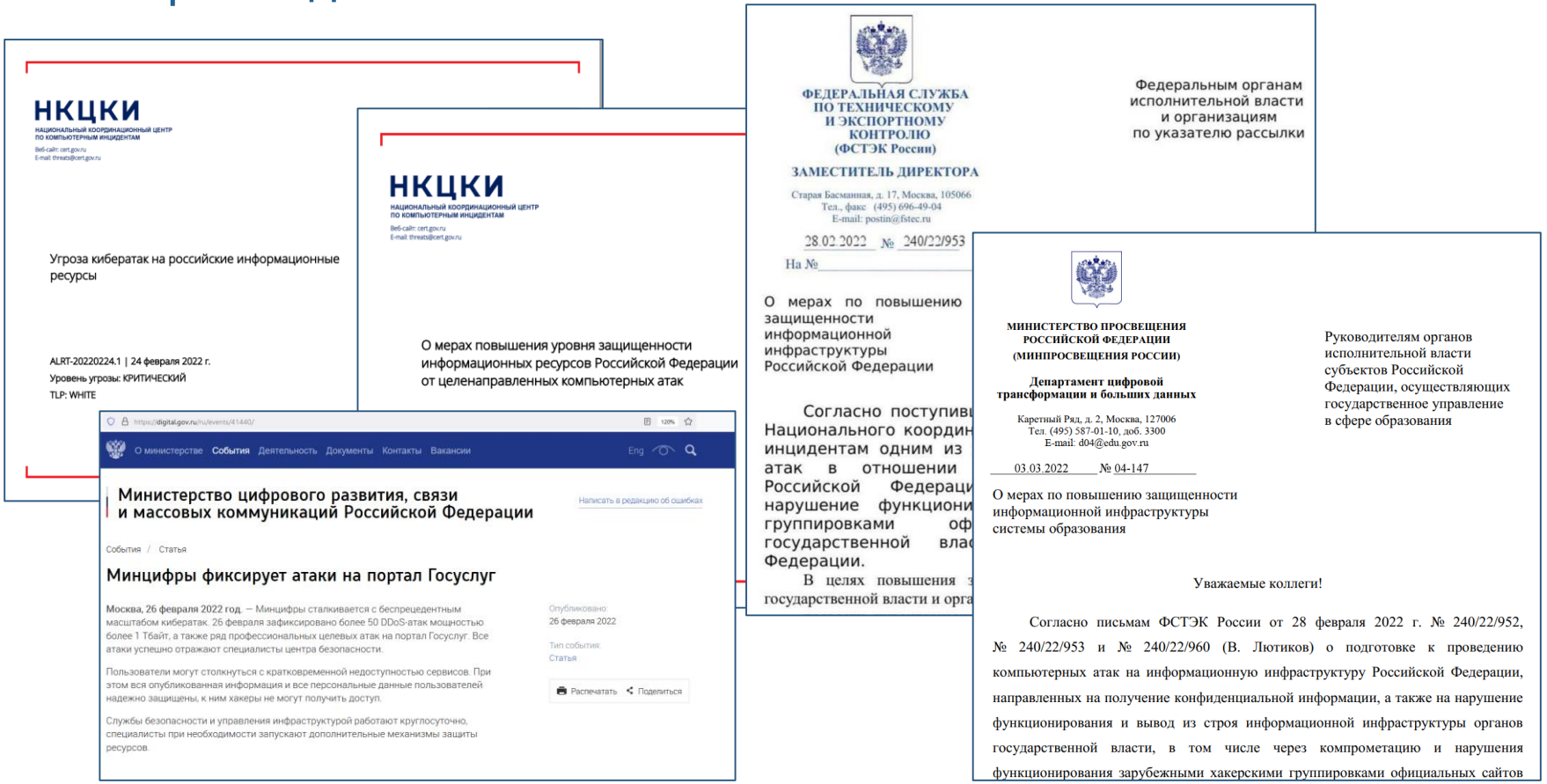


Типовые решения по защите информации на объектах КИИ

Антон Картамышев
руководитель направления

Киберпогода



НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ
Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Угроза кибератак на российские информационные ресурсы

