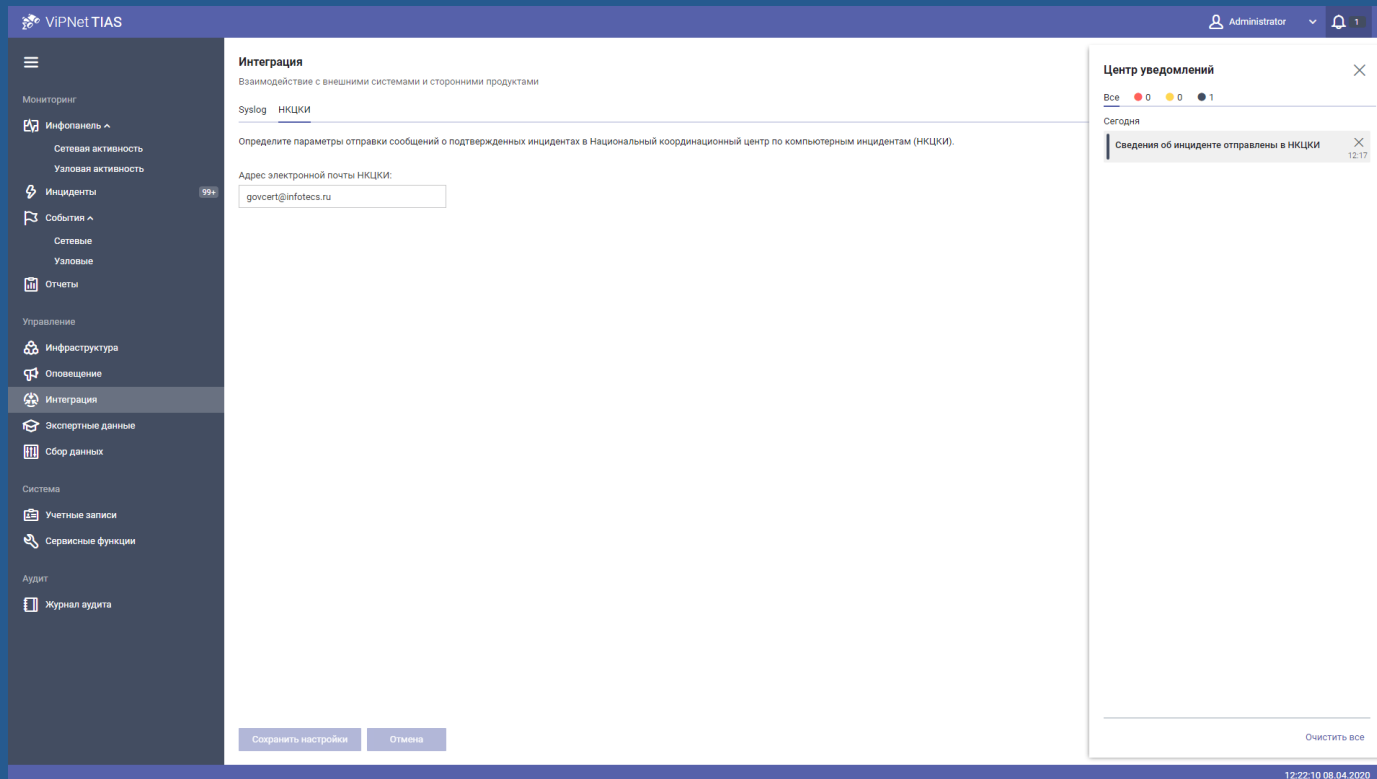


- Информация о компьютерном инциденте, связанном с функционированием значимого объекта критической информационной инфраструктуры, направляется субъектом критической информационной инфраструктуры в НКЦКИ **в срок не позднее 3 часов** с момента обнаружения компьютерного инцидента, а в отношении иных объектов 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



