государственное общеобразовательное учреждение Ярославской области
«Лицей № 86»

ЗАЩИТА ЭЛЕМЕНТОВ ИНТЕРНЕТА ВЕЩЕЙ НА ПРИМЕРЕ УМНОГО ГОРОДА

Выполнил
Темников Артём Андреевич
ученик 9 «а» класса
ГОУ ЯО лицей №86
научные руководители:
Петров Антон Игоревич
Петрова Екатерина Олеговна

Ярославль 2023

Содержание

Введение..... 3
1. Теоретическая часть..... 3
1.1. Общие сведения..... 3
1.2. Безопасность объекта..... 4
2. Практическая часть..... 4
2.1. Создание макета объекта «Умный город» под управлением web-сервера через Wi-Fi..... 4
2.2 Моделирование атаки на умную городскую инфраструктуру 6
2.2.1 Атака с помощью программного обеспечения KaliLinux..... 6
2.2.2 Атака с помощью оборудования Wi-Fi jammer..... 7
2.3. Моделирование защиты 8
Заключение..... 9
Список использованных источников..... 10
Приложения..... 11

Введение

Умный город имеет множество проблем в связи с пересечением цифровой и физической инфраструктуры. По мере своего развития, своевременно должна развиваться система защиты информационной системы.

Актуальность. Умная городская среда быстро поглощает жизнь современного человека. Малейший сбой в работе данной системы может привести не только к временным неудобствам, но и к человеческим жертвам. Крупные кибератаки могут возникнуть в любой точке города, но, из-за связи систем умных устройств между собой, масштаб последствий может охватить весь город. Между тем, возможно множество сценариев, приводящих к краже личной информации в частном секторе. К сожалению, развитие систем кибербезопасности для умных городов не успевает за растущим потенциалом IoT-устройств. Как только город становится «умным» из-за взаимосвязанности устройств в нем, шанс катастрофы вырастает в разы.

Новизна: отрасль интернета вещей и умной городской среды, мало изучена, т.к. начала свое развитие с 2000-х гг. Реализованные в проектной работе кибератака и защита являются уникальными.

Цель: выбрать опытным путем метод защиты объектов «Умного города» от атаки деаунтефикации через Wi-Fi.

Задачи:

1. Изучить умной городской среды, в особенности ее актуальных проблем информационной безопасности;
2. Создать макета объекта «Умный город» под управлением web-сервера черезWi-Fi;
3. Собрать макета атаки и защиты на систему «Умный город».

Методы исследования: наблюдение, моделирование, описание, эксперимент, формулирование выводов.

Практическая значимость моей работы в том, что она может быть использована на уроках для передачи полученных знаний одноклассникам, с целью расширения их кругозора в области информатики и кибербезопасности.

1 Теоретическая часть

1.1Общие сведения

Умный город – совокупность, состоящая из интернета вещей и городской инфраструктуры для управления городскими имуществом и сервисами. Преимуществами данной совокупности является:

- Энергоэффективность и экономия используемых ресурсов. Сокращение затрат электроэнергии, водных и отопительных ресурсов, что способствует не только к снижению расходов, но и к улучшению состояния экологии.

- Оптимизация транспортной системы.[1] Минимизация аварий на дорогах, повышение уровня транспортной безопасности, сокращение пробок и опозданий, более экономный расход топлива.

[1] Умный» светофор в России - [Электронный ресурс]/ - Электрон. дан. - Режим доступа: https://trashbox.ru/topics/111337/v-rossii-predstavili-umnyj-svetofor (26.11.2022)

- Повышение уровня безопасности. Снижению техносферных рисков способствует распространение автоматизированных систем. За счет использования и обработки биометрических данных снижается уровень преступности, что способствует улучшению общественной безопасности.

- Повышение комфорта и уровня жизни. Управление процессами внутри дома и на прилежащих территориях с помощью смартфона.

- Упрощение множества процессов. Онлайн-плата коммунальных счетов, сбор информации со счетчиков без вмешательства человека, быстрый поиск парковочного места и многие другие возможности. [2]

Компонентами умного города являются:

- Система ЖКХ и городского управления;
- Инфраструктура сетей и связи;
- Интеллектуальные системы экологической и общественной безопасности;
- Городской транспорт.

1.2 Безопасность объекта

Выявление актуальных угроз производилось на основе анализа принципов работы и устройства различных ИС Умного города и изучения известных угроз из БДУ ФСТЭК и матрицы MITREATT&CK.

