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

менеджер продукта Старовойт Светлана

Подключение к ГосСОПКА

Структура ГосСОПКА

Перечень мероприятий

infotecs

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

ГОССОПКА

Субъект ГосСОПКА

- Заключить соглашение с 8Ц ФСБ России
- Выполнить организационные и технологические требования к центру ГосСОПКА
- Обеспечить взаимодействие с технической инфраструктурой НКЦКИ

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Объект КИИ

Подключение через корпоративный центр

ГОССОПКА

Корпоративный центр ГосСОПКА

- Заключить соглашение с корпоративным (ведомственным) центром ГосСОПКА
- Уведомить НКЦКИ о включении своих ресурсов в зону ответственности цента

Приказы ФСБ России

- **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)

Перечень информации

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.

Приказ № 367 от 24 июля 2018 года

Порядок обмена

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";

Приказ № 368 от 24 июля 2018 года

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.

Приказ № 196 от 6 мая 2019 года

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;

Приказ № 196 от 6 мая 2019 года

Требования к средствам обмена и криптографическим средствам защиты информации

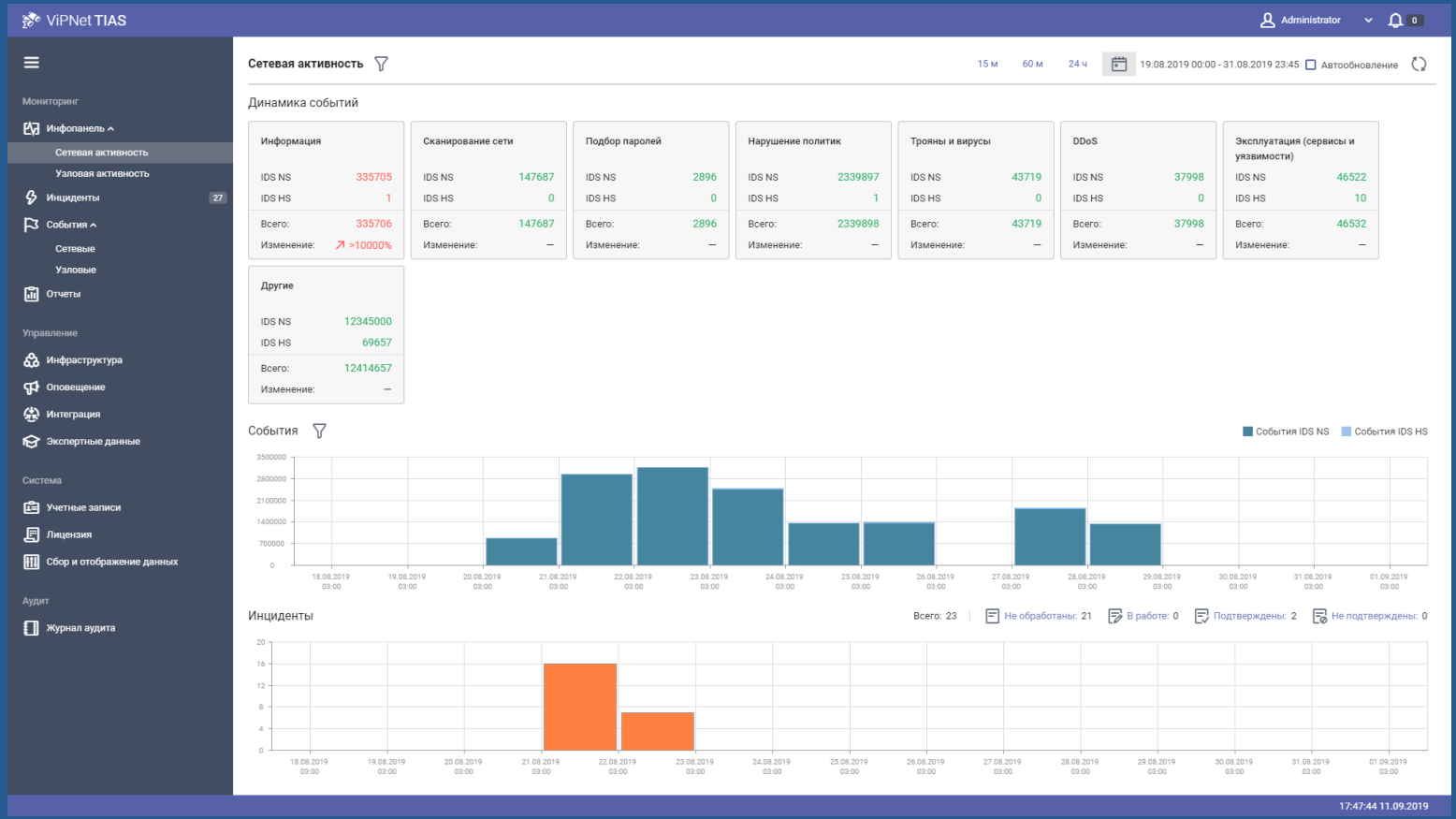
- Средства обмена должны обеспечивать передачу, прием и целостность при передаче и приеме информации, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.
- Криптографические средства защиты информации, необходимой субъектам критической информационной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

Приказ № 196 от 6 мая 2019 года

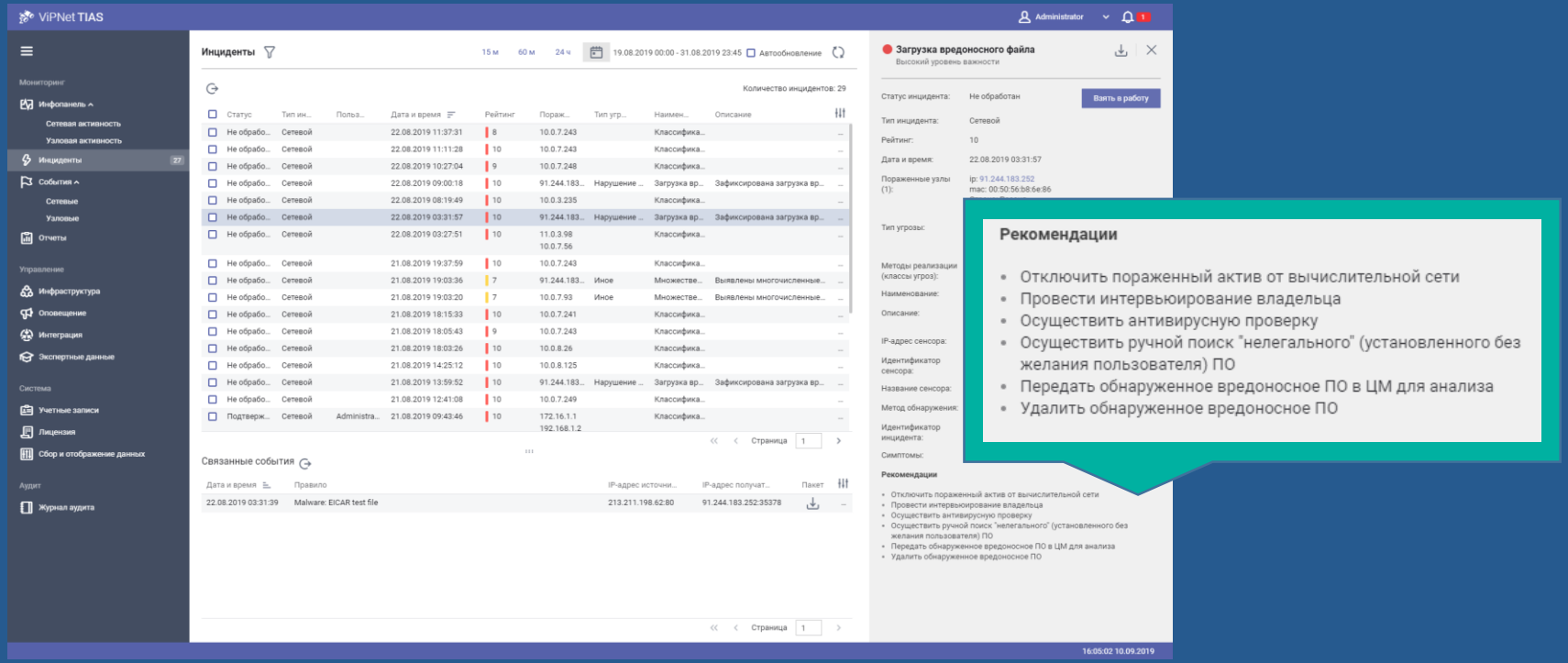
Средства ГосСОПКА

Средство ГосСОПКА	Продукты и сервисы
Средства обнаружения	Продукты ИнфоТеКС: • 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: • Управление уязвимостями • Учет угроз
Средства ликвидации последствий	ViPNet TIAS: • Учет и обработка КА • Взаимодействие с НКЦКИ Сервис ПМ: • Управление процессами реагирования • Взаимодействие с НКЦКИ • Информационно-аналитическое сопровождение пользователей
Средства ППКА	COA ViPNet IDS NS * для IT-сетей
СКЗИ	• ViPNet Coordinator • ViPNet Client

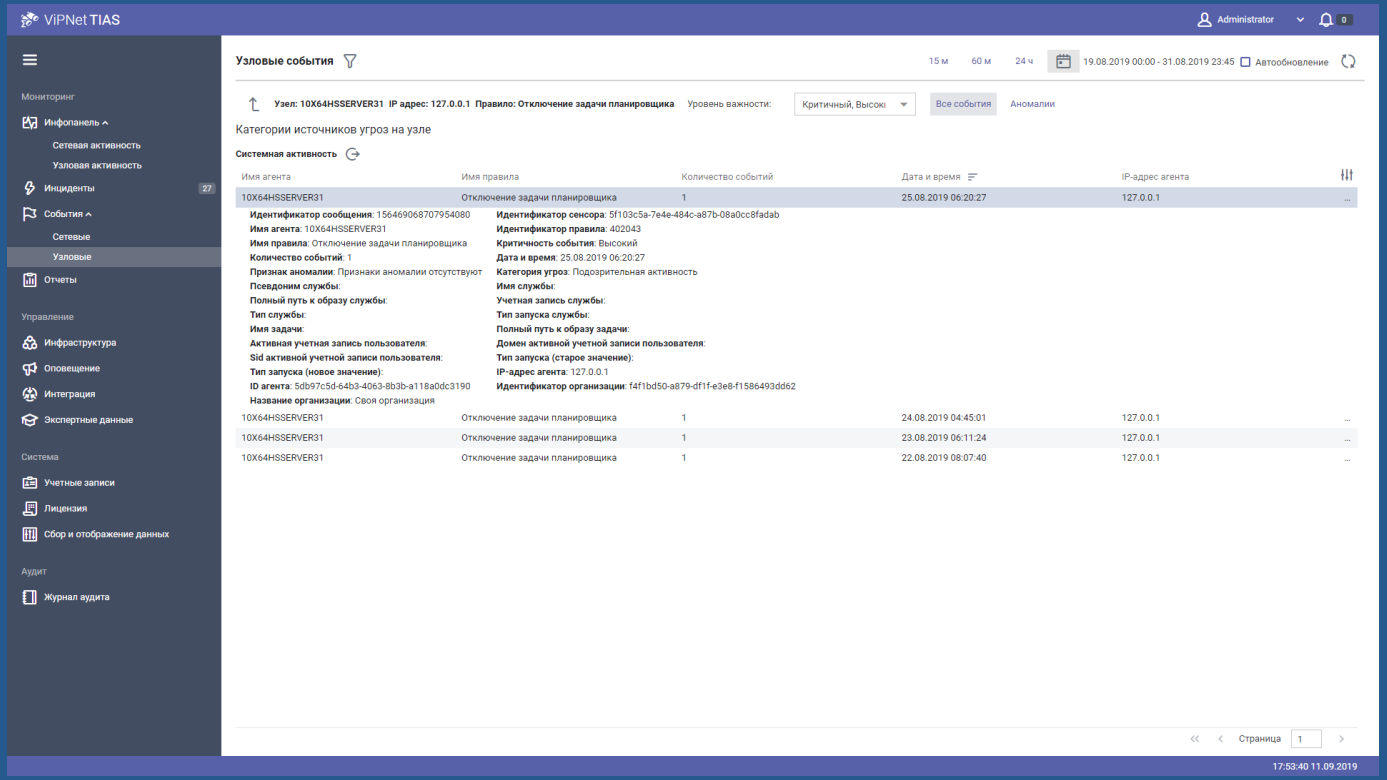
Обнаружение



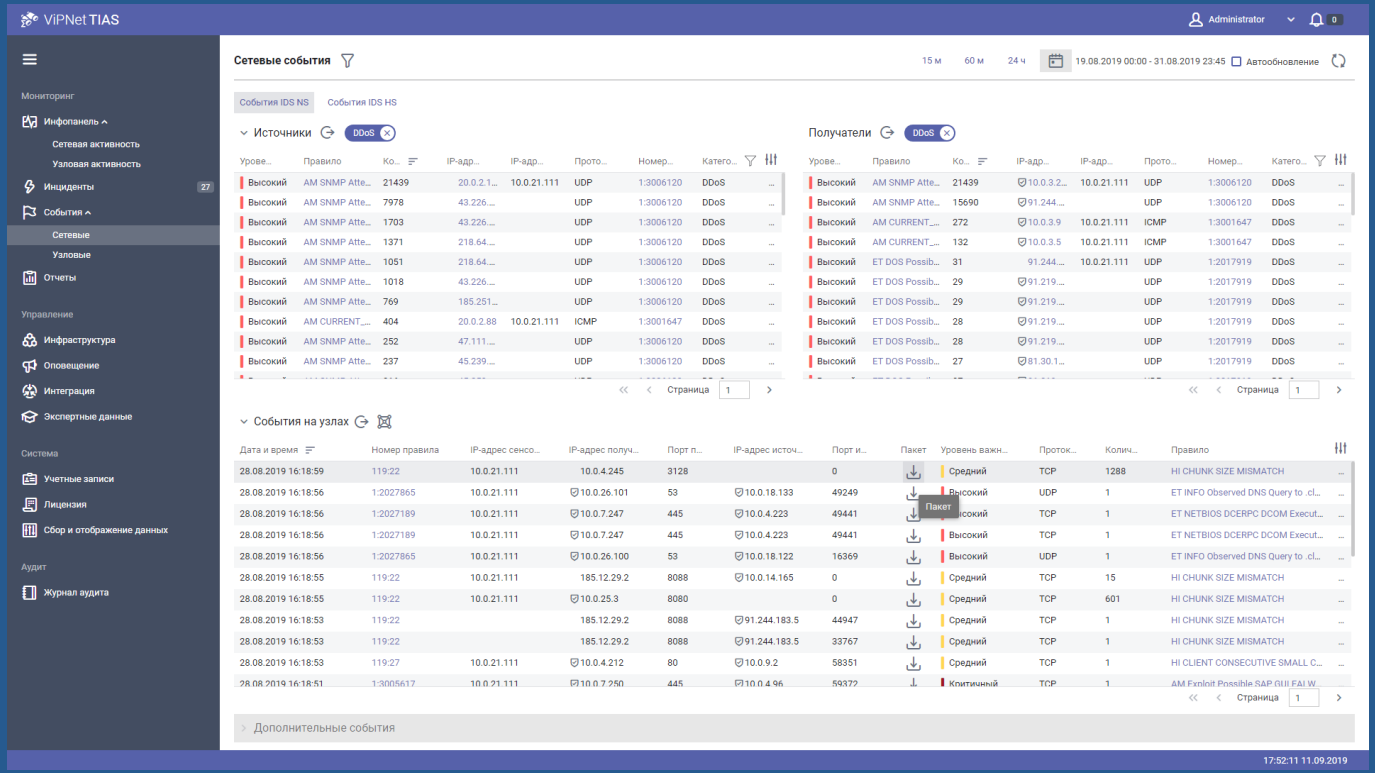
Реагирование



Расследование



Сбор доказательной базы



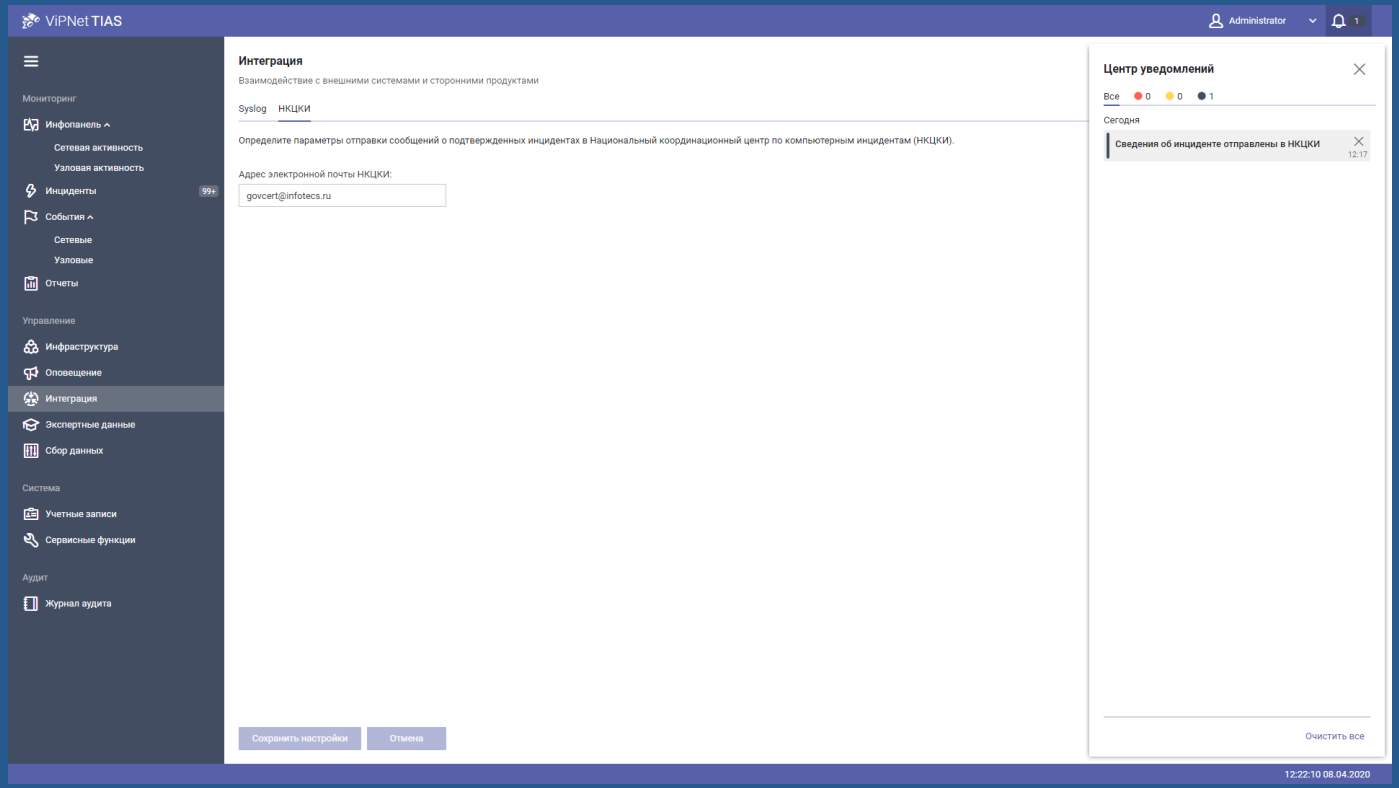
Порядок информирования

- 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

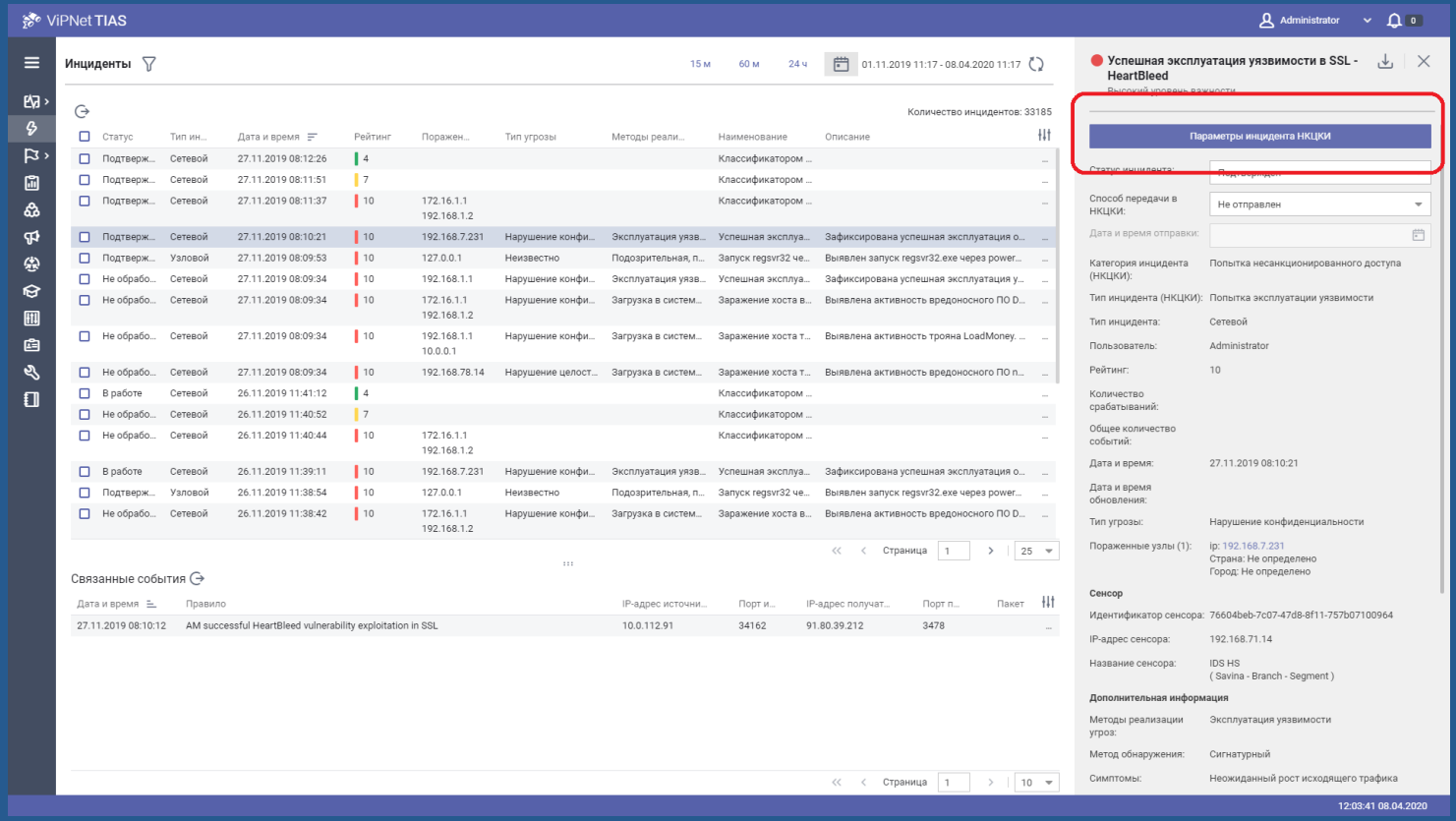
Приказ ФСБ России №282 от 19.06.2019

Взаимодействие с НКЦКИ через ViPNet TIAS

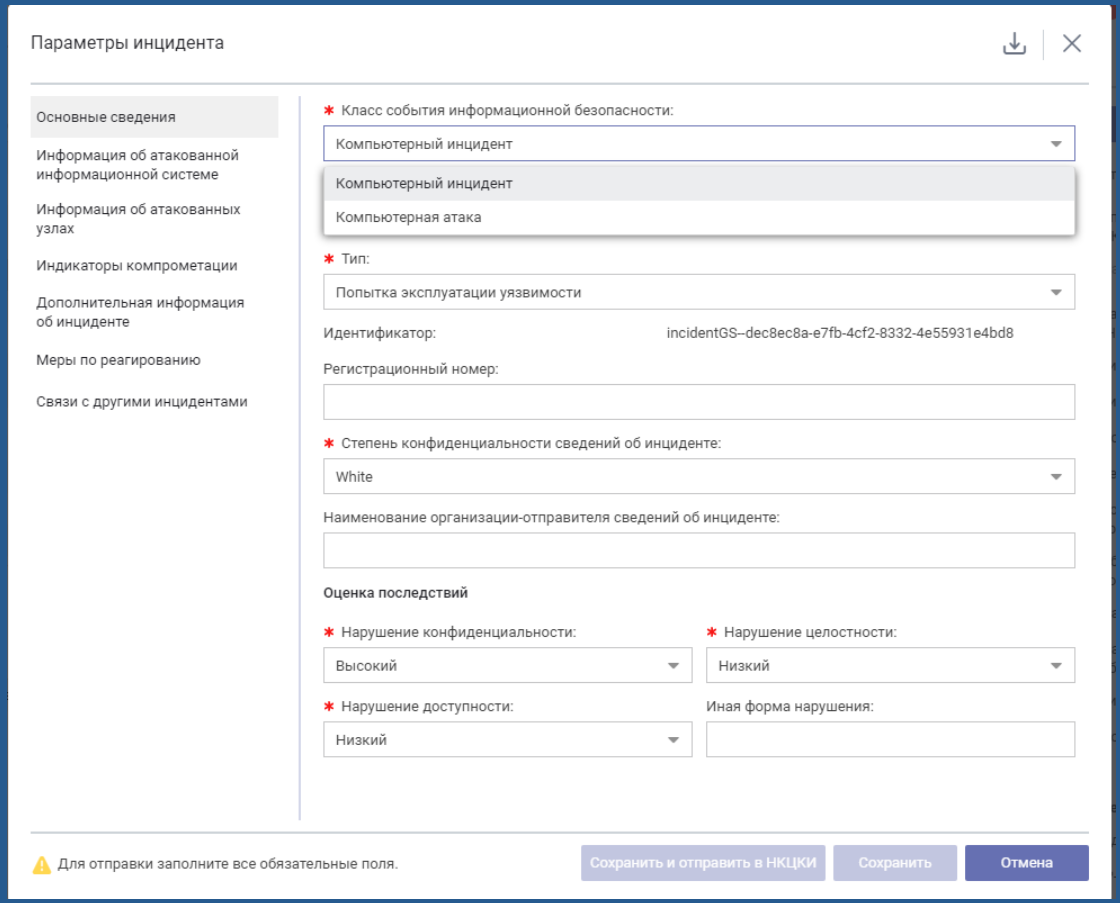
Настройка передачи инцидентов в НКЦКИ



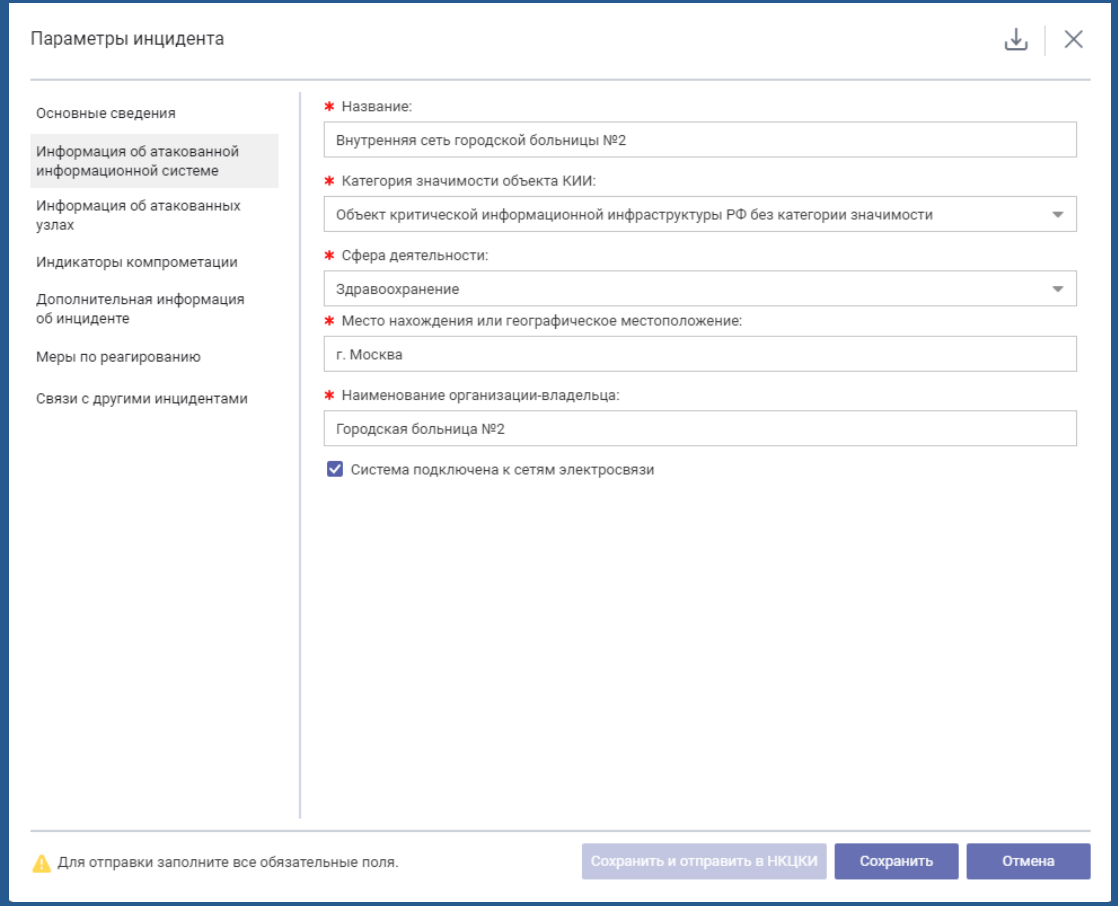
Карточка инцидента



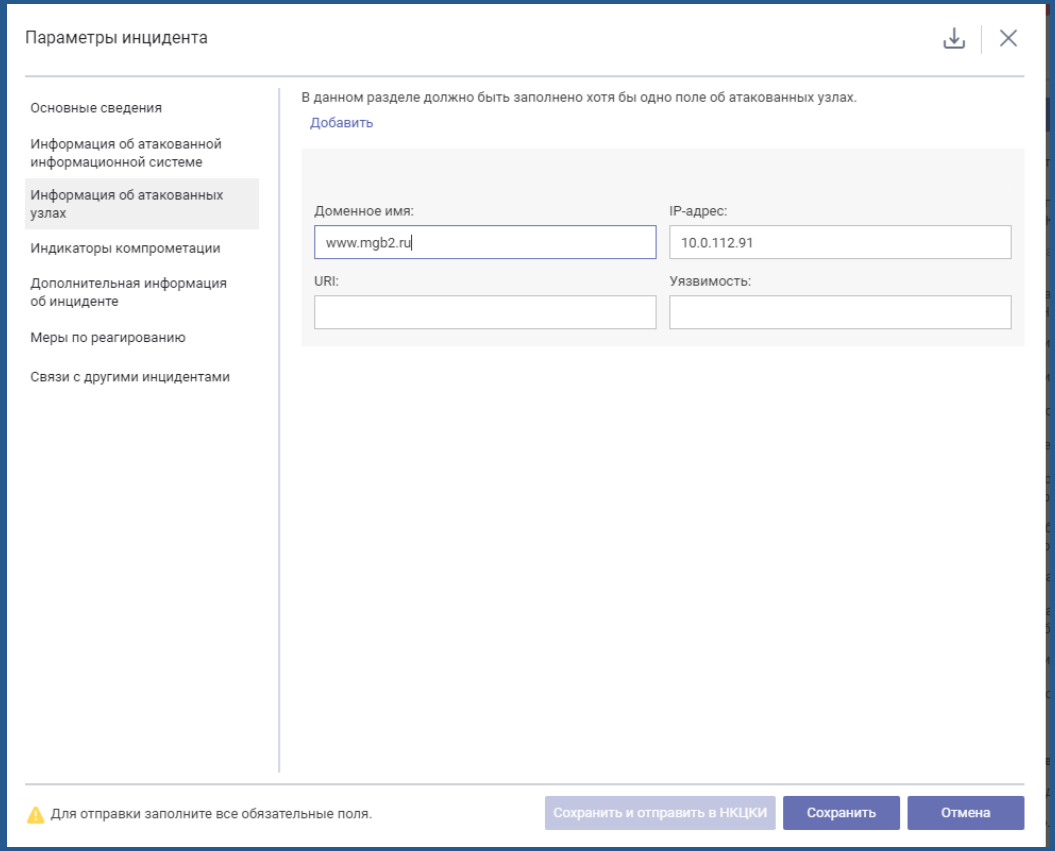
Карточка инцидента в формате НКЦКИ



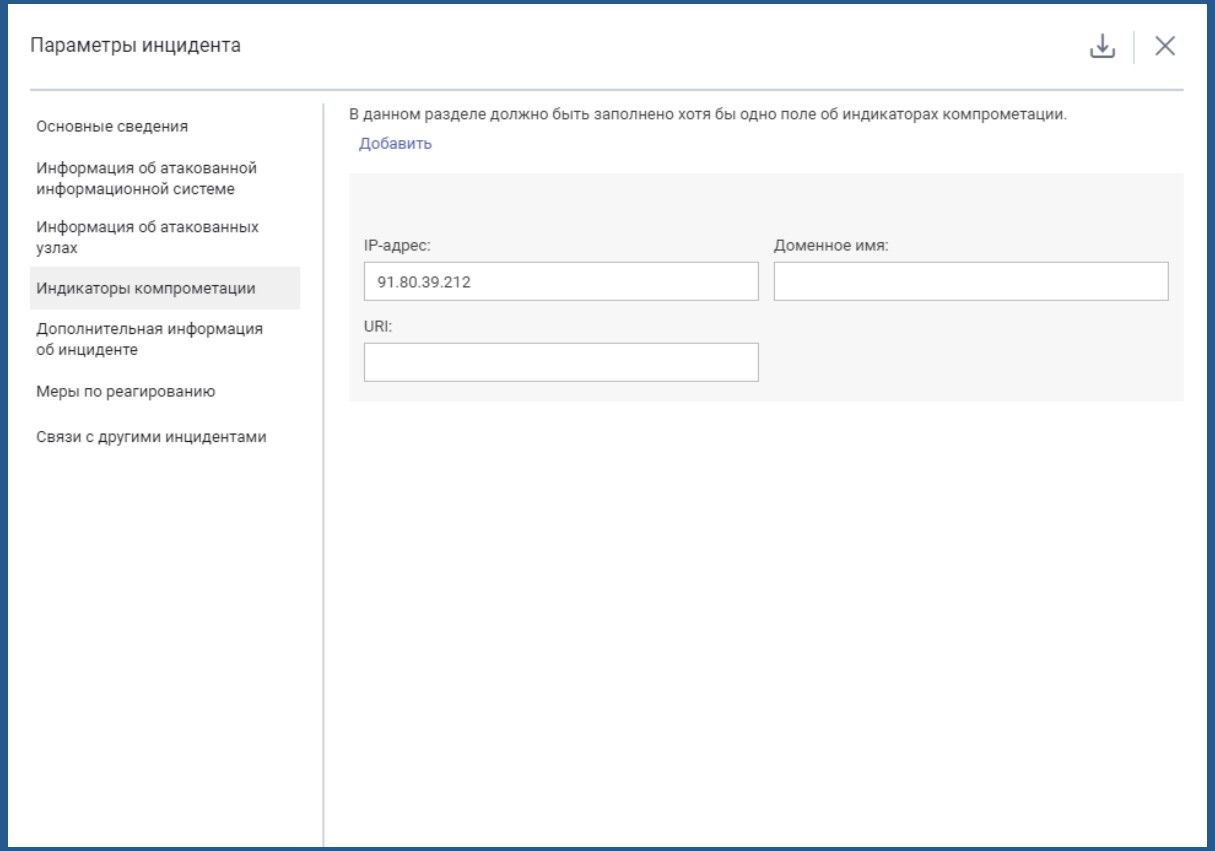
Карточка инцидента в формате НКЦКИ



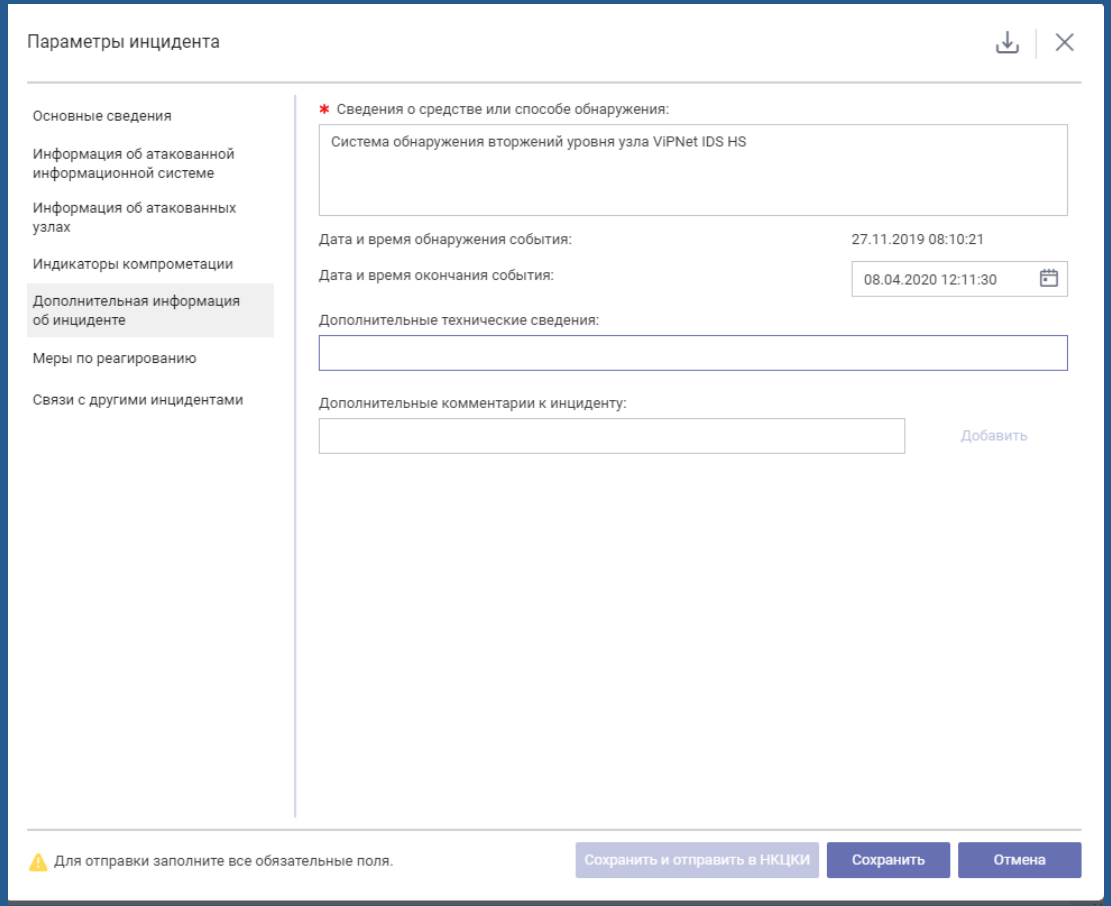
Карточка инцидента в формате НКЦКИ



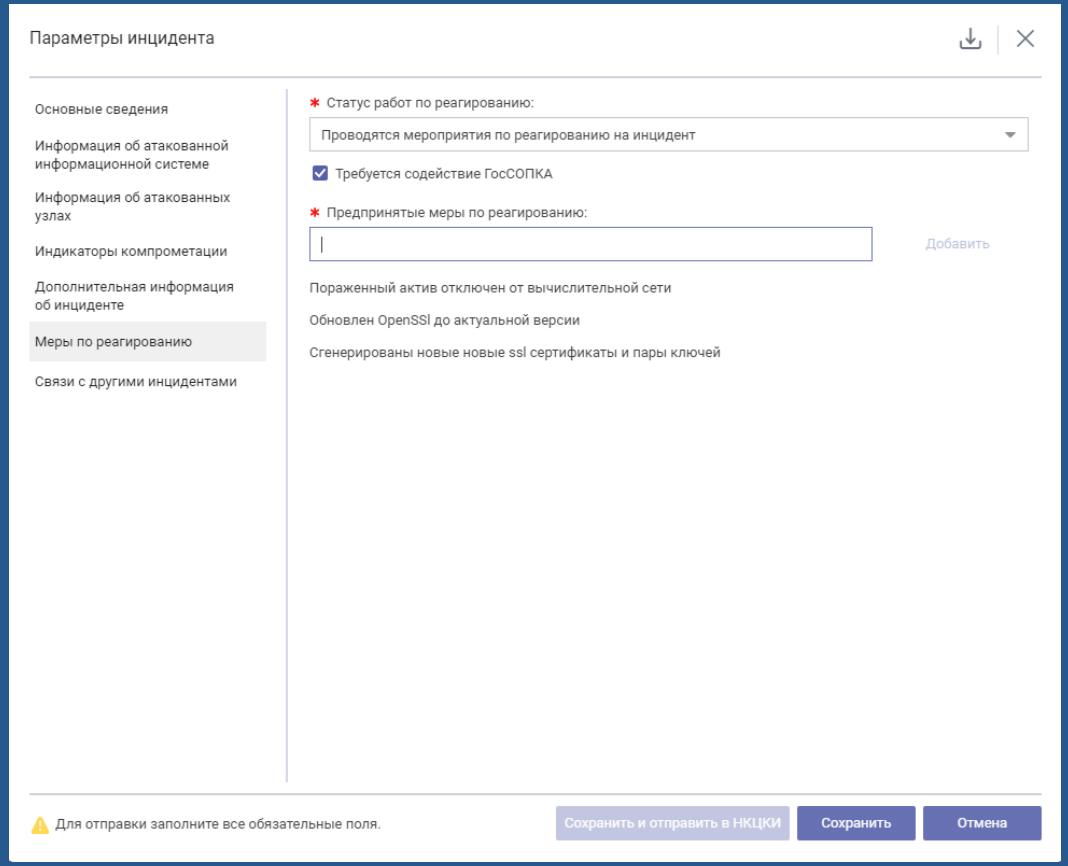
Карточка инцидента в формате НКЦКИ



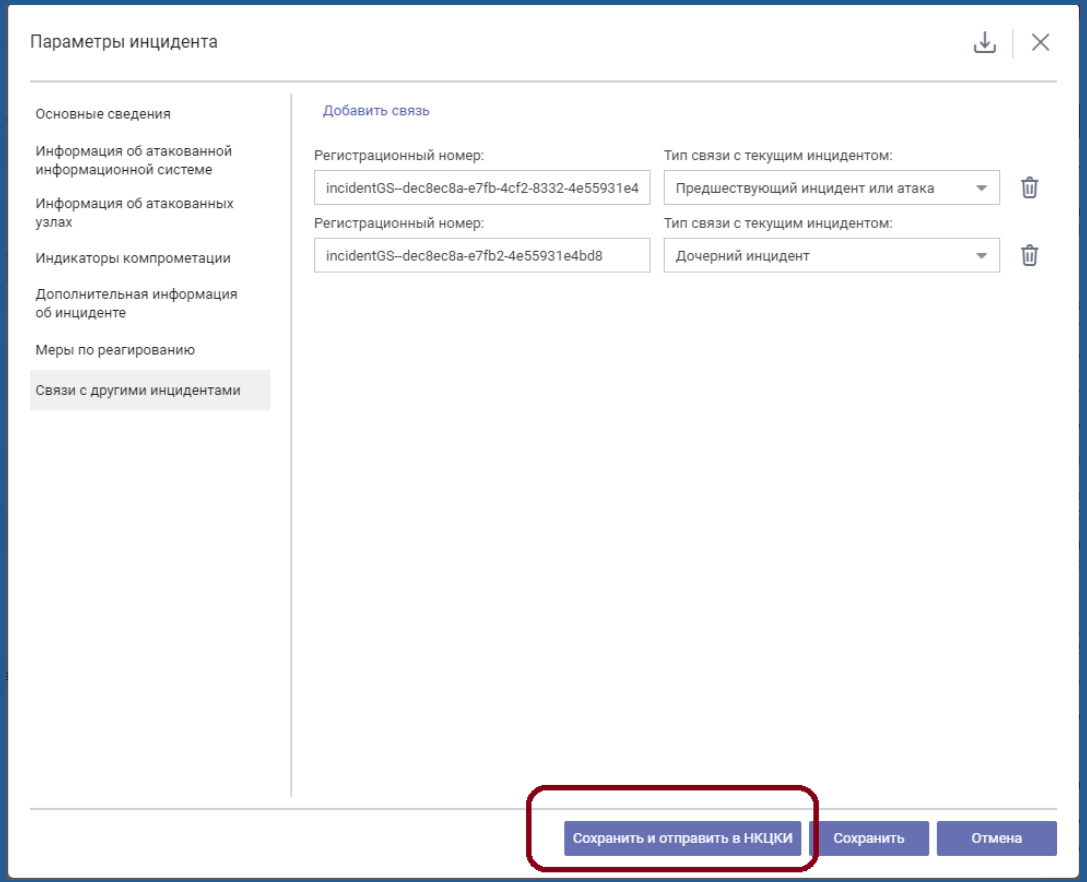
Карточка инцидента в формате НКЦКИ



Карточка инцидента в формате НКЦКИ

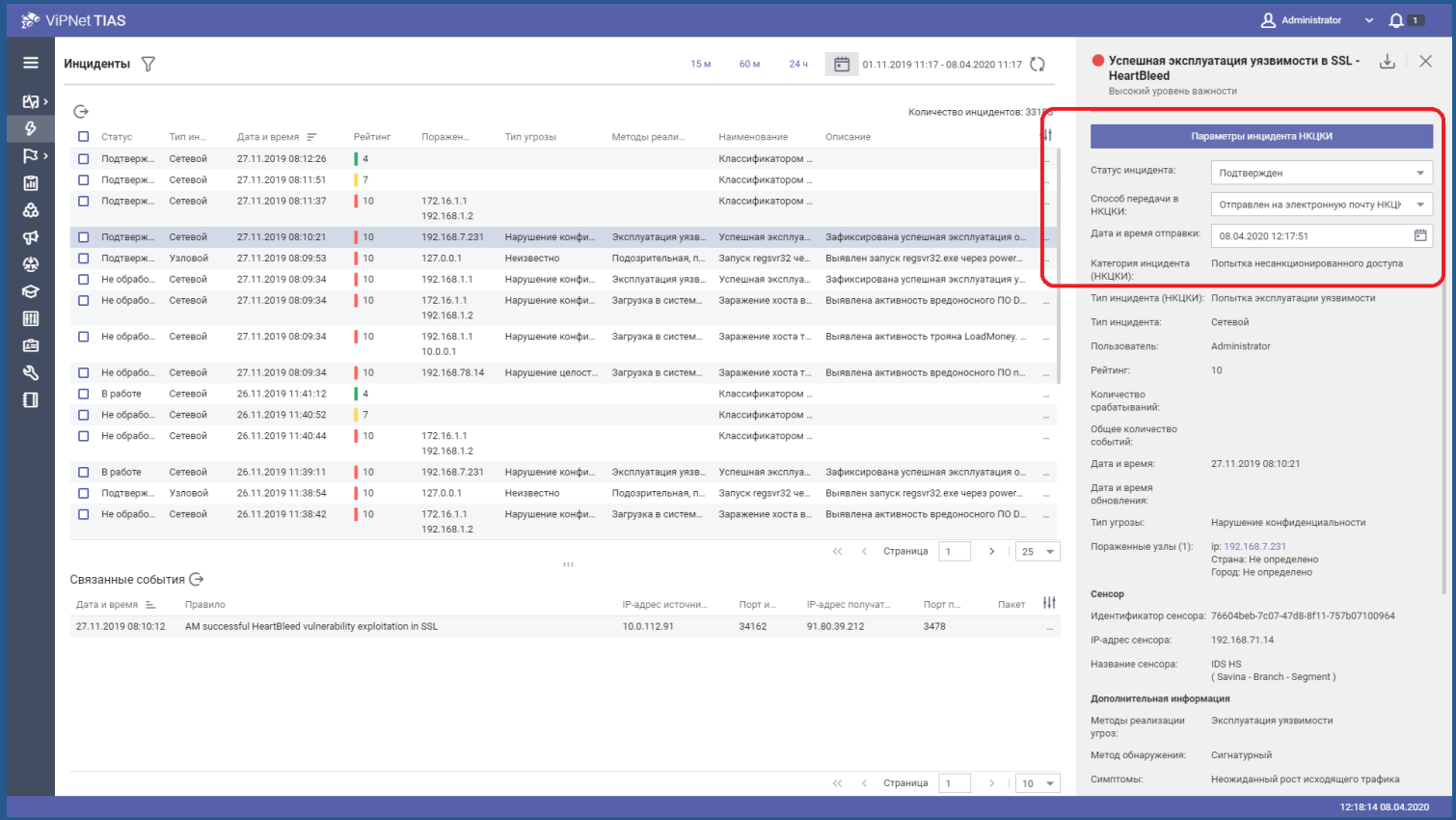


Карточка инцидента в формате НКЦКИ



Карточка инцидента в формате НКЦКИ

infotecs



infotecs

Спасибо