УДК 004.056
DOI: 10.25559/SITITO.14.201804.938-946

АНАЛИЗ ЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ КЛИЕНТОВ

Е.А. Баранова, С.В. Зарешин
Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия

ANALYSIS OF WIRELESS CLIENTS' SECURITY

Elena A. Baranova, Sergey V. Zareshin
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia

Ключевые слова

Беспроводные сети; Wi-Fi; уязвимость; точка доступа; аутентификация; безопасность.

Аннотация

На сегодняшний день каждый из нас пользуется возможностями беспроводной связи. Практически в любой точке города можно найти точку доступа и получить доступ в сеть Интернет. Зачастую люди пользуются открытыми точками доступа в транспорте, парках, торговых центрах или кафе. Но в таких случаях клиенты беспроводной сети особенно рискуют быть атакованными злоумышленниками и потерять личные данные.

В данной статье рассматривается вопрос безопасности беспроводных клиентов, а также наличие уязвимости беспроводных сетей Wi-Fi. Эта уязвимость может быть использована в следствие появления новых возможностей библиотеки для захвата сетевого трафика libpcap. Данная библиотека позволяет не только перехватывать трафик беспроводных сетей, но и отправлять пакеты в сеть, используя драйвер сетевой карты.

В статье описывается метод усиления сигнала точек доступа, а также отключения беспроводных клиентов от сети и дальнейшего переподключения их к посторонним точкам доступа. Данное исследование иллюстрирует возможную схему действия злоумышленника и ситуацию атаки на клиента. Результатом исследования является ответ на вопрос, является ли возможность отправки пакетов в сеть программным способом потенциальной угрозой для клиентов. Обрабатывается информация, полученная в результате исследования и сбора данных. Статья также содержит статистику успешного усиления силы сигнала точки доступа и статистику успешного переподключения клиентов к точке доступа со слабой силой сигнала, которая была увеличена злоумышленником программным способом. Статистика приведена для клиентов с различными версиями ОС Android в зависимости от характеристик программного обеспечения, которое может использовать потенциальный злоумышленник для осуществления атаки такого типа.

Об авторах:

Баранова Елена Алексеевна, магистрант, кафедра информационных систем и технологий, Национальный исследовательский ядерный университет «МИФИ» (115409, Россия, г. Москва, Каширское шоссе, д. 31), ORCID: http://orcid.org/0000-0002-4439-297X, baranovaeaa@yandex.ru

Зарешин Сергей Владимирович, магистр, ассистент, Институт интеллектуальных кибернетических систем, Национальный исследовательский ядерный университет «МИФИ» (115409, Россия, г. Москва, Каширское шоссе, д. 31), ORCID: http://orcid.org/0000-0002-4183-1535, svzareshin@gmail.com

Keywords

Wireless networks; Wi-Fi; weakness; access point; authentication; security.

Abstract

For today, each of us is using wireless communication capabilities. Almost anywhere in cities such as Moscow you can find an access point and access to the Internet. Often people use open access points in transport, parks, shopping centers or cafes. But in such cases, wireless network clients are particularly at risk of being attacked by intruders and losing personal data. This article discusses the security of wireless clients, as well as the vulnerability of wireless Wi-Fi networks. This vulnerability can be exploited as a result of the new library features for capturing network traffic named as libpcap. This library allows not only to intercept the traffic of wireless networks, but also to send packets to the network using the network card driver.
The article describes the method of amplifying the signal of access points, as well as disconnecting wireless clients from the network and further reconnecting them to unauthorized access points. This study illustrates the possible scheme of the attacker's actions and the situation of the attack on the client. The result of the study is the answer to the question whether the ability to send packets to the network programmatically is a potential threat to customers. The information obtained as a result of research and data collection is processed. The article also contains statistics on the successful amplification of the signal strength of the access point and the statistics of successful reconnection of clients to an access point with a weak signal strength, which was increased by the attacker programmatically. The statistics are for customers with different versions of the Android OS, depending on the characteristics of the software that a potential attacker may use to perform this type of attack.

Введение

Мы живем в век бурного развития информационных технологий. На сегодняшний день люди практически всю необходимую им информацию хранят в электронном виде, используя различную цифровую технику и носители информации. Это могут быть личные данные, фотографии, книги, банковские карты, счета и многое другое. Чтобы иметь возможность пользоваться информацией в любое время, необходимы технологии, позволяющие производить обмен информацией необходимого объема с необходимой скоростью передачи данных.

