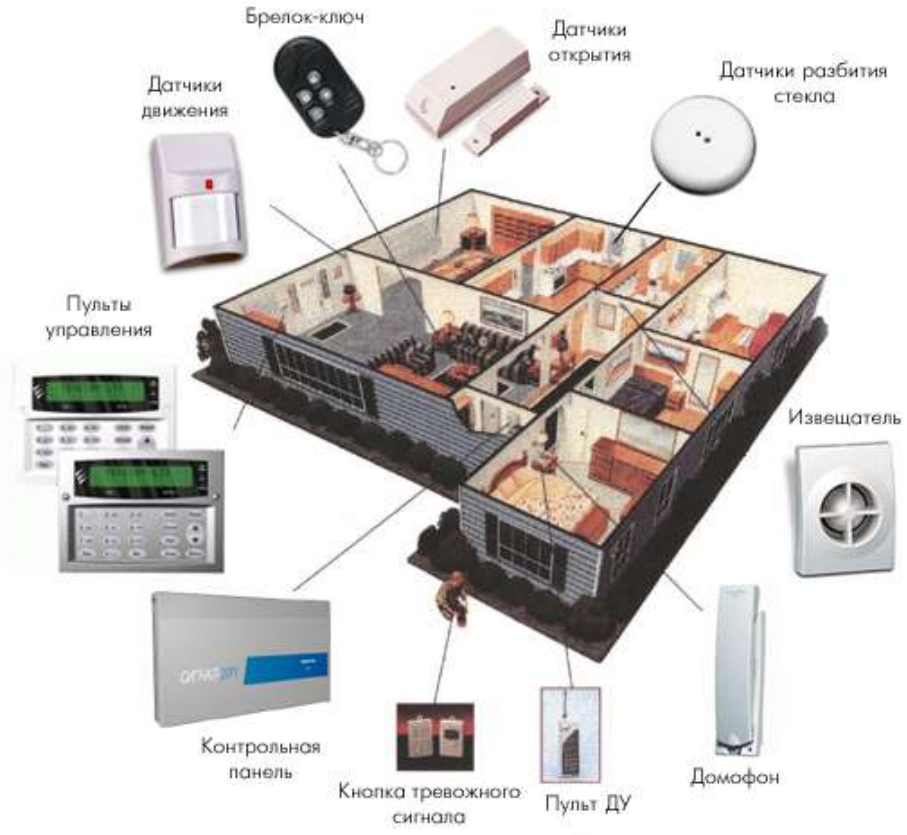
Комплекс защиты систем автоматизации зданий «ЩИТ»

Безопасность систем автоматизации зданий



- Системы **автоматизаций зданий** в настоящее время контролируют почти все аспекты жизнедеятельности человека в помещении, при этом являются абсолютно незащищенными для **компьютерных атак и вирусов**

- 90% систем автоматизации не защищаются, так как ошибочно полагается, что вирусов\компьютерных атак для таких систем не существует

Угрозы безопасности

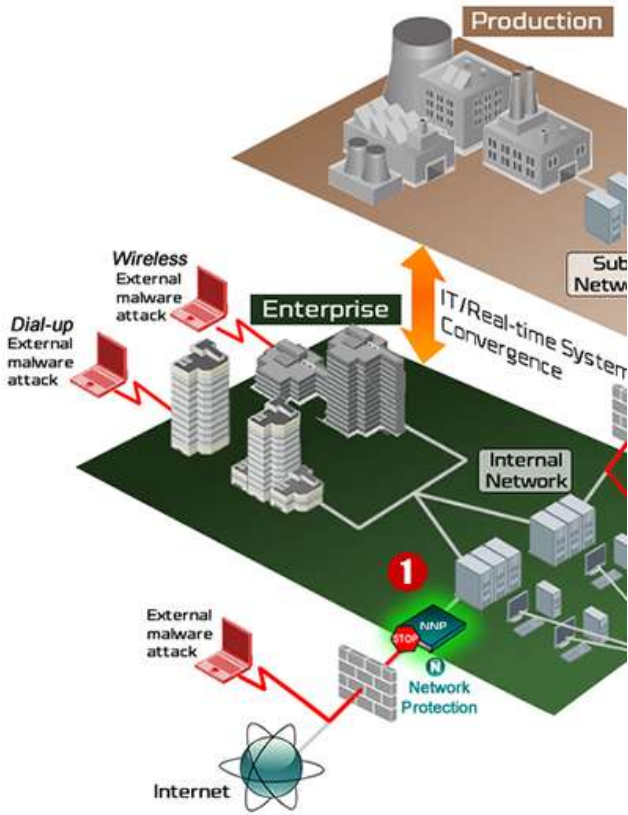
Злоумышленник, подключившись по витой паре к контуру автоматизации здания, может:

- Перехватить **управление над зданием в критической ситуации**
- Вывести систему **управления зданием** из строя
- **Перехватить и скопировать** информацию, циркулирующую по системе управления зданием

Атака на системы автоматизации

- Впервые вирус **stuxnet** остановил ядерную программу Ирана летом 2010 года, поразив систему автоматизации управления атомного объекта

- В офисном\жилом здании вирусы могут привести к отключению или изменению логики работы:
  - системы вентиляции;
  - системы отопления;
  - системы освещения;
  - системы контроля дверей.



Пути попадания вирусов в систему автоматизации зданием

- Проникновение вирус на сервер управления зданием **на флешке\по каналу Интернет** с последующим поражением всей системы

- Проникновение вируса после **подключения злоумышленника** к системе автоматизации в местах, где возможен открытый доступ к витой паре

- **Замена** злоумышленником легального устройства\ контролера в сети автоматизации с целью получения контроля над зданием

Известные здания, оборудованные системой автоматизации в России

- **Офисные и гостиничные здания**
  - Отель **«Балчуг Кемпински»**
  - Отель **«Ритц Карлтон»**
  - **Сберегательный банк** России
- **Торговые комплексы**
  - Торговый комплекс **«Дрим-Хаус»**
  - **Крокус Сити Холл**
- **Общественно значимые здания и сооружения**
  - Аэропорт **Шереметьево-2**
  - Аэропорт **Домодедово**
  - Останкинская телебашня

Реализованный комплекс

Состав комплекса

Линияс истемы управления (витая пара\линия силовой проводки)

Ethernet\USB

сканнер витой пары\силовой проводки

программное обеспечение для Windows\Unix\MacOS

Ethernet\USB

сканнер беспроводных каналов сязи

Сканнер витой пары\силовой проводки

Аппаратное устройство, подключаемое к витой паре\силовой проводке и фиксирующие несанкционированное подключение мошенников к сети

Поддерживаемые протоколы:

- KNX\EIB
- X10

Возможна поддержка:

- LonWorks
- BacNet
- SCADA системы Siemens
- анализ Ethernet траффика

Тех.характеристики:

- Размер 10 x 10 x 15 см
- Разъемы: Ethernet, USB, питание (15 V)

Сканнер витой пары\силовой проводки

Установка:

- Устанавливается в разрыв соединения витой пары или силовой проводки
- Возможна скрытая установка прибора для вывода информации на пульт управления
- Возможна установка прибора в открытом доступе для мониторинга состояния сети на опциональном мониторе непосредственно на устройстве

Сигнализация:

•Сигнализирует о доступе злоумышленника в сеть

•Сканирование сети осуществляется в режиме он-лайн в непрерывном режиме

Сканнер беспроводных частот

Аппаратное устройство, устанавливаемое в помещении и предназначенное для фиксации на заданной площади источников передачи Wi-Fi, Bluetooth-пакетов, GSM-пакетов

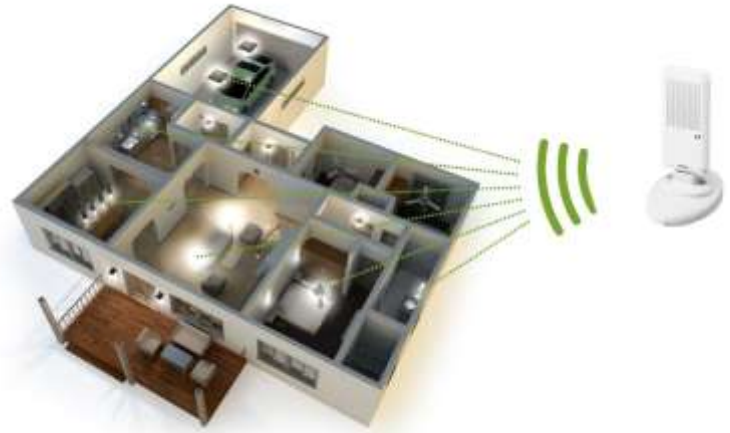
Тех.характеристики:

- Размер 10 x 10 x 15 см
- Разъемы: Ethernet, USB, питание (15 V)
- Автономная работа на батарейке 5 часов

Сканнер беспроводных частот

Режим работы:

- Постоянно сканирование с передачей результатов в режиме он-лайн на единый пульт
- Сканирование в режиме разовой проверки периметра на наличие побочных беспроводных каналов с информированием на опциальном экране



Установка:

•Устанавливается в любой части обследуемого помещения

•Может переноситься из помещения в помещение для разовой проверки

Программное обеспечение для Windows\Unix\MacOS

Программное обеспечение позволяет:

- осуществлять сбор информации и ее анализ;
- указывать время и место подключения злоумышленника к системе;
- подавать тревожный сигнал в случае несанкционированного подключения;
- указывать скрытые несанкционированные каналы передачи данных из периметра автоматизированного здания как по проводным, так и по беспроводным каналам;
- Может работать под ОС Windows\UNIX\MacOS

Установка системы

Устройство контроля беспроводных каналов устанавливается в помещениях, откуда требуется контролировать утечку данных

Для контроля здания достаточна установка одного устройства-сканнер в любом месте здания, где есть доступ к витой паре

Результат работы системы «ЩИТ»

Обнаружение недокументированных устройств

- При несанкционированной активности штатных устройств
- При подключении новых устройств

Защита системы управления

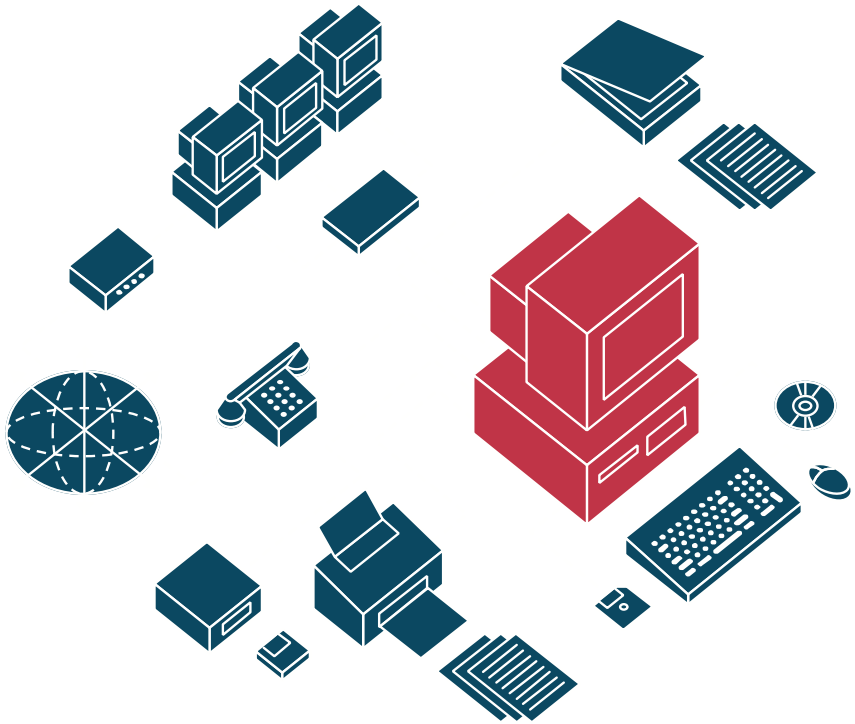
- Защита от деструктивных пакетов
- Защита от запрещенных управляющих команд
- Проверка адресатов и отправителей
- Защита от перегрузок

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

WEB - ПРИЛОЖЕНИЯ

УПРАВЛЕНИЕ ДАННЫМИ УЧЕТА

СЕРВИСНАЯ ПОДДЕРЖКА



Генгринович Евгений Леонидович
Заместитель Генерального директора ЗАО «НПФ «СИМет»
тел. +7 (985) 9288602 E-mail: geleon4@gmail.com