ALRT-20220224.1 | 24 февраля 2022 г.
Уровень угрозы: КРИТИЧЕСКИЙ
TLP: WHITE

НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ
Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

О мерах повышения уровня защищенности информационных ресурсов Российской Федерации от целенаправленных компьютерных атак

https://digital.gov.ru/ru/events/41440/
О министерстве | События | Деятельность | Документы | Контакты | Вакансии | Eng

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Написать в редакцию об ошибках

События / Статья

Минцифры фиксирует атаки на портал Госуслуг

Москва, 26 февраля 2022 год. – Минцифры сталкивается с беспрецедентным масштабом кибератак. 26 февраля зафиксировано более 50 DDoS-атак мощностью более 1 Тбайт, а также ряд профессиональных целевых атак на портал Госуслуг. Все атаки успешно отражают специалисты центра безопасности.

Пользователи могут столкнуться с кратковременной недоступностью сервисов. При этом вся опубликованная информация и все персональные данные пользователей надежно защищены, к ним хакеры не могут получить доступ.

Службы безопасности и управления инфраструктурой работают круглосуточно, специалисты при необходимости запускают дополнительные механизмы защиты ресурсов.

Опубликовано:
26 февраля 2022

Тип события:
Статья

Распечатать | Поделиться

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК России)

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА

Старая Басманная, д. 17, Москва, 105066
Тел., факс (495) 696-49-04
E-mail: postin@fstec.ru

28.02.2022 № 240/22/953
На №

О мерах по повышению защищенности информационной инфраструктуры Российской Федерации

Согласно поступивш
Национального координ
инцидентам одним из
атак в отношении
Российской Федераци
нарушение функционир
группировками оф
государственной влас
Федерации.

В целях повышения з
государственной власти и орга

Федеральным органам исполнительной власти и организациям по указателю рассылки

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ (МИНПРОСВЕЩЕНИЯ РОССИИ)

Департамент цифровой трансформации и больших данных

Каретный Ряд, д. 2, Москва, 127006
Тел. (495) 587-01-10, доб. 3300
E-mail: d04@edu.gov.ru

03.03.2022 № 04-147

О мерах по повышению защищенности информационной инфраструктуры системы образования

Руководителям органов исполнительной власти субъектов Российской Федерации, осуществляющих государственное управление в сфере образования

Уважаемые коллеги!

Согласно письмам ФСТЭК России от 28 февраля 2022 г. № 240/22/952, № 240/22/953 и № 240/22/960 (В. Лютиков) о подготовке к проведению компьютерных атак на информационную инфраструктуру Российской Федерации, направленных на получение конфиденциальной информации, а также на нарушение функционирования и вывод из строя информационной инфраструктуры органов государственной власти, в том числе через компрометацию и нарушения функционирования зарубежными хакерскими группировками официальных сайтов

Субъекты и объекты КИИ РФ


Здравоохранение


Наука


Транспорт


Связь


Энергетика


Банковская сфера


Финансовые рынки


ТЭК


Атомная энергетика


Оборонная промышленность


Ракетно-космическая промышленность


Горнодобывающая промышленность


Металлургическая промышленность


Химическая промышленность


Обеспечение Взаимодействия ИС/ИТКС/АСУ


Информационные системы (ИС)


Информационно-телекоммуникационные сети (ИТС)


Автоматизированные системы управления (АСУ)