Взаимодействие с НКЦКИ
через ViPNet TIAS

Настройка передачи инцидентов в НКЦКИ



The screenshot displays the VIPNet TIAS web interface. The top navigation bar includes the logo, the text "VIPNet TIAS", and the user role "Administrator". A left sidebar contains a menu with categories: "Мониторинг" (Monitoring), "Управление" (Management), and "Аудит" (Audit). Under "Мониторинг", the "Инциденты" (Incidents) item is selected and shows a notification badge with "99+". The main content area is titled "Интеграция" (Integration) and contains the following text: "Взаимодействие с внешними системами и сторонними продуктами" (Interaction with external systems and third-party products), "Syslog НКЦКИ" (Syslog NKCCCI), and "Определите параметры отправки сообщений о подтвержденных инцидентах в Национальный координационный центр по компьютерным инцидентам (НКЦКИ)." (Specify the parameters for sending messages about confirmed incidents to the National Coordination Center for Computer Incidents (NKCCCI)). A form field labeled "Адрес электронной почты НКЦКИ:" (NKCCCI email address:) contains the text "govcert@infotecs.ru". At the bottom of the main area are two buttons: "Сохранить настройки" (Save settings) and "Отмена" (Cancel). On the right side, a "Центр уведомлений" (Notification Center) panel is open, showing a notification: "Сведения об инциденте отправлены в НКЦКИ" (Incident information sent to NKCCCI) at 12:17. The notification center also shows a summary: "Все" (All) with 0 red, 0 yellow, and 1 blue dots, and "Сегодня" (Today). At the bottom right of the notification center is a button "Очистить все" (Clear all). The footer of the interface shows the time "12:22:10 08.04.2020".

Карточка инцидента

VIPNet TIAS Administrator 0

Инциденты 15 м 60 м 24 ч 01.11.2019 11:17 - 08.04.2020 11:17

Количество инцидентов: 33185

Статус	Тип ин...	Дата и время	Рейтинг	Поражен...	Тип угрозы	Методы реали...	Наименование	Описание
Подтверж...	Сетевой	27.11.2019 08:12:26	4				Классификатором ...	
Подтверж...	Сетевой	27.11.2019 08:11:51	7				Классификатором ...	
Подтверж...	Сетевой	27.11.2019 08:11:37	10	172.16.1.1 192.168.1.2			Классификатором ...	
Подтверж...	Сетевой	27.11.2019 08:10:21	10	192.168.7.231	Нарушение конфи...	Эксплуатация уязв...	Успешная эксплуа...	Зафиксирована успешная эксплуатация о...
Подтверж...	Узловой	27.11.2019 08:09:53	10	127.0.0.1	Неизвестно	Подозрительная, п...	Запуск regsvr32 че...	Выявлен запуск regsvr32.exe через power...
Не обрабо...	Сетевой	27.11.2019 08:09:34	10	192.168.1.1	Нарушение конфи...	Эксплуатация уязв...	Успешная эксплуа...	Зафиксирована успешная эксплуатация у...
Не обрабо...	Сетевой	27.11.2019 08:09:34	10	172.16.1.1 192.168.1.2	Нарушение конфи...	Загрузка в систем...	Заражение хоста в...	Выявлена активность вредоносного ПО D...
Не обрабо...	Сетевой	27.11.2019 08:09:34	10	192.168.1.1 10.0.0.1	Нарушение конфи...	Загрузка в систем...	Заражение хоста т...	Выявлена активность трояна LoadMoney...
Не обрабо...	Сетевой	27.11.2019 08:09:34	10	192.168.78.14	Нарушение целост...	Загрузка в систем...	Заражение хоста т...	Выявлена активность вредоносного ПО п...
В работе	Сетевой	26.11.2019 11:41:12	4				Классификатором ...	
Не обрабо...	Сетевой	26.11.2019 11:40:52	7				Классификатором ...	
Не обрабо...	Сетевой	26.11.2019 11:40:44	10	172.16.1.1 192.168.1.2			Классификатором ...	
В работе	Сетевой	26.11.2019 11:39:11	10	192.168.7.231	Нарушение конфи...	Эксплуатация уязв...	Успешная эксплуа...	Зафиксирована успешная эксплуатация о...
Подтверж...	Узловой	26.11.2019 11:38:54	10	127.0.0.1	Неизвестно	Подозрительная, п...	Запуск regsvr32 че...	Выявлен запуск regsvr32.exe через power...
Не обрабо...	Сетевой	26.11.2019 11:38:42	10	172.16.1.1 192.168.1.2	Нарушение конфи...	Загрузка в систем...	Заражение хоста в...	Выявлена активность вредоносного ПО D...

Страница 1 / 25

Связанные события

Дата и время	Правило	IP-адрес источни...	Порт и...	IP-адрес получат...	Порт п...	Пакет
27.11.2019 08:10:12	AM successful HeartBleed vulnerability exploitation in SSL	10.0.112.91	34162	91.80.39.212	3478	

Успешная эксплуатация уязвимости в SSL - HeartBleed

Высокий уровень важности

Параметры инцидента НКЦКИ

Статус инцидента: Тип инцидента:

Способ передачи в НКЦКИ:

Дата и время отправки:

Категория инцидента (НКЦКИ):

Тип инцидента (НКЦКИ):

Тип инцидента:

Пользователь:

Рейтинг:

Количество срабатываний:

Общее количество событий:

Дата и время:

Дата и время обновления:

Тип угрозы:

Пораженные узлы (1):
Страна: Не определено
Город: Не определено

Сенсор

Идентификатор сенсора: 76604beb-7c07-47d8-8f11-757b07100964

IP-адрес сенсора: 192.168.71.14

Название сенсора: IDS HS (Savina - Branch - Segment)

Дополнительная информация

Методы реализации угрозы:

Метод обнаружения:

Симптомы:

12:03:41 08.04.2020

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
- Связи с другими инцидентами

*** Класс события информационной безопасности:**

Компьютерный инцидент

Компьютерный инцидент

Компьютерная атака

*** Тип:**

Попытка эксплуатации уязвимости

Идентификатор: incidentGS-dec8ec8a-e7fb-4cf2-8332-4e55931e4bd8

Регистрационный номер:

*** Степень конфиденциальности сведений об инциденте:**

White

Наименование организации-отправителя сведений об инциденте:

Оценка последствий

*** Нарушение конфиденциальности:** Высокий

*** Нарушение целостности:** Низкий

*** Нарушение доступности:** Низкий

Иная форма нарушения:

⚠ Для отправки заполните все обязательные поля.

Сохранить и отправить в НКЦКИ | Сохранить | Отмена

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
- Связи с другими инцидентами

* Название:
Внутренняя сеть городской больницы №2

* Категория значимости объекта КИИ:
Объект критической информационной инфраструктуры РФ без категории значимости

* Сфера деятельности:
Здравоохранение

* Место нахождения или географическое местоположение:
г. Москва

* Наименование организации-владельца:
Городская больница №2

Система подключена к сетям электросвязи

⚠ Для отправки заполните все обязательные поля.

Сохранить и отправить в НКЦКИ | Сохранить | Отмена

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

Связи с другими инцидентами

В данном разделе должно быть заполнено хотя бы одно поле об атакованных узлах.
[Добавить](#)

Доменное имя:	IP-адрес:
<input type="text" value="www.mgb2.ru"/>	<input type="text" value="10.0.112.91"/>
URI:	Уязвимость:
<input type="text"/>	<input type="text"/>

 Для отправки заполните все обязательные поля.

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

Связи с другими инцидентами

В данном разделе должно быть заполнено хотя бы одно поле об индикаторах компрометации.

[Добавить](#)

IP-адрес:	Доменное имя:
<input type="text" value="91.80.39.212"/>	<input type="text"/>
URI:	
<input type="text"/>	

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

Связи с другими инцидентами

*** Сведения о средстве или способе обнаружения:**


Система обнаружения вторжений уровня узла VIPNet IDS HS

Дата и время обнаружения события: 27.11.2019 08:10:21

Дата и время окончания события: 08.04.2020 12:11:30 

Дополнительные технические сведения:

Дополнительные комментарии к инциденту: Добавить

 Для отправки заполните все обязательные поля.

Сохранить и отправить в НКЦКИ Сохранить Отмена

Карточка инцидента в формате НКЦКИ

Параметры инцидента

Основное меню: [Основное меню](#) | [Настройка](#) | [Справка](#) | [Выход](#)

- Основные сведения
- Информация об атакованной информационной системе
- Информация об атакованных узлах
- Индикаторы компрометации
- Дополнительная информация об инциденте
- Меры по реагированию**
- Связи с другими инцидентами

*** Статус работ по реагированию:**

Проводятся мероприятия по реагированию на инцидент

Требуется содействие ГосСОПКА

*** Предпринятые меры по реагированию:**


[Добавить](#)

Пораженный актив отключен от вычислительной сети

Обновлен OpenSSL до актуальной версии

Сгенерированы новые новые ssl сертификаты и пары ключей

Сохранить и отправить в НКЦКИ | **Сохранить** | **Отмена**

 Для отправки заполните все обязательные поля.



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
- Связи с другими инцидентами**

[Добавить связь](#)

Регистрационный номер:	Тип связи с текущим инцидентом:	
<input type="text" value="incidentGS--dec8ec8a-e7fb-4cf2-8332-4e55931e4"/>	<input type="text" value="Предшествующий инцидент или атака"/>	
Регистрационный номер:	Тип связи с текущим инцидентом:	
<input type="text" value="incidentGS--dec8ec8a-e7fb2-4e55931e4bd8"/>	<input type="text" value="Дочерний инцидент"/>	