Для обеспечения передачи данных существует множество интерфейсов. На сегодняшний день наиболее часто используемым является беспроводной интерфейс передачи данных. Подавляющее большинство мобильных устройств и персональных компьютеров поддерживают возможность приёма и передачи данных с помощью интерфейса IEEE 802.11, также известного как группа стандартов для сетей Wi-Fi [1]. Стандарт относится к категории WLAN (Wireless Local Area Network). Именно широкое распространение данного интерфейса является основной причиной для анализа реализации стандарта на предмет возможных уязвимостей.

Для обеспечения конфиденциальности при использовании Wi-Fi существуют механизмы защиты передачи данных по радиоканалу, такие как WEP-шифрование (Wired Equivalent Privacy) или WPA/WPA2-шифрование (Wi-Fi Protected Access) [2]. Но зачастую встречаются сети с открытой аутентификацией без шифрования [3]. Как правило, это сети для общего доступа, функционирующие в транспорте, в парках, в торговых центрах или в кафе. В таких сетях много клиентов, и из-за отсутствия шифрования их легче всего атаковать злоумышленнику [4, 5].

Вопрос уязвимости сетей Wi-Fi и протокола IEEE 802.11 изучается в течение долгого времени. Несмотря на это, проблема безопасности не стала менее важной, так как появляются новые стандарты и технологии для передачи данных [6]. Новые исследования уязвимостей стандарта IEEE 802.11 необходимы для предотвращения новых преступлений в этой области [7, 8].

Цель исследования

Радиус действия сети при использовании технологии Wi-Fi может достигать 300 метров в пределах прямой видимости и 50 метров в закрытых помещениях. Такой большой радиус действия сети является не только достоинством стандарта, но и его недостатком. В большинстве случаев клиент не имеет никакой физической связи с точкой доступа Wi-Fi, к сети которой он собирается подключиться. Этой особенностью могут воспользоваться злоумышленники [9].

При выборе точки доступа для последующего подключения устройства клиент, как правило, руководствуется следующими правилами выбора сети:

- SSID точки доступа: клиент в первую очередь подключается к точке, SSID которой ему знаком;
- Уровень сигнала точки доступа: чем выше сигнал точки, тем больше скорость передачи данных и, следовательно, тем предпочтительнее для клиента эта сеть [10, 11];
- Метод аутентификации: при отсутствии известных сетей и наличии сети с открытой аутентификацией клиент подключится к открытой точке доступа [12].

Чтобы понять, может ли злоумышленник воспользоваться такой информацией о поведении клиента, необходимо провести исследование, анализирующее защищенность беспроводных клиентов. С его помощью можно проанализировать, может ли злоумышленник подключить Wi-Fi клиента к другой точке доступа и возможно ли с использованием программных средств создать точку доступа, к которой устройство клиента подключилось бы по умолчанию.

Используемое оборудование и ПО

Для анализа использовалось собственное программное обеспечение, обеспечивающее подготовку сетевого устройства беспроводной передачи данных к информационному захвату Wi-Fi трафика, генерацию пакета данных с необходимой конфигурацией по стандарту IEEE 802.11 и отправку данных с целью дальнейшего возможного выявления уязвимостей стандарта [13].

Разработанное программное обеспечение работает под управлением операционной системы Linux. Выбор используемой операционной системы основан на том, что в реализации библиотеки, работающей с драйвером сетевой карты, для других операционных систем есть особенности, которые в перспективе могут препятствовать проведению данного эксперимента.

Для разработки был выбран язык программирования C/C++.

Настройка сетевого адаптера и отправка пакета в сеть возможны с использованием специализированной статической библиотеки для захвата пакетов libpcap. Эта библиотека взаимодействует с драйвером сетевого адаптера на низком уровне. Libpcap используется известными снифферами, такими как Wireshark или TCPDump, для того, чтобы реализовать возможность захвата пакетов, фильтрации пакетов, анализа трафика, сохранение трафика в файл [14, 15]. Также в более новых версиях библиотеки появилась возможность передачи пакетов в сеть.

Для проведения эксперимента необходимо наличие двух сетевых адаптеров IEEE 802.11. Один из них работает в режиме мониторинга сети, с помощью второго адаптера будет производиться инжектирование пакетов. Данные режимы поддерживаются не всеми Wi-Fi модулями [16]. Мониторинг сети и отправка пакетов возможна только с теми чипами беспроводной связи, для которых написаны открытые драйверы. Wi-Fi адаптер D-Link DWA-137 на основе чипсета Ralink RT5372 совместим с соответствующим драйвером для Linux, в следствие чего он и был использован в данной работе.

Исходя из целей исследования, можно обозначить функции и возможности, которыми должно обладать программное обеспечение.

Во-первых, это необходимость конфигурации оборудования: изменение режима работы адаптера и изменение канала, на котором будет работать сетевое устройство [17]. Для того, чтобы отправить фрейм с сетевого устройства, необходимо перевести беспроводную карту в режим монитора (контроля), иначе программа не будет корректно работать [18]. Если адаптер работает в режиме монитора, он не отбрасывает сторонние пакеты, которые отправляет пользовательское приложение, и обрабатывает их наравне с фреймами, которые генерирует адаптер. В других режимах, альтернативных режиму монитора, такие пакеты будут игнорироваться адаптером.

Во-вторых, чтобы подключить клиента к другой точке доступа, нужно выполнить следующие действия:

1. Заставить клиента отключиться от точки доступа, к которой он подключен в данный момент времени;
2. Передать клиенту информацию о том, что вторая точка доступа, на которую необходимо переключить клиента (точка доступа 2), приоритетнее той, к которой он был подключен (точка доступа 1).

Эти задачи осуществимы с помощью отправки фрейма деаутентификации с указанием MAC-адреса источника, совпадающим с MAC-адресом точки доступа 1, и сигнального фрейма с указанием MAC-адреса источника, совпадающим с MAC-адресом точки доступа 2 [19, 20]. При этом необходимо, чтобы адаптер находился к клиенту ближе точки доступа 1, а мощность передатчика адаптера с учетом коэффициента усиления антенны была не ниже мощности точки доступа, так как сила сигнала точки доступа определяется устройством клиента и не зависит от содержания отправляемого фрейма [21, 22].

Алгоритм работы собственного программного обеспечения представлен на рисунке 1 с помощью блок-схемы алгоритма.

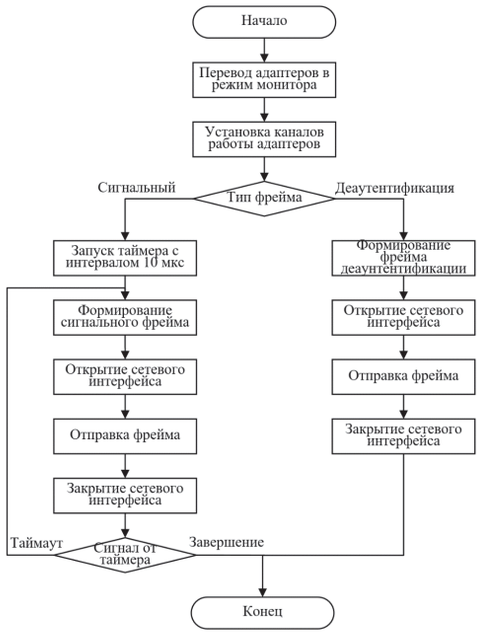

Рис. 1. Блок-схема алгоритма работы ПО
Fig. 1. Block diagram of the software operation

Методика эксперимента

Проведенный эксперимент состоял из нескольких этапов.

Вначале была настроена беспроводная сеть, в которой все точки доступа имеют SSID «Test» и тип шифрования WPA2. Сеть включает в себя две точки доступа и три различных устройства, являющихся клиентами. Для получения более точных результатов исследования все клиенты имеют различные версии ОС.

Клиент 1 является мобильным устройством Samsung с установленной ОС Android 7.1.1. Клиент 2 является мобильным устройством Huawei с установленной ОС Android 4.4.4.

В ходе эксперимента к сети подключался генератор фреймов стандарта IEEE 802.11, реализованный с использованием собственного ПО. Схема стенда представлена на рисунке 2.

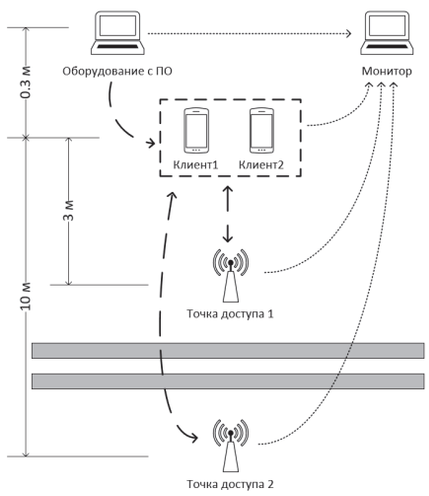

Рис. 2. Схема используемого стенда
Fig. 2. Diagram of the stand used

Используемые точки доступа расположены на различном расстоянии от клиентов и сетевого адаптера, с которым работает ПО. Точка доступа 1 находится вблизи, поэтому к ней клиенты подключаются по умолчанию. Точка доступа 2 находится в соседнем помещении, вдали от клиентов. Список точек доступа сети «Test» с приведением их характеристик представлены на рисунке 3 с помощью скриншота одного из клиентов.

Рис. 3. Характеристики сети «Test»

Fig. 3. Test Network Characteristics

При первичном подключении клиентов к сети «Test», наблюдается подключение к точке доступа 1 для всех клиентов. Информация о подключенной точке доступа для каждого клиента приведена в таблице 1.

Таблица 1. Информация о подключенной точке доступа на этапе 1

Table 1. Information about the connected access point in step 1

	Клиент 1	Клиент 2
SSID	Test	Test
BSSID	E4:18:6B:0D:E1:F8	E4:18:6B:0D:E1:F8
RSSI	-37	-42

При переносе клиентов от точки доступа 1 к точке доступа 2 происходит усиление сигнала точки доступа 2. В зависимости от производителя клиента и его ОС, может происходить автоматическое переподключение некоторых клиентов к точке доступа 2, так как она становится приоритетной. Информация о поведении каждого клиента при переносе приведена в таблице 2.

Таблица 2. Информация о подключенной точке доступа на этапе 2

Table 2. Information about the connected access point in step 2

Промежуток времени	Свойства точки	Клиент 1	Клиент 2
T1	SSID	Test	Test
	BSSID	E4:18:6B:0D:E1:F8	E4:18:6B:0D:E1:F8
	RSSI	-37	-42
T2	SSID	Test	Test
	BSSID	E4:18:6B:0D:E1:F8	E4:18:6B:0D:E1:F8
	RSSI	-57	-60

На следующем этапе был произведен перезапуск Wi-Fi модулей на всех клиентах. Наблюдаемым результатом было автоматическое подключение к точке доступа 2 всех клиентов. Информация о поведении каждого клиента на данном этапе приведена в таблице 3.

Таблица 3. Информация о подключенной точке доступа на этапе 3

Table 3. Information about the connected access point in step 3

Промежуток времени	Свойства точки	Клиент 1	Клиент 2
T1	SSID	Test	Test
	BSSID	E4:18:6B:0D:E1:F8	E4:18:6B:0D:E1:F8
	RSSI	-57	-60
T2	SSID	Test	Test
	BSSID	04:BF:6D:0D:EA:BA	04:BF:6D:0D:EA:BA
	RSSI	-36	-37

Изменение уровня сигнала и результат переподключения представлен на рисунке 4 с помощью скриншота одного из клиентов. На рисунке 5 приведен скриншот работы сниффера Wireshark, с помощью которого можно наглядно наблюдать результаты исследования. Процесс переподключения представлен на примере клиента 1.

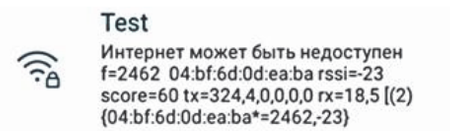

Рис. 4. Результат переподключения клиента 1

Fig. 4. Result of client reconnection 1

Процесс переподключения представляет собой «рукопожатие» между клиентом и точкой доступа. Клиент отключается от сети, но так как настройками задано автоматическое подключение к этой сети, он отправляет точке доступа фрейм запроса на зондирование Probe request. Точка доступа отвечает фреймом Probe response и клиент производит попытку аутентификации (фрейм Authentification). Точка доступа подтверждает аутентификацию соответствующим фреймом (Authentification), затем происходит процесс ассоциации и аутентификации по заданному точкой доступа механизму (в данном случае это обмен ключами шифрования EAPOL-Key).

```
3673 25.743297815  SamsungE_50:80:4a   ZyxelCom_0d:e1:f8   802.11    147 QoS Data, SN=349, FN=0, Flags=.p.....T
3743 26.141356064  SamsungE_50:80:4a   ZyxelCom_0d:e1:f8   802.11     42 Null function (No data), SN=382, FN=0, Flags=...P...T
4087 28.682959333  SamsungE_50:80:4a   ZyxelCom_0d:e1:f8   802.11     44 Deauthentication, SN=384, FN=0, Flags=....R...
4089 28.683669700  ZyxelCom_0d:e1:f8   SamsungE_50:80:4a   802.11     48 Action, SN=2064, FN=0, Flags=........
4091 28.684484105  ZyxelCom_0d:e1:f8   SamsungE_50:80:4a   802.11     48 Action, SN=2065, FN=0, Flags=........
4093 28.685289514  ZyxelCom_0d:e1:f8   SamsungE_50:80:4a   802.11     48 Action, SN=2066, FN=0, Flags=........
4242 29.828058438  ZyxelCom_0d:e1:f8   SamsungE_50:80:4a   802.11    369 Probe Response, SN=2087, FN=0, Flags=........, BI=100, SSID=Test
4257 29.913057991  ZyxelCom_0d:e1:f8   SamsungE_50:80:4a   802.11    369 Probe Response, SN=2265, FN=0, Flags=........, BI=100, SSID=Test
4258 29.916238434  ZyxelCom_0d:e1:f8   SamsungE_50:80:4a   802.11    369 Probe Response, SN=2266, FN=0, Flags=........, BI=100, SSID=Test
4260 29.919776377  SamsungE_50:80:4a   ZyxelCom_0d:ea:ba   802.11    122 Probe Request, SN=739, FN=0, Flags=........, SSID=Test
4265 29.929634927  ZyxelCom_0d:ea:ba   SamsungE_50:80:4a   802.11    352 Probe Response, SN=1985, FN=0, Flags=........, BI=100, SSID=Test
4267 29.932904410  ZyxelCom_0d:ea:ba   SamsungE_50:80:4a   802.11    352 Probe Response, SN=1986, FN=0, Flags=........, BI=100, SSID=Test
4774 33.609222603  ZyxelCom_0d:ea:ba   SamsungE_50:80:4a   802.11    352 Probe Response, SN=1987, FN=0, Flags=........, BI=100, SSID=Test
4775 33.613724117  SamsungE_50:80:4a   ZyxelCom_0d:ea:ba   802.11     48 Authentication, SN=740, FN=0, Flags=........
4777 33.617085496  ZyxelCom_0d:ea:ba   SamsungE_50:80:4a   802.11     48 Authentication, SN=1988, FN=0, Flags=........
4778 33.620160294  SamsungE_50:80:4a   ZyxelCom_0d:ea:ba   802.11    127 Association Request, SN=741, FN=0, Flags=........, SSID=Test
4780 33.623977977  ZyxelCom_0d:ea:ba   SamsungE_50:80:4a   802.11    211 Association Response, SN=1989, FN=0, Flags=........
4782 33.627311027  SamsungE_50:80:4a   ZyxelCom_0d:ea:ba   EAPOL     173 Key (Message 2 of 4)
4785 33.634315541  ZyxelCom_0d:ea:ba   SamsungE_50:80:4a   EAPOL     151 Key (Message 1 of 4)
4789 33.643007003  SamsungE_50:80:4a   ZyxelCom_0d:ea:ba   EAPOL     173 Key (Message 2 of 4)
4791 33.649627725  ZyxelCom_0d:ea:ba   SamsungE_50:80:4a   EAPOL     151 Key (Message 1 of 4)
4796 33.660484372  SamsungE_50:80:4a   IPv6mcast_ff:50:80:… 802.11   132 QoS Data, SN=0, FN=0, Flags=.p..R..T
4798 33.663780038  SamsungE_50:80:4a   IPv6mcast_ff:50:80:… 802.11   130 Data, SN=3744, FN=0, Flags=.p....F.
4809 33.711908934  SamsungE_50:80:4a   Broadcast           802.11    402 QoS Data, SN=1, FN=0, Flags=.p.....T
5349 37.917622524  ZyxelCom_0d:ea:ba   SamsungE_50:80:4a   802.11    396 QoS Data, SN=2, FN=0, Flags=.p....F.
5350 37.920660973  ZyxelCom_0d:ea:ba   SamsungE_50:80:4a   802.11     51 Action, SN=3745, FN=0, Flags=........
5352 37.924009861  SamsungE_50:80:4a   ZyxelCom_0d:ea:ba   802.11     51 Action, SN=117, FN=0, Flags=........
```

Рис. 5. Процесс переподключения клиента 1

Fig. 5. Client reconnection process 1

При переносе клиентов от точки доступа 2 к точке доступа 1 происходит усиление сигнала точки доступа 1, и она снова становится приоритетной. Исходя из результатов предыдущих этапов исследования, ожидаемым действием со стороны клиентов является переподключение к приоритетной точке либо сразу же после переноса клиента, либо после перезагрузки его Wi-Fi модуля или получения фрейма деаутентификации со стороны точки доступа. В соответствие с целью исследования, стояла задача понять, сможет ли злоