

# Как проверить на предприятии наличие IPv4-адресов, уязвимых для удалённых атак?

Инструкция для самостоятельного анализа в базах Shodan и Censys



Эксперты InfoWatch ARMA провели исследование с применением поисковиков Shodan, Censys и Google, чтобы определить количество и типы устройств АСУ ТП, используемых на российских предприятиях, к которым существует потенциальный внешний доступ из интернета. В результате удалось найти более 4 000 подобных устройств. Среди выявленных устройств 2000 — открытое коммутационное оборудование, на 500 не настроена авторизация, а более 700 имеют критические уязвимости. Обнаруженные уязвимости позволяют сделать вывод, что с высокой вероятностью в ходе подготовленной кибератаки они станут источником проникновения и получения контроля над промышленной сетью.

**Проверьте уровень защищённости вашего предприятия, не допустите проникновение злоумышленника в промышленную сеть АСУ ТП. Воспользуйтесь инструкцией для самостоятельной проверки и устранения уязвимостей, которую подготовили эксперты InfoWatch ARMA.**

[Читать исследование](#)

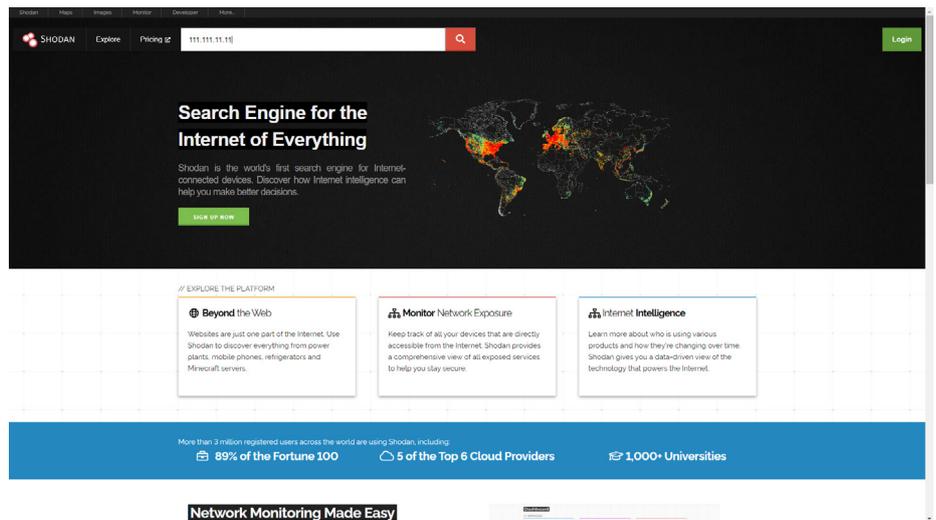
## Для проведения анализа доступных IP-адресов во внешней сети потребуется

- Список всех статических IP-адресов, полученный в ходе инвентаризации или аудита
  - Определить внешние IP-адреса (могут быть внешними). В случае, если внешних IP-адресов не должно быть, рекомендуем проверить все внутренние или пограничные на наличие в поисковых системах
  - Зарегистрированный аккаунт Shodan
  - Подписка для аккаунта Shodan как минимум уровня Freelancer для расширения возможностей API-ключа (опционально)
- Пример**
- **Список открытых IP:** 111.111.11.11, 222.222.22.x
  - **Shodan API-ключ** (на странице [Shodan Account Overview](#)):  
ShOdAnAplKeYsHoDaNaPiKeY

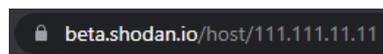
# Shodan

## Поиск одиночных IP-адресов

Вводим запрос в поисковик Shodan: `111.111.11.11`



Возможно ввести IP в URL: `https://beta.shodan.io/host/111.111.11.11`



## Поиск диапазона IP-адресов

Диапазон IP-адресов не обрабатывается стандартным поисковиком Shodan, для этих целей нужен сторонний инструмент (например, [device-pharmer](#)) и приобретённый Shodan API-ключ.

### Пример использования

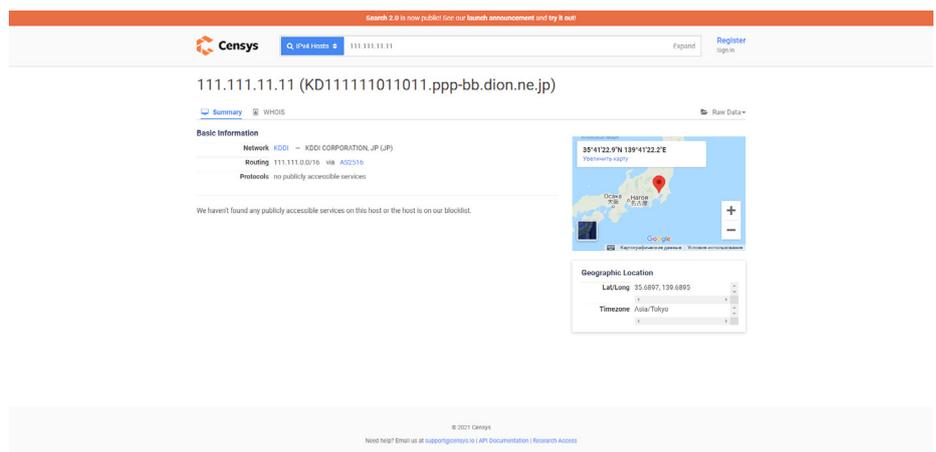
```
python device-pharmer.py -t 222.222.22.1-222.222.22.255 -c 100 -a ShOdAnApIKeYsHoDaNaPiKeY
```

В случае, если диапазон небольшой, все адреса можно проверить ручным вводом и без платной подписки, однако можно столкнуться с ограничениями бесплатного аккаунта (не более 50 результатов по одному запросу, не более 10 расширенных запросов в день).

# Censys

## Поиск одиночных IP-адресов

В URL вводим IP-адрес: `https://censys.io/ipv4/111.111.11.11`





# InfoWatch ARMA



Отечественная система комплексной защиты информации в АСУ ТП на промышленных предприятиях. Система разработана российским вендором решений в сфере информационной безопасности ГК InfoWatch, президентом которой является Наталья Касперская.

InfoWatch ARMA позволяет построить эшелонированную защиту информации в АСУ ТП от современных киберугроз, которые исходят как от внутренних, так и от внешних нарушителей, и выполнить до 90% технических мер ФСТЭК России (Приказ N°239).

Если у вас возникнут дополнительные вопросы, напишите на почту: [anna@team.infowatch.com](mailto:anna@team.infowatch.com)