ИНФОКУБ

CIO CLUB ПЕРМЬ

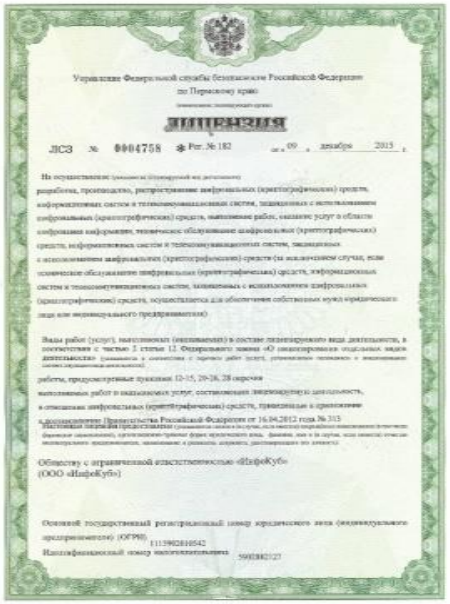
Система мониторинга несанкционированных подключений к корпоративной сети предприятия

конференция

Пермь - 2020

О компании ООО «ИнфоКуб»

Основана в 2011 году, является системным интегратором в области ИБ с полным спектром услуг.



Управление Федеральной службы безопасности Российской Федерации по Пермскому краю

ЛИЦЕНЗИЯ

ЛСЗ № 0004758 Рег.№ 182 от «09» декабря 2015 г.

На осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)

Виды работ (услуг), выполняемых (оказываемых) в составе лицензируемого вида деятельности, в соответствии с частью 2 статьи 12 Федерального закона «О лицензировании отдельных видов деятельности»: выполнение и соответствии с перечнем работ (услуг), составляющих лицензируемый вид деятельности

работы, предусмотренные пунктами 12-15, 20-24, 28 перечня

выполнение работ и оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, приведенные в приложении к постановлению Правительства Российской Федерации от 16.04.2012 года № 313

Настоящая лицензия предоставлена (указывается полное и (в случае, если имеется) сокращенное наименование, в том числе фирменное наименование, организационно-правовая форма юридического лица, фамилия, имя и (в случае, если имеется) отчество индивидуального предпринимателя, наименование и реквизиты документа, подтверждающего его личность)

Обществу с ограниченной ответственностью «ИнфоКуб»
(ООО «ИнфоКуб»)

Основной государственный регистрационный номер юридического лица (индивидуального предпринимателя) (ОГРН) 1115902010542

Идентификационный номер налогоплательщика 5902882127

серия КИ 0277 номер 013807

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер 3167 от 10 февраля 2017 г.

Лицензия предоставлена Обществу с ограниченной ответственностью «ИнфоКуб» (ООО «ИнфоКуб») ОГРН 1115902010542, ИНН 5902882127

Адрес места нахождения: 614068, г. Пермь, ул. Советская, д. 104, офис 503

Адрес места осуществления лицензируемого вида деятельности: 614068, г. Пермь, ул. Советская, д. 104

Перечень работ и услуг, на которые распространяется настоящая лицензия:

контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

установка, монтаж, испытания, ремонт средств защиты информации (программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

Лицензия предоставлена на основании приказа ФСТЭК России от 10 февраля 2017 г. № 84-л

Лицензия действует бессрочно

Заместитель директора

А.Хух

Комплексных проектов	Комплексных поставок	Проведено Аудитов
> 400	> 1800	> 260

Проблема и подходы к ее решению

ПРОБЛЕМА: сотрудники приходят со своими устройствами, будь то ноутбук, планшет, или wi-fi роутер. Это в корне подрывает политику безопасности многих предприятий, а в некоторых случаях нарушает работу сети, либо вовсе позволяет создать уязвимый сегмент для злоумышленников. Все эти манипуляции ведут к потенциальной утечке информации.

На рынке нет полностью готовых и универсальных решений по мониторингу несанкционированных устройств.

С помощью популярных решений мониторинга, таких как, например, zabbix мы упираемся в функциональные возможности системы.

ЗАДАЧА: обнаружить несанкционированно подключаемые устройства в сети предприятия, разделить санкционированные и несанкционированные устройства в сети

РЕШЕНИЕ: разработано собственное программное обеспечение, которое позволяет своевременно уведомлять администратора безопасности сети о случившемся инциденте удобным способом.

Возможности разработанного ПО

ИНФОКУБ

1) автоматическое определение производителя и модели коммутаторов для применения необходимых надстроек;

2) механизмы, позволяющие исключить ошибки в получении данных со шлюзов;

3) доверенная и недоверенная базы подключаемых устройств в сети;

4) наполнение базы устройств в полуавтоматическом режиме (за счет выбора администратором, санкционированное или нет устройство);

5) наполнение базы устройств в автоматическом режиме (за счет "снимка" mac-адресов со всех устройств);

6) просмотр истории обнаружений несанкционированных устройств к коммутаторам (как общей , так и персонально по каждому устройству);

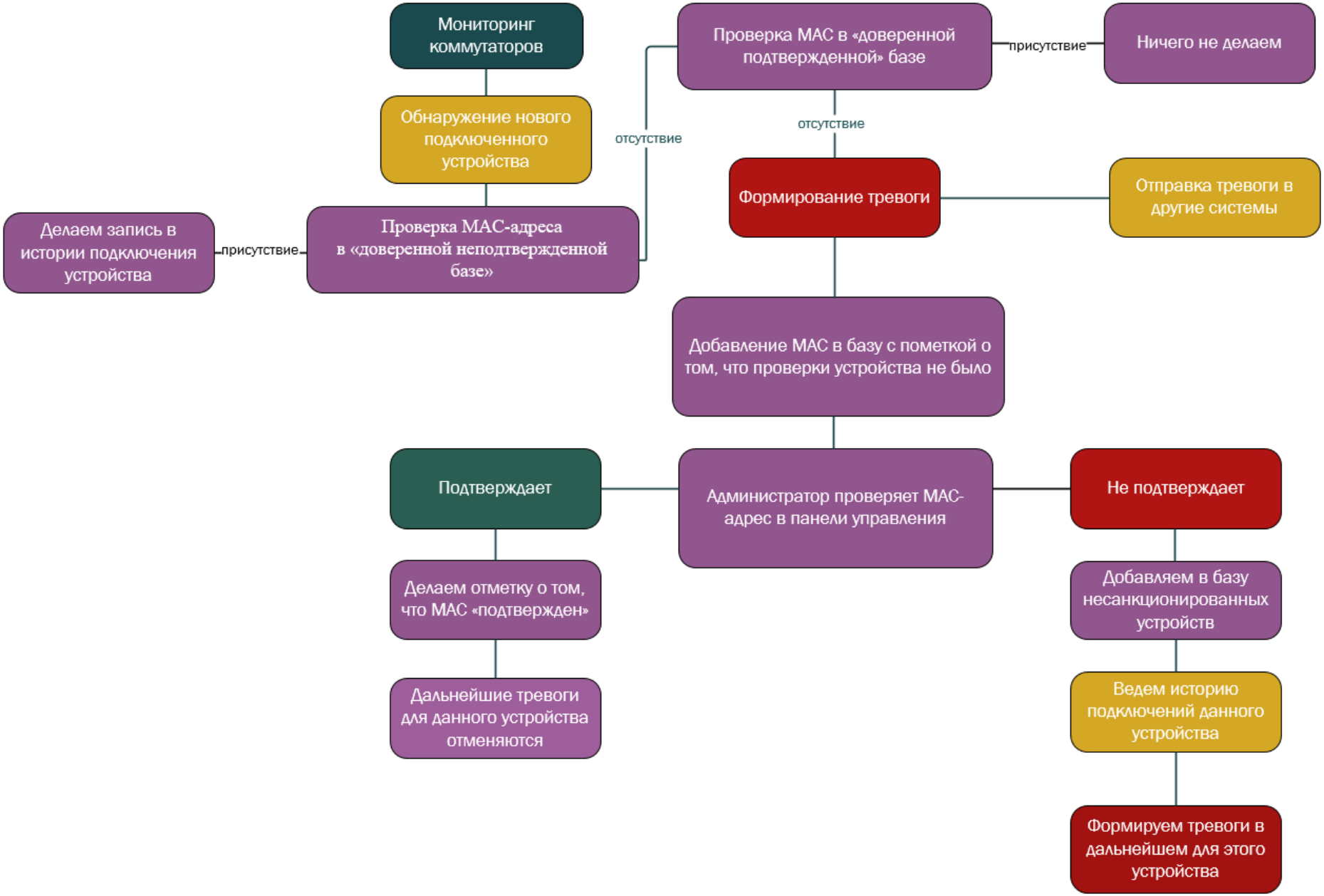
7) вызов триггера об обнаружении несанкционированного устройства в zabbix, либо любую другую систему (доработка по запросу);

8) возможность сделать "примечание" для устройства в списках;

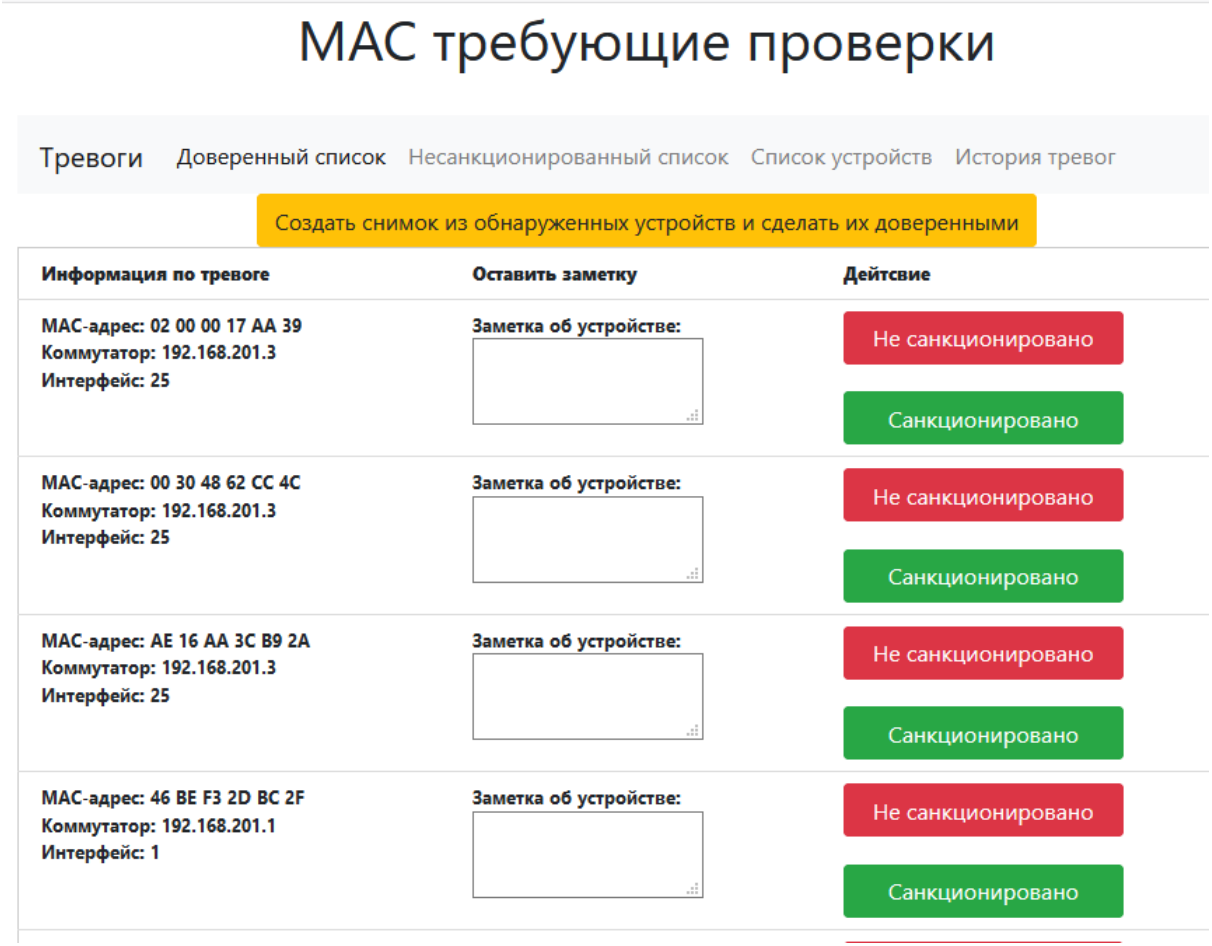
9) управление продуктом осуществляется через веб-панель;

10) полная история обнаружения устройств.

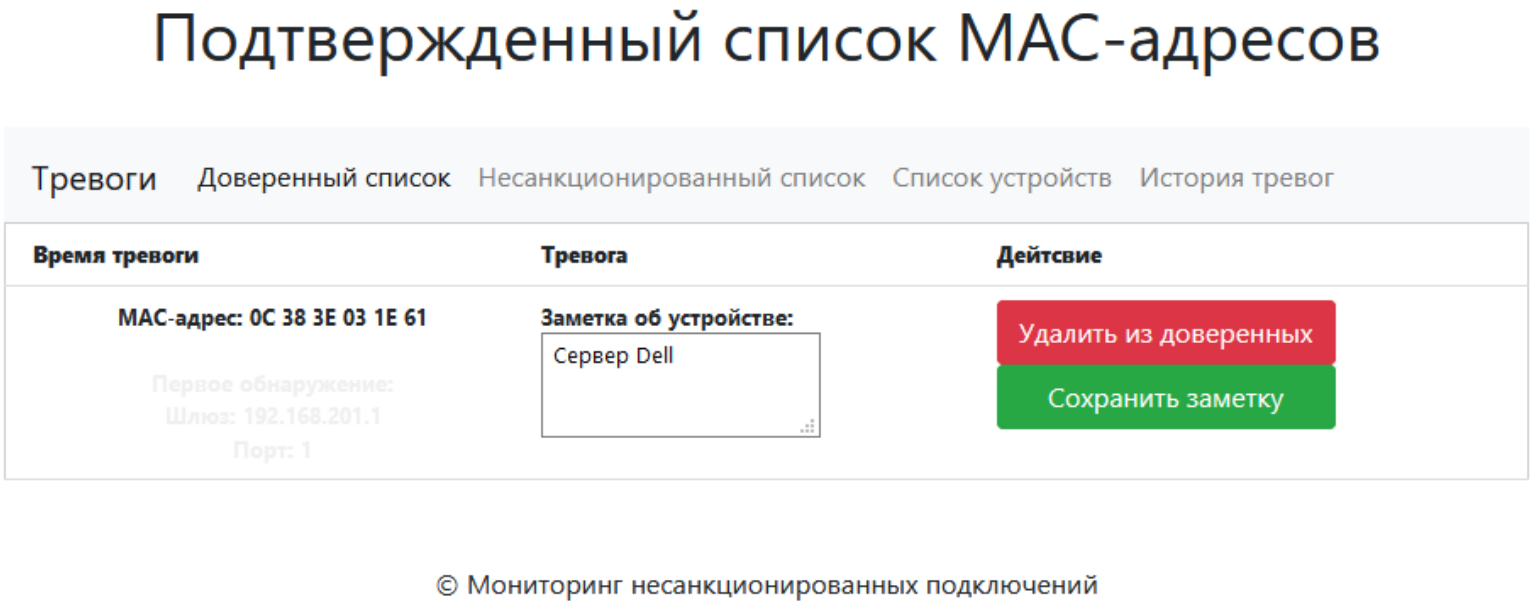
Общий принцип работы



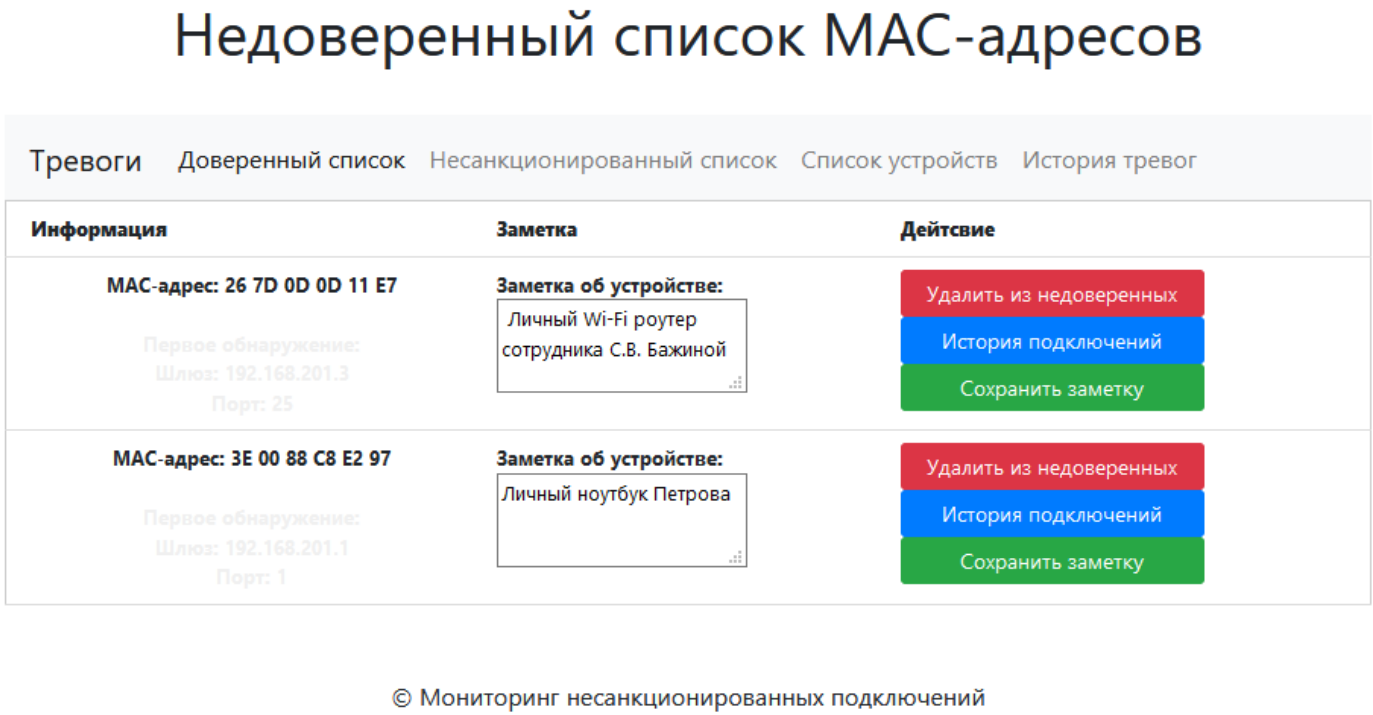
Тревоги – обнаруженные устройства



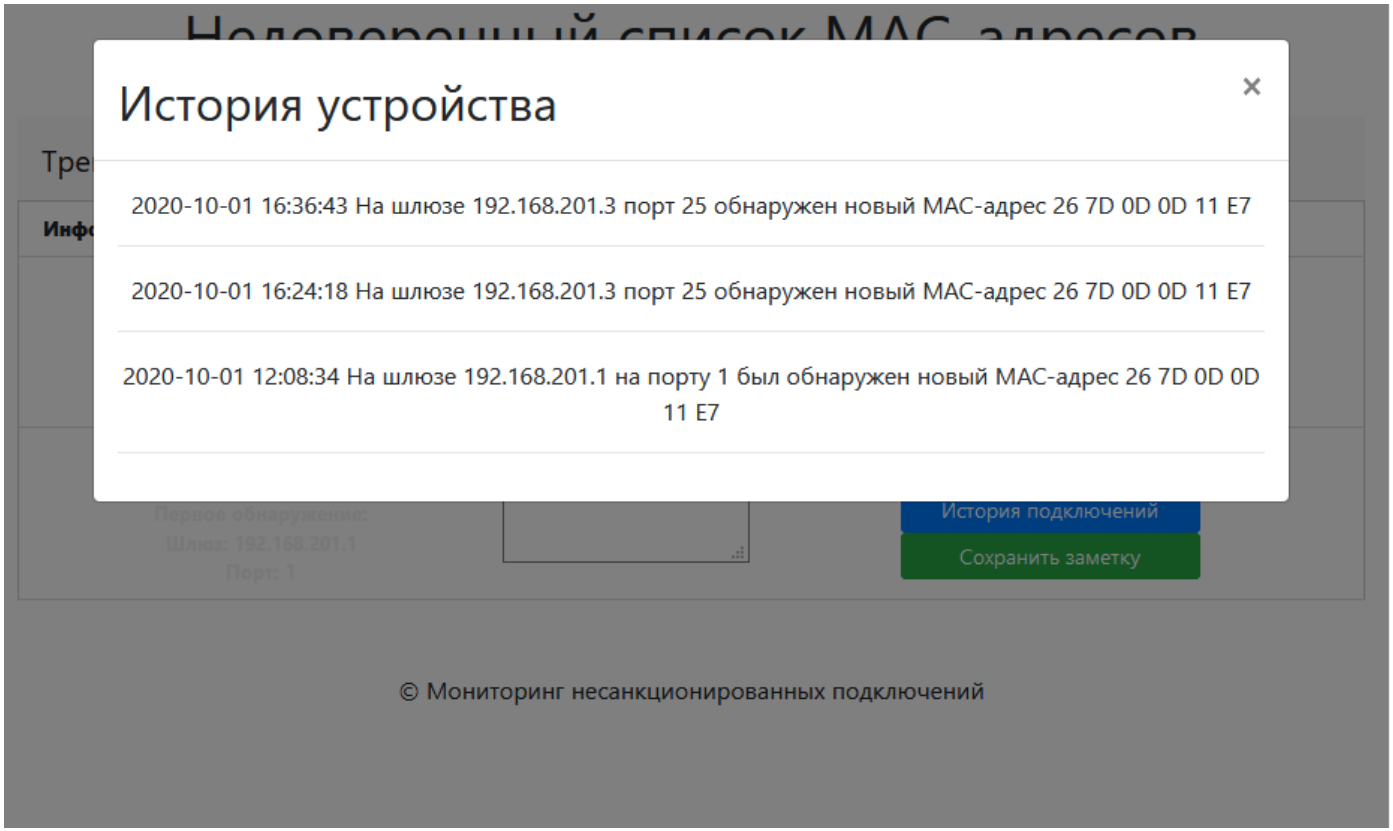
Список доверенных устройств



Список не доверенных устройств



История подключений не доверенных устройств



Список шлюзов под мониторингом

ИНФОКУБ

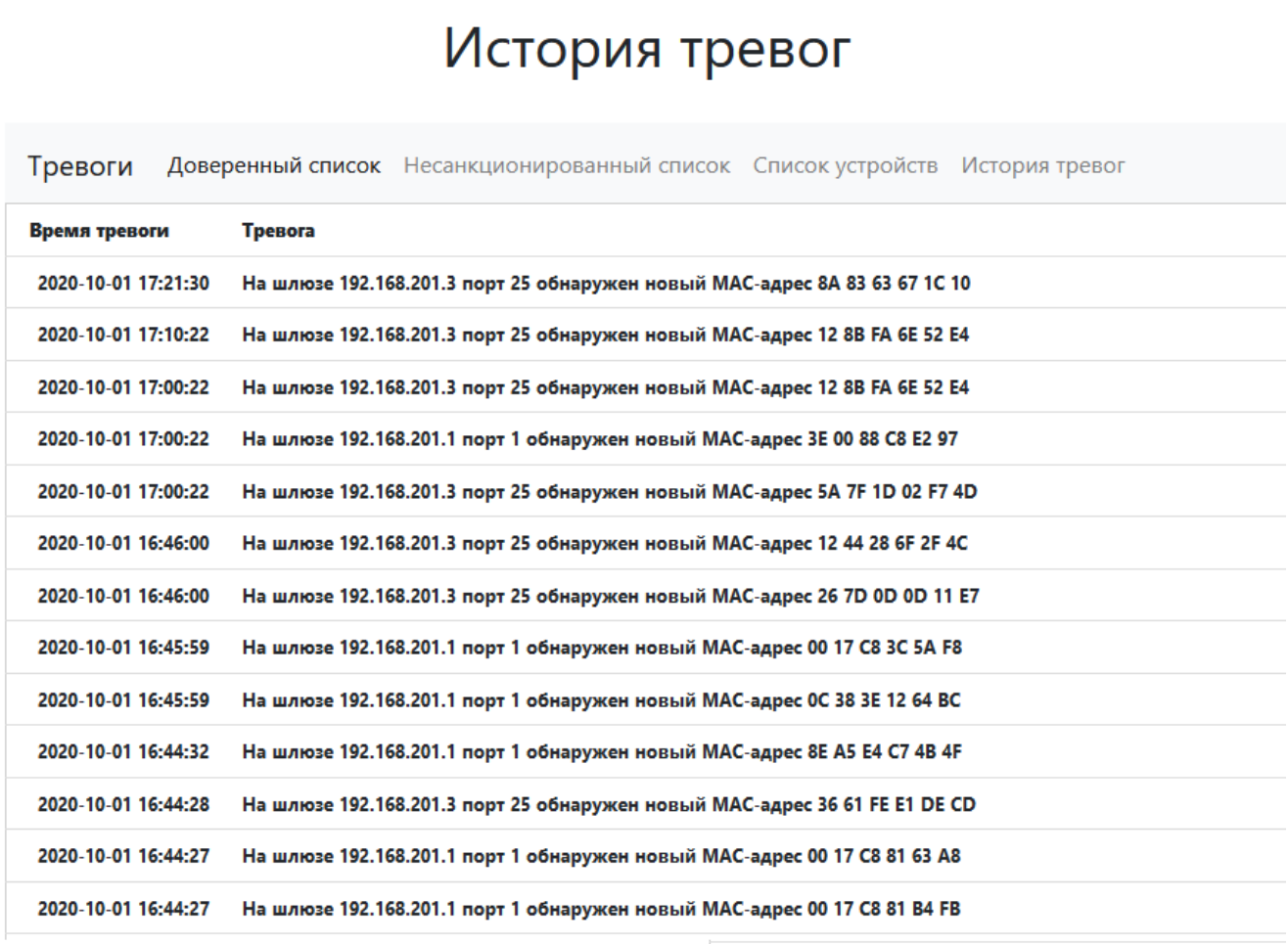
Список IP-адресов отслеживаемых устройств

Тревоги | Доверенный список | Несанкционированный список | Список устройств | История тревог

IP-адреса коммутатора	Информация об устройстве	Последняя проверка (время)
192.168.201.15	S2700-26TP-EI-AC Huawei Versatile Routing Platform Software VRP (R) software,Version 5.70 (S2700 V100R006C05) Copyright (C) 2003-2013 Huawei Technologies Co., Ltd.	2020-10-01 16:59:03
192.168.201.1	RouterOS CCR1009-7G-1C-1S+	2020-10-01 16:59:03
192.168.201.2	RouterOS CRS317-1G-16S+	2020-10-01 16:59:03
192.168.201.3	RouterOS CRS328-24P-4S+	2020-10-01 16:59:03

© Мониторинг несанкционированных подключений

История тревог (общая)



Сроки выхода решения на рынок, стоимость

Сроки выхода решения на рынок:
1 квартал 2021 года
Текущий – этап: тестирование, финальная доработка

Стоимость решения:
Стоимость типового внедрения 500 тысяч рублей (1000 ПК, 50 коммутаторов двух производителей)
Стоимость зависит от количества коммутаторов и однородности их парка
Стоимость технической поддержки, включая обновления очередной год – 25%

ИНФОКУБ

Благодарим за внимание!

ГК "ИнфоКуб"
E-mail: info@infokube.ru
https://www.infokube.ru
Тел. (342) 254-04-44