Наиболее актуальными угрозами для ИС умного города являются:

- Угрозы, связанные с подключением к сети Интернет;
- Угрозы, связанные с использованием прикладного ПО и его функций;
- Угрозы, связанные с низкоуровневым ПО;
- Угрозы, связанные с использованием облачных услугу;
- Угрозы, связанные с использованием вредоносного ПО;
- Угрозы, связанные с использованием идентификационной информации;
- Угрозы, связанные с использованием ОС, ее встроенных средств и утилит;
- Угрозы, связанные с человеческим фактором;
- Угрозы, связанные с физическим воздействием.

Далее был проведен более детальный анализ угроз из нового раздела БДУ ФСТЭК.[3]

В Приложении 1 приведена таблица с распространенными объектами интернета вещей и их актуальными угрозами в г. Москва по новому разделу БДУ ФСТЭК.

2 Практическая часть

2.1. Создание макета объекта «Умный город» под управлением web-сервера через Wi-Fi

Проект построен на базе аппаратной платформы NodeMCU. Язык программирования C++. ПО разработано собственными силами. Необходимое

---

[2] Климович, А.Н. Алгоритм управления перекрестком на основе V2I взаимодействия // Системный анализ прикладная информатика. – 2018. – № 4. – С. 21.

[3] Банк данных угроз информационной безопасности ФСТЭК - [Электронный ресурс]/ - Электрон. дан. - Режим доступа: https://bdu.fstec.ru/threat

оборудование: 1 микроконтроллер NodeMCU esp8266; 4 красных светодиода; 4 желтых светодиода; 4 зелёных светодиода; 2 сверхъярких светодиода; 14 резисторов на 220 ОМ; макетная плата; провод micro USB; провода.

Собираем по схеме (рис.1):

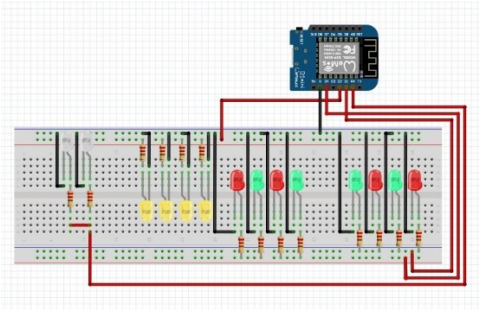


Рисунок 1 - Схема объекта «Умный город» на базе аппаратной платформы NODEMCU.

Макет объекта в собранном виде представлен на рисунке 2.

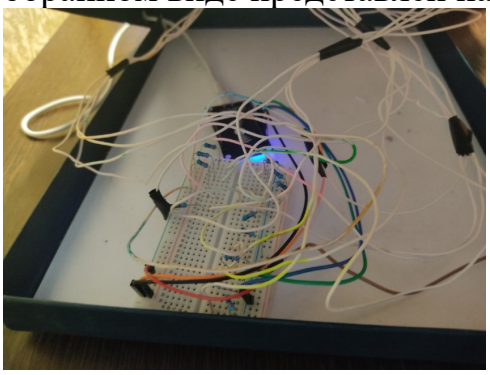


Рисунок 2 - Макет в собранном виде.

Настройка работы объекта «Умный город» представлена в приложении 2:

1.Загрузка кода на плату NodeMCU esp8266;

2.После открытия монитора порта нажать кнопку EN/RST;

3. Подключиться к Wi-Fi сети, указанной в программном коде.

4.Открыть браузер и ввести IP-адрес web-станицы, указанный в мониторе порта. Откроется стартовая страница;

5.Нажать кнопку на странице, загорятся нужные сигналы светофора и включение умного освещения.

Соберем модель макета (рис. 3).



Рисунок 3 - Готовая модель под управлением web-сервера черезWi-Fi.

Алгоритм работы умного города представлен в Приложении 3.

Таким образом, собран макет объекта умной городской инфраструктуры, который включает в себя объекты «Умный город» и «Умное освещение» на базе аппаратной платформы NODEMCU, отвечающий заданным параметрам. [4]

2.2. Моделирование атаки на умную городскую инфраструктуру

При неконтролируемом манипулировании системами объектов «Умный город» возникает прямая опасность жизни людей (провоцирование ДТП), экономическая (задержки в пути, расход бензина), экологическая (выхлопы). В качестве примера возможной выбрали атаку деаутефикации Wi-Fi. Она отправляет пакеты для разъединения одному или более клиентам, подключенным в данный момент к конкретной точке доступа. Злоумышленник лишает законного пользователя доступа к беспроводной сети или делает сеть недоступной, вызывая ее сбой, что в дальнейшем может привести к атаке «злой двойник», тем самым заставив пользователя подключиться к поддельной точке доступа, которую поднял злоумышленник, или захвату хендшейка с последующим подключением к этой точке доступа. Беспроводные сети чрезвычайно восприимчивы к DoS-атакам, локализовать злоумышленника в распределенной беспроводной сети сложно.[5]

Для примера атаки деаутефикацииWi-Fiвыбрали два способа:

1.С помощью программного обеспечения KaliLinux;

2.С помощью оборудования Wi-Fi jammer.