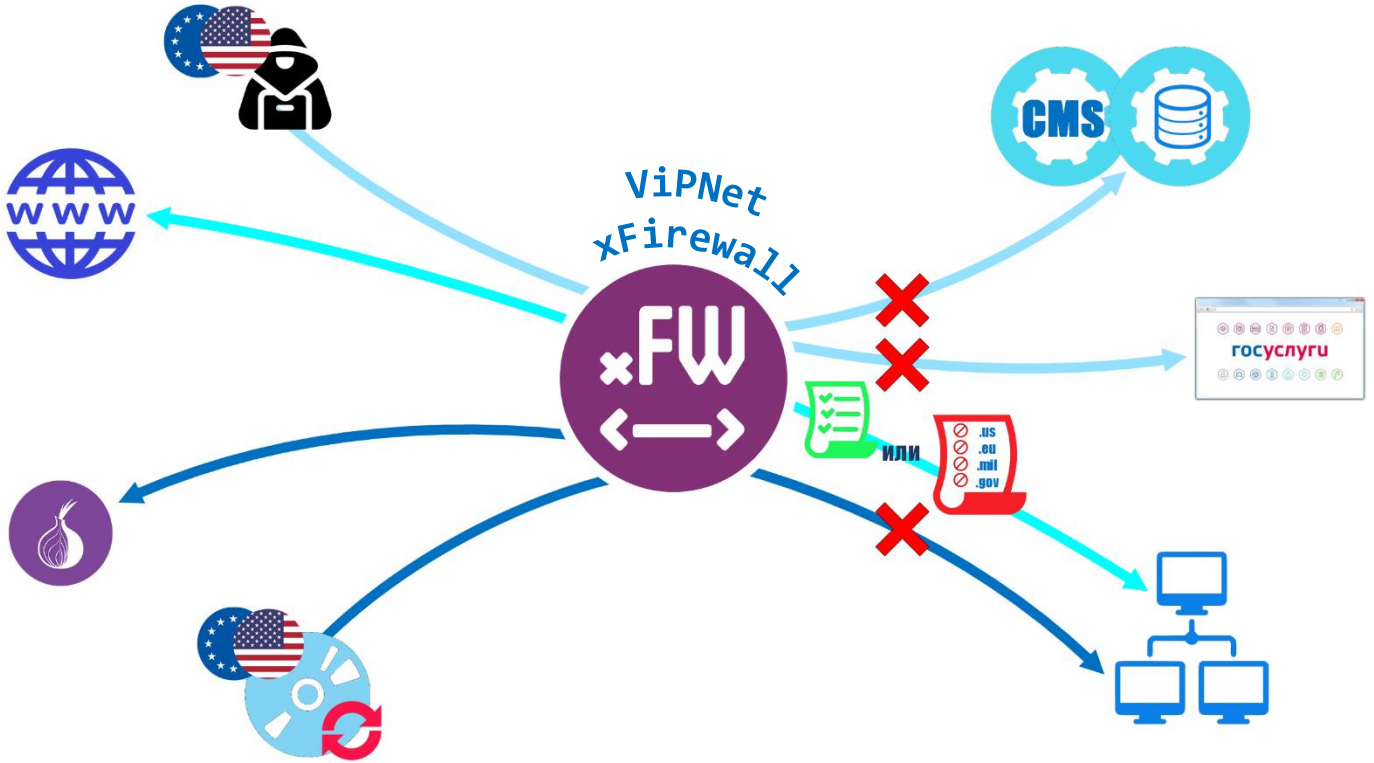
СЗИ ViPNet


Криптографическая защита данных
Защита сетей
Защита рабочих станций и серверов
Инфраструктура открытых ключей
ViPNet
Virtual Private Network
Защита индустриальных систем
Обнаружение и предотвращение вторжений
Защита мобильных устройств
Квантовая криптография



Типовые решения по защите информации

Сценарий 1. Защита ИС органов государственной власти



ViPNet xFirewall

Шлюз безопасности нового поколения

ИАФ | УПД | АУД | ЗИС

ОДТ | СОВ | ИНЦ



- Межсетевое экранирование уровня приложений
- Система предотвращения вторжений
- Прокси сервер



Сценарий 2. Защита информационного обмена и межсетевое экранирование



ViPNet Coordinator HW

Шлюз безопасности

ИАФ | УПД | АУД | ЗИС

ОДТ



- Криптографическая защита каналов связи
- Межсетевое экранирование
- Сегментирование сети
- Сетевые и сервисные функции
- Доверенная платформа





ViPNet Coordinator IG

Промышленный шлюз безопасности

ИАФ | УПД | АУД | ЗИС | ОДТ



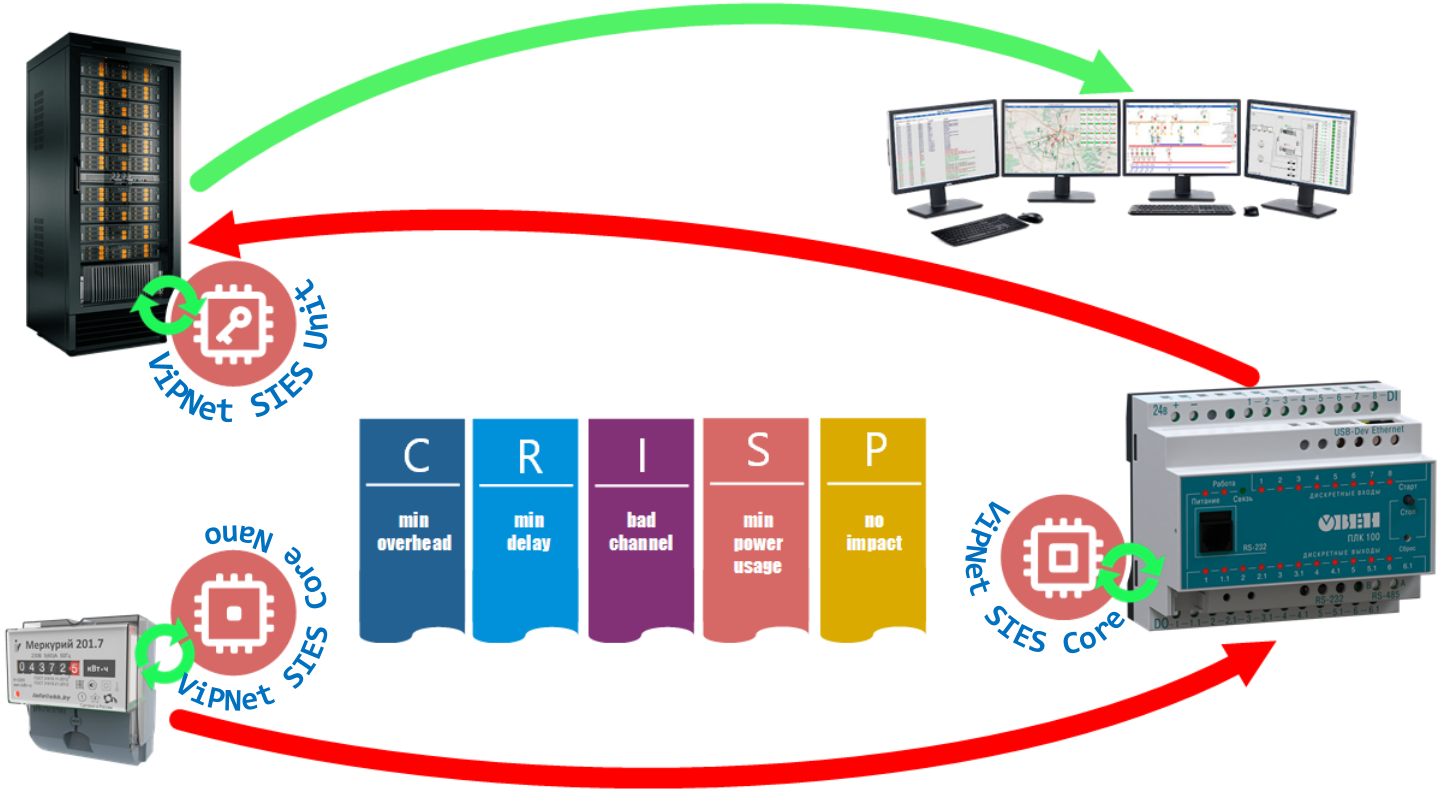


- Криптографическая защита каналов связи
- Межсетевое экранирование
- Глубокая фильтрация промышленных протоколов
- Преобразование Modbus RTU/TCP
- Расширенный температурный диапазон работы