Карточка инцидента в формате НКЦКИ

VIPNet TIAS Administrator 1

Инциденты

15 м 60 м 24 ч 01.11.2019 11:17 - 08.04.2020 11:17

Успешная эксплуатация уязвимости в SSL - HeartBleed
Высокий уровень важности

Параметры инцидента НКЦКИ

Статус инцидента: Подтвержден

Способ передачи в НКЦКИ: Отправлен на электронную почту НКЦК

Дата и время отправки: 08.04.2020 12:17:51

Категория инцидента (НКЦКИ): Попытка несанкционированного доступа

Тип инцидента (НКЦКИ): Попытка эксплуатации уязвимости

Тип инцидента: Сетевой

Пользователь: Administrator

Рейтинг: 10

Количество срабатываний: --

Общее количество событий: --

Дата и время: 27.11.2019 08:10:21

Дата и время обновления: --

Тип угрозы: Нарушение конфиденциальности

Пораженные узлы (1):
IP: 192.168.7.231
Страна: Не определено
Город: Не определено

Сенсор

Идентификатор сенсора: 76604beb-7c07-47d8-8f11-757b07100964

IP-адрес сенсора: 192.168.71.14

Название сенсора: IDS HS (Savina - Branch - Segment)

Дополнительная информация

Методы реализации угроз: Эксплуатация уязвимости

Метод обнаружения: Сигнатурный

Симптомы: Неожиданный рост исходящего трафика

Статус	Тип ин...	Дата и время	Рейтинг	Поражен...	Тип угрозы	Методы реали...	Наименование	Описание	Количество инцидентов: 331
Подтверж...	Сетевой	27.11.2019 08:12:26	4				Классификатором ...		
Подтверж...	Сетевой	27.11.2019 08:11:51	7				Классификатором ...		
Подтверж...	Сетевой	27.11.2019 08:11:37	10	172.16.1.1 192.168.1.2			Классификатором ...		
Подтверж...	Сетевой	27.11.2019 08:10:21	10	192.168.7.231	Нарушение конфи...	Эксплуатация уязв...	Успешная эксплуа...	Зафиксирована успешная эксплуатация о...	
Подтверж...	Узловой	27.11.2019 08:09:53	10	127.0.0.1	Неизвестно	Подозрительная, п...	Запуск regsvr32 че...	Выявлен запуск regsvr32.exe через power...	
Не обрабо...	Сетевой	27.11.2019 08:09:34	10	192.168.1.1	Нарушение конфи...	Эксплуатация уязв...	Успешная эксплуа...	Зафиксирована успешная эксплуатация у...	
Не обрабо...	Сетевой	27.11.2019 08:09:34	10	172.16.1.1 192.168.1.2	Нарушение конфи...	Загрузка в систем...	Заражение хоста в...	Выявлена активность вредоносного ПО D...	
Не обрабо...	Сетевой	27.11.2019 08:09:34	10	192.168.1.1 10.0.0.1	Нарушение конфи...	Загрузка в систем...	Заражение хоста т...	Выявлена активность трояна LoadMoney ...	
Не обрабо...	Сетевой	27.11.2019 08:09:34	10	192.168.78.14	Нарушение целост...	Загрузка в систем...	Заражение хоста т...	Выявлена активность вредоносного ПО п...	
В работе	Сетевой	26.11.2019 11:41:12	4				Классификатором ...		
Не обрабо...	Сетевой	26.11.2019 11:40:52	7				Классификатором ...		
Не обрабо...	Сетевой	26.11.2019 11:40:44	10	172.16.1.1 192.168.1.2			Классификатором ...		
В работе	Сетевой	26.11.2019 11:39:11	10	192.168.7.231	Нарушение конфи...	Эксплуатация уязв...	Успешная эксплуа...	Зафиксирована успешная эксплуатация о...	
Подтверж...	Узловой	26.11.2019 11:38:54	10	127.0.0.1	Неизвестно	Подозрительная, п...	Запуск regsvr32 че...	Выявлен запуск regsvr32.exe через power...	
Не обрабо...	Сетевой	26.11.2019 11:38:42	10	172.16.1.1 192.168.1.2	Нарушение конфи...	Загрузка в систем...	Заражение хоста в...	Выявлена активность вредоносного ПО D...	

Связанные события

Дата и время	Правило	IP-адрес источни...	Порт и...	IP-адрес получат...	Порт п...	Пакет
27.11.2019 08:10:12	AM successful HeartBleed vulnerability exploitation in SSL	10.0.112.91	34162	91.80.39.212	3478	--

12:18:14 08.04.2020

The logo for 'infotecs' features the word in a bold, white, lowercase sans-serif font. Above the letter 'i' is a small orange dot, and a thin orange arc curves over the top of the letters 'f' and 'o'.

infotecs

A thin, vertical orange line is positioned between the logo and the text.

Спасибо