Все кибератаки производятся в исследовательских целях!

2.2.1 Атака с помощью программного обеспечения KaliLinux

KaliLinux — дистрибутив Linux на основе Debian с открытым исходным кодом, предназначенный для решения задач информационной безопасности: тестирование на проникновение, исследование безопасности, компьютерная криминалистика и обратный инжиниринг.

Для подключения атаки:

1. Запустить операционную систему KaliLinux и подключить адаптер (Tp-linktl-wn722n).
2. Переход в терминал, где пишется команда: sudosu.
3. Команда: ifconfig, чтобы узнать какие Wi-Fi- адаптеры у нас есть.
4. Ввод команды: airmon-ngcheckkill, «убить» лишние службы и сервисы, которые могут помешать реализовать атаку.
5. Ввод: airmon-ngstartwlan0, перевести адаптер в режим монитора.
6. Ввод: airmon-ngwlan0, чтобы сканировать все ближайшие точки доступа.
7. Ввод: airodump-ng -bssid указываем mac - адрес сети, которую собираемся атаковать с номер канала wlan0, чтобы сканировать определенную точку доступа;
8. Открываем новую вкладку, одновременным нажатием клавиш CTRL+Shift+T;

---

[4] Принцип действия «умного» светофора - [Электронный ресурс]/ - Электрон. дан. - Режим доступа: http://www.bolshoyvopros.ru/questions/679414-kak-dejstvuet-umnyj-svetofor.html (30.01.2023)

[5] Умный светофор - [Электронный ресурс]/ - Электрон. дан. - Режим доступа:Arduino технологии: https://arduino-tech.ru/2018/12/29/umnyj-svetofor/ (30.11.2022)

9. В новой вкладке ввод команды: sudosu, чтобы снова перейти в режим root прав;

10. Ввод команды: aireplay-ng --deauth 0 -amac-адрес сети wlan0, чтобы начать атакудеаутефикации.

11. Для окончания атаки вводим команду нажатием клавиш CTRL+C.

Фотографии кода атаки деаунтефикации в KaliLinux представлены приложении 4.

Таким образом, с помощью программного обеспечения KaliLinux реализована атака деаутефикации на Умный город.

2.2.2 Атака с помощью оборудования Wi-Fi jammer

Wi-Fi jammer- устройство, предназначенное для отключения беспроводных устройств от точки доступа. Ниже представлен самостоятельно собранный Wifi jammert (рисунок 4):



Рисунок 4 - Wi-Fi jammer.

Для начала атаки при помощи Wi-Fi jammer необходимо (рисунок 5):

1.Включить Wi-Fijammer. Появится точка доступа под названием - pwned.

2.Подключаемся к ней в любом браузере, вписываемIP-адрес web-страницы: 192.168.4.1.

3.Выбираем нашу Wi-Fi сеть и переходим в режим Attaks.

4.Напротив Deauth нажимаем start, атака началась.

5.Для остановки атаки нажимаем stop.

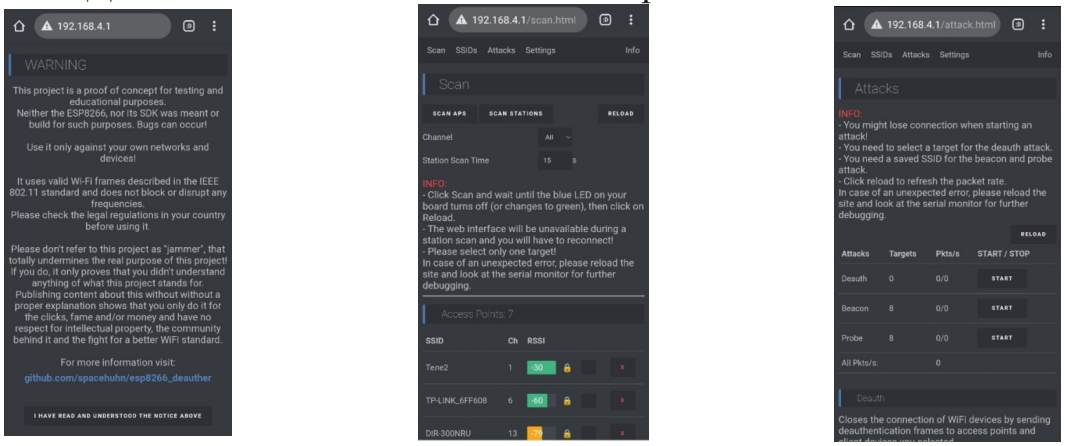


Рисунок 5 - Экраны проведения атаки деаутефикации с помощью Wi-Fi jammer.

С помощью оборудования Wi-Fi jammer была реализована атака деаутефикации.

2.3. Моделирование защиты

Основные методы защиты объектов «Умный город» представлены в приложении 5. Подбор средств нейтрализации угроз для защиты системы представлен в приложении 6.

Все вышеперечисленные средства защиты имеют лицензирование и сертифицированы ФСТЭК, а также являются продуктами российского производства, что способствует развитию системы ИБ в период импортозамещения

В данной работе представлено обнаружение атаки деаутентификации.

Атака деаутентификации—проблема со стандартом 802.11i. Кадры деаутентификации, как и все другие кадры управления 802.11, не шифруются.Поэтому любой может создать кадры деаутентификации или любой другой фрейм управления. При обнаружениииатакииспользуется сканирование всех доступных точек доступа и выявление в них фреймов деаутефикации. Если число таких фреймов в одной точке доступа в одно время превышает пять, загорается светодиод, возникает звуковой сигнал и данные об атаках сохраняются на карте памяти (рис.6 -7).

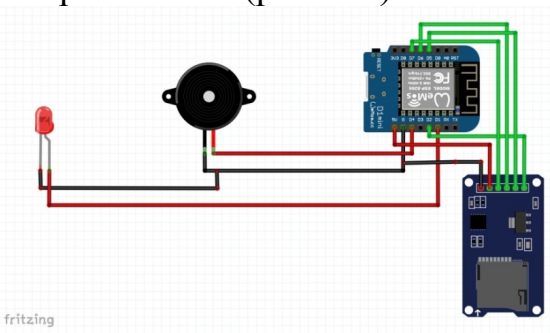


Рисунок 6 - Схема детектора.

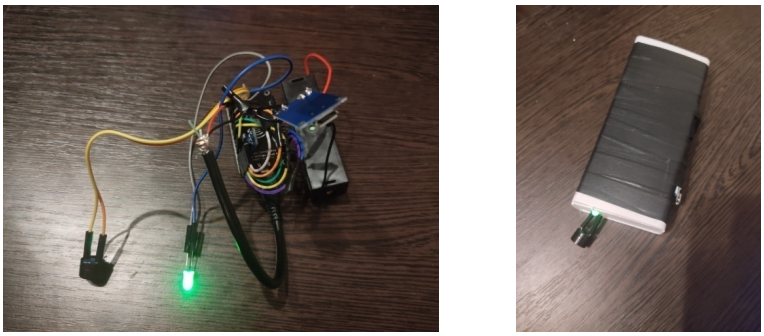


Рисунок 7 - Самостоятельно собранный детектор.

Ссылка на видео-подтверждение работающего макета объекта «Умный город» и проведение испытания детектора Wi-Fi атак, а также их программные коды: https://disk.yandex.ru/d/ZR3ct2YJ7hG0pg

С помощью данного оборудования можно обнаружить атаки деаутефикации по Wi-Fi. Кибератаки в настоящее время актуальные и популярные. Разработаннаясистема защиты может применяться не только для

защиты умного города, но и для защиты многих сфер общества, где используется сеть WI-FI.

Заключение

В результате работы над данным проектом:

- собран макет умной городской среды, состоящий из объектов «умное освещение» и «умный светофор»;
- проведена атака с помощью программного обеспечения KaliLinux;
- совершена атака с использованием оборудования Wi-Fi jammer;
- произведено моделирование защиты на систему умной городской инфраструктуры.

Кибератаки в настоящее время актуальные и популярные. Разработанная система защиты может применяться не только для защиты умного города, но и для защиты многих сфер общества, где используется сеть WI-FI.

Поставленные цель и задачи выполнены.

Перспективы развития:

Повышение функциональности программного обеспечения для внедрения его в различные объекты «Умного города», которое включает в себя инновационные функции, улучшение производительности, расширенные возможности управления и множество других удобных опций, которые позволят увеличить безопасность и надежность его работы.

Список использованных источников:

1. Климович, А.Н. Алгоритм управления перекрестком на основе V2I взаимодействия // Системный анализ и прикладная информатика. – 2018. – № 4. – С. 21–27.

2. Банк данных угроз информационной безопасности ФСТЭК - [Электронный ресурс]/ - Электрон. дан. - Режим доступа: https://bdu.fstec.ru/threat (12.01.2023)

3. Принцип действия «умного» светофора - [Электронный ресурс]/ - Электрон. дан. - Режим доступа: http://www.bolshoyvopros.ru/questions/679414-kak-dejstvuet-umnyj-svetofor.html (30.01.2023)

4. «Умный» светофор в России - [Электронный ресурс]/ - Электрон. дан. - Режим доступа: https://trashbox.ru/topics/111337/v-rossii-predstavili-umnyj-svetofor (26.11.2022)

5. Умный светофор - [Электронный ресурс]/ - Электрон. дан. - Режим доступа:Arduino технологии: https://arduino-tech.ru/2018/12/29/umnyj-svetofor/ (30.11.2022)

ПРИЛОЖЕНИЕ 1

Анализ на примере объектов IoT по новому разделу БДУ ФСТЭК

Объект IoT	**Угрозы**	**Способы реализации**	**Последствия**	**Способы предотвращения**
Умный светофор	УБИ.1 УБИ.2 УБИ.3 УБИ.4 УБИ.5 УБИ.6 УБИ.7 УБИ.8 УБИ.9 УБИ.11	СП.1 СП.2 СП.3 СП.4 СП.5 СП.6 СП.7 СП.9 СП.10 СП.13 СП.15 СП.16 СП.18 СП.19 СП.21 СП.23 СП.24	– Нарушение целостности, конфиденциальности и доступности данных; – Выход оборудования из строя; – Остановка работы системы; – Автокатастрофы и человеческие жертвы.	– Использование рекомендуемых СЗИ; – Выполнение требований приказов и постановлений ФСТЭК и правительства РФ; – Наличие специалистов в организации, которые будут отсматривать аномальную активность на умных устройствах и предотвращать атаки на них.
Умное городское освещение	УБИ.1 УБИ.2 УБИ.3 УБИ.4 УБИ.5 УБИ.6 УБИ.7 УБИ.8 УБИ.9 УБИ.11	СП.1 СП.2 СП.3 СП.4 СП.5 СП.6 СП.7 СП.9 СП.10 СП.13 СП.15 СП.16 СП.18 СП.19 СП.21 СП.23 СП.24	– Нарушение целостности, конфиденциальности и доступности данных; – Выход оборудования из строя; – Остановка работы системы; – Финансовый ущерб; – Нарушение штатного режима функционирования автоматизирован системы управления и управляемого объекта и процесса; – Автокатастрофы, кражи и человеческие жертвы (угроза жизни и здоровью).	

ПРИЛОЖЕНИЕ 2

Скриншоты интерфейса умного города



Скриншот монитора порта.



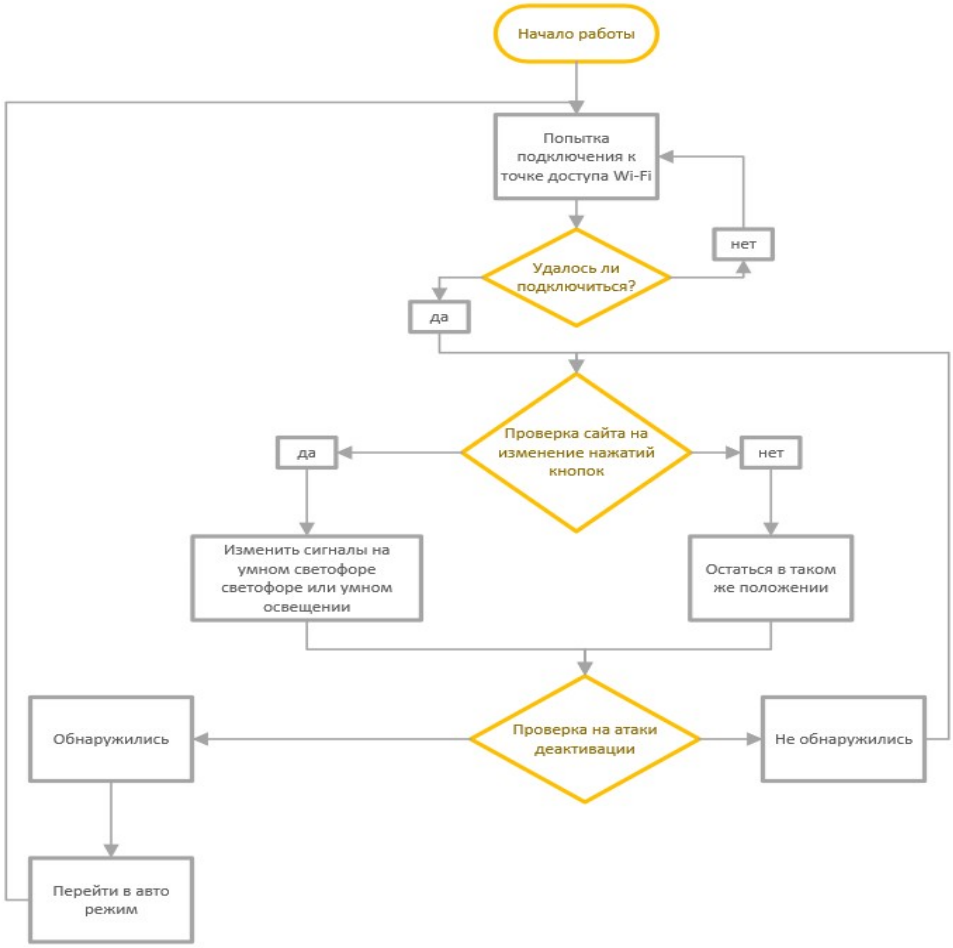
Экран интерфейса управления «Умным городом».



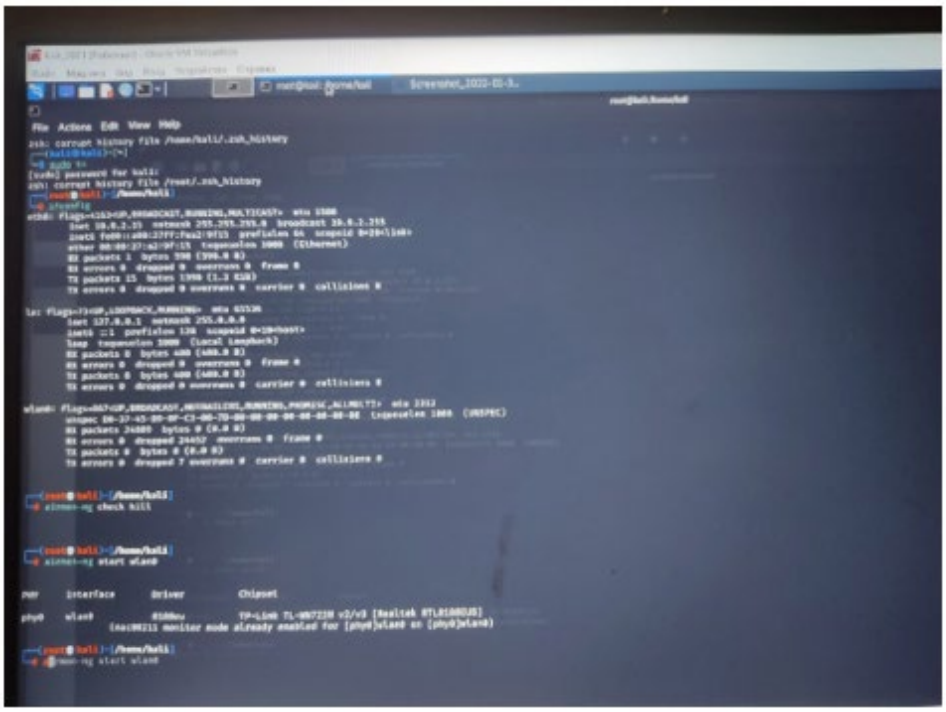
Экран интерфейса управления «Умным городом».

ПРИЛОЖЕНИЕ 3

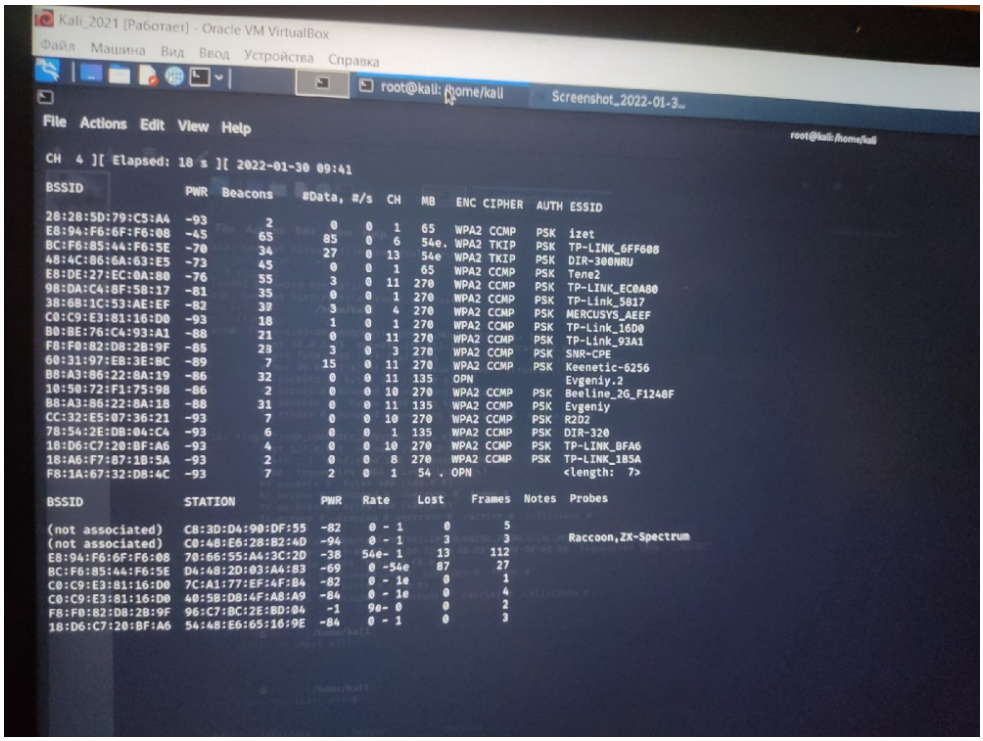
Алгоритм работы умного города



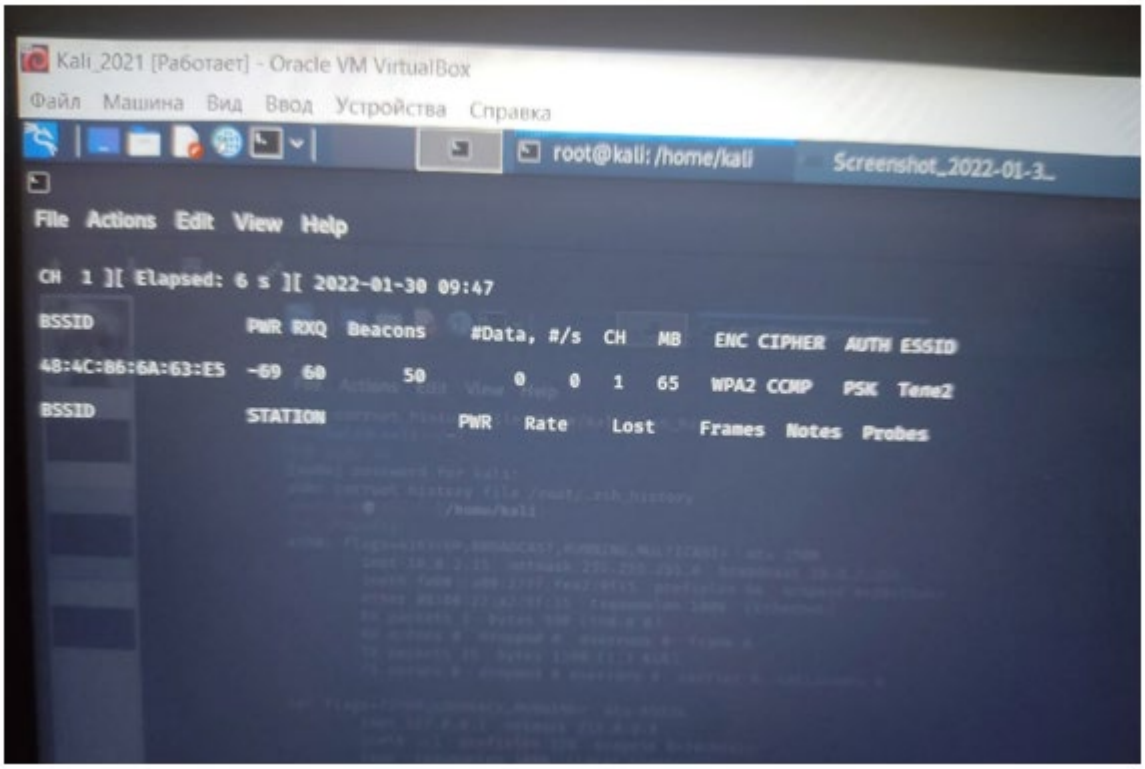
Фотографии кода атаки деаунтефикации в KaliLinux



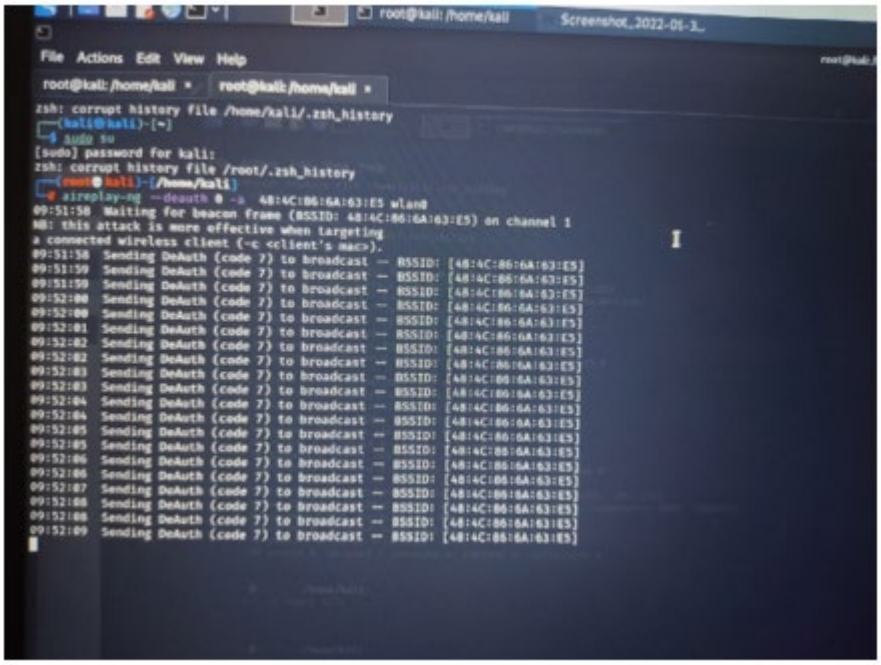
Экран терминала атаки-деаутефикацииWi-Fi.



Экран сканирования доступных Wi-Fi сетей.



Экран сканирования определенной точки доступаWi-Fi сети.



Экран атаки на точку доступа Wi-Fi сети.

ПРИЛОЖЕНИЕ 5

Основные методы защиты объектов «Умный город»

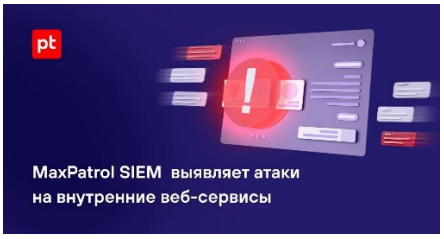
Метод	Суть метода
Проведение тестов на проникновение.	Тщательно проверить систему на предмет взлома —легальные хакеры проведут поиск уязвимостей и дадут советы по устранению.
Своевременное обновление ПО	Регулярное обновление прошивок закрывает известные уязвимости и значительно повышает безопасность инфраструктуры
Регулярное обновление парка оборудования	Элементы интернета вещей имеют больший жизненный цикл, но нуждаются в замене.
Придание высшего приоритета сохранению приватности.	Пересылаемые в рамках «умного» города данные максимально обезличены. Доступ к конфиденциальным данным строго ограничен
Шифрование и сложная аутентификация	По возможности весь трафик «умного» города зашифрован. Каждый сеанс доступа к оборудованию защищать токеном или сессионным ключом. Доступ к сервисам защитить факторами аутентификации: биометрия, разовые пароли, двухфакторная авторизация
Наличие «ручного управления»	Возможность прямого ручного управления на случай сбоя автоматики
Обеспечение отказоустойчивости	резервирование и дублирование серверов и сетей

ПРИЛОЖЕНИЕ 6

Подбор средств нейтрализации угроз для защиты системы



Антивирусное ПО **«KasperskyEndpointSecurity»**, обеспечивает высокий уровень защиты, взаимодействует с большой и регулярно обновляемой базой угроз



Система мониторинга событий информационной безопасности **«MaxPatrolSIEM»**. Используется для контроля защищенности и соответствия стандартам ИБ



ПК **«Acronis Защита Данных»** – ПО для резервного копирования данных необходимых для обеспечения работы ИС. Также необходимо хранение биометрических и прочих персональных данных граждан



СЗИ **«SecretNetStudio»** – многофункциональное средство защиты от несанкционированного доступа, имеет встроенный межсетевой экран. Имеет единую консоль управления, которая упрощает администрирование СЗИ, интегрированность защитных механизмов между собой.