Сценарий 3. Защита информационного обмена в промышленных сетях

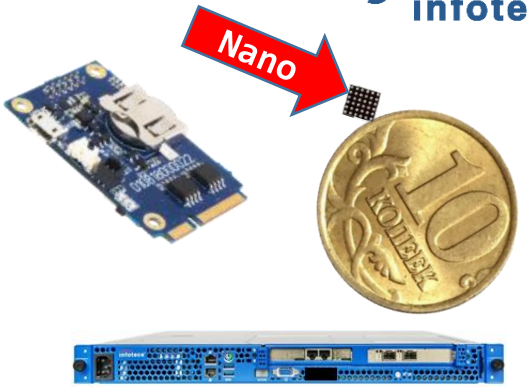


ViPNet SIES

Средство защиты информации в АСУ ТП

ИАФ | ОПС | АУД | ЗИС

ОДТ | ОПО

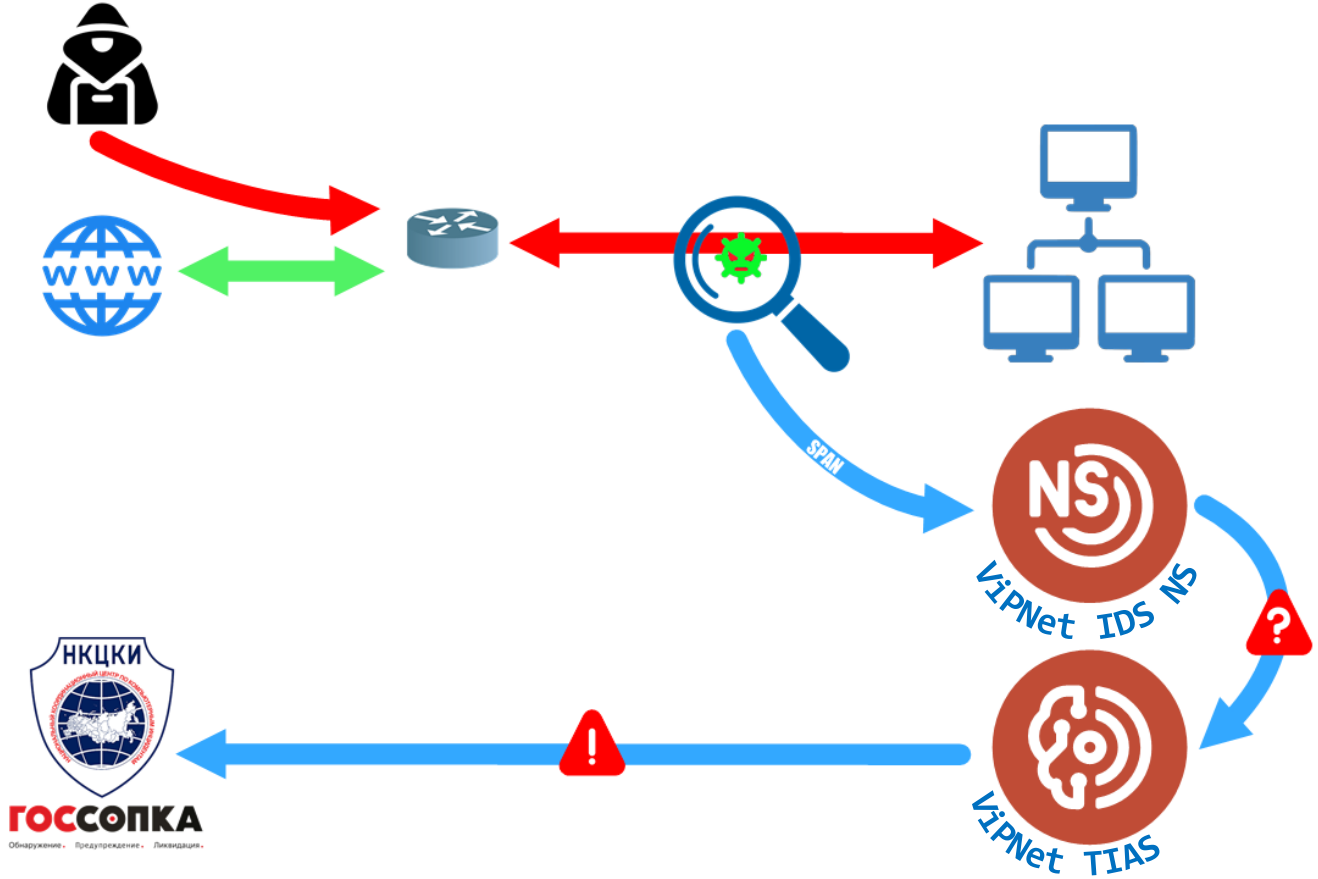


- Работа с любыми каналами связи и протоколами передачи данных с использованием CRISP
- Зашифрование/расшифрование
- Создание имитовставки/проверка имитовставки
- Создание ЭП/проверка ЭП в CMS
- Создание хэш/проверка хэш





Сценарий 4. Обнаружение вторжений и взаимодействие с НКЦКИ



ViPNet IDS NS

Средство обнаружения сетевых атак (вторжений) уровня сети

СОВ ИНЦ АУД



- Анализ сетевого трафика
- Сигнатурный и эвристический метод выявления аномалий
- Выявление сетевых атак
- Собственная обновляемая база сигнатур





ViPNet TIAS

Средство автоматического выявления инцидентов ИБ

ИНЦ АУД



- Прием событий ИБ от сенсоров уровня сети и хоста
- Сигнатурный и эвристический метод анализа
- Автоматическая регистрация инцидентов ИБ
- Взаимодействие с ГосСОПКА





Сценарий 5. Защита автоматизированных рабочих мест

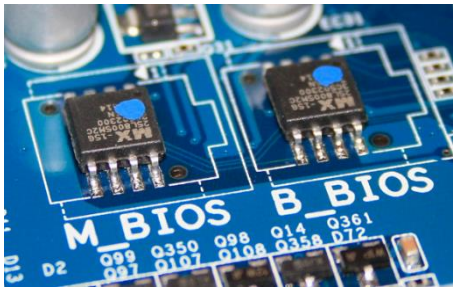


ViPNet SafeBoot

Средство доверенной загрузки

ИАФ | УПД | ОЦЛ | АУД

- Доверенная загрузка ОС
- Контроль целостности ПО и данных
- Авторизация на уровне BIOS
- Защита на уровне прерываний (SMM)

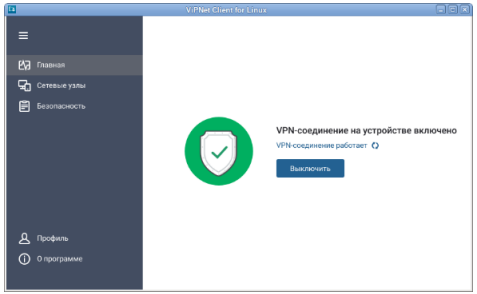




ViPNet Client 4U

Криптоклиент

ИАФ АУД ЗИС



- VPN-соединение с использованием технологии ViPNet по IP адресу/DNS имени или внутреннему идентификатору узла сети ViPNet
- Двухфакторная авторизация
- Прозрачность для приложений пользователя и сервисов ОС
- Поддержка Windows, Linux, MacOS, Android, iOS, Aurora (Sailfish)



ViPNet EndPoint Protection

Средство предотвращения сетевых атак (вторжений) уровня хоста

СОВ | УПД | ИНЦ | АУД

- Обнаружение сетевых атак и атак уровня хоста
- Блокировка сетевых атак с помощью персонального межсетевого экрана
- Собственная обновляемая база сигнатур



В процессе сертификации (ФСЭК России)

ViPNet SafePoint

Средство защиты информации от несанкционированного доступа

ИАФ | УПД | ЗНИ | АУД

ОЦЛ | ОПС





- Идентификация и аутентификация пользователей
- Контроль (разграничение) прав доступа пользователей
- Контроль целостности
- Контроль устройств
- Контроль запуска приложений и замкнутость программной среды

Сценарий 6. Пример комплексного решения

ИАФ

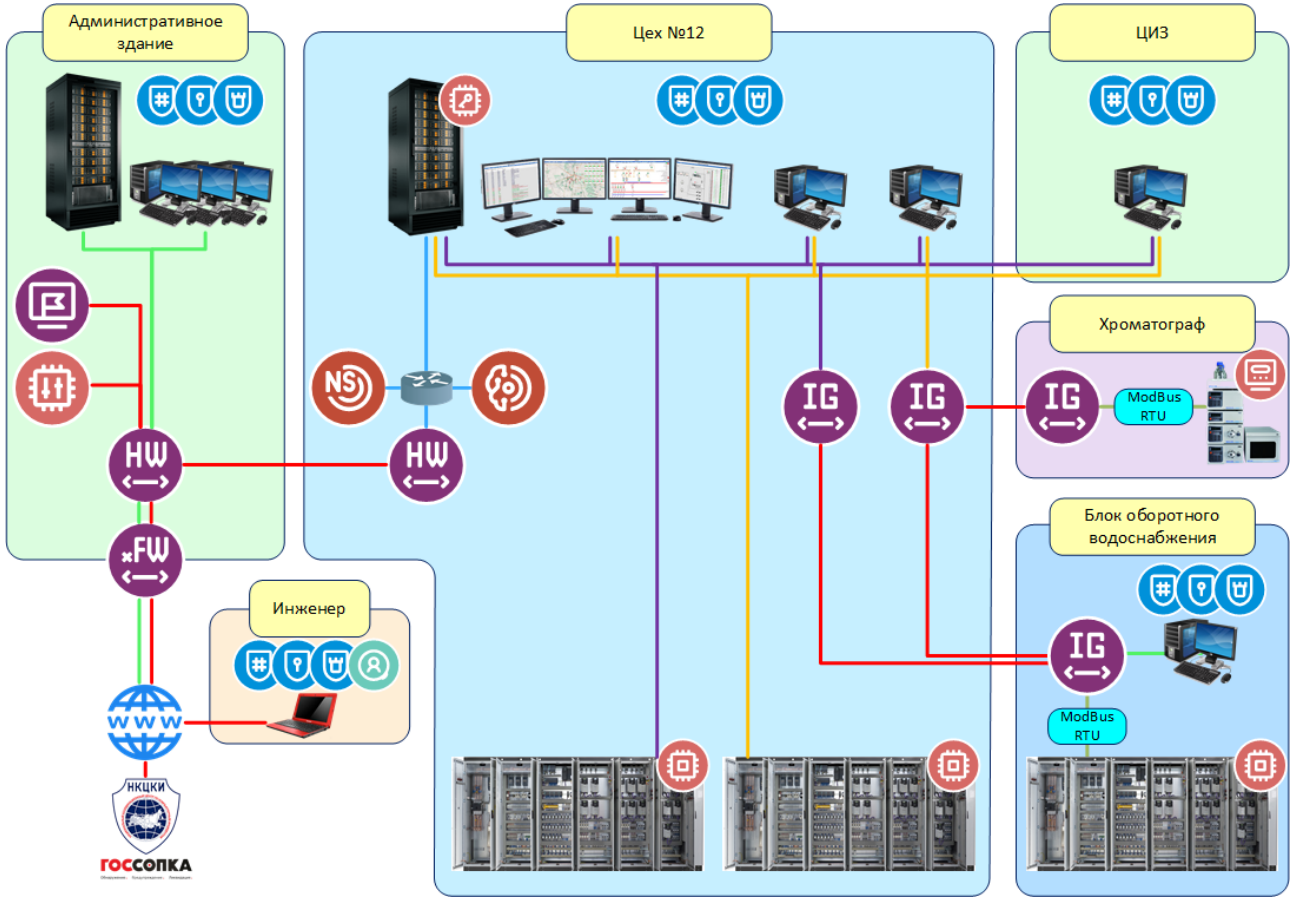
УПД

АУД

ЗИС

ОДТ

СОВ



ЗНИ

ОПС

ОЦЛ

ОПО

ИНЦ

Спасибо за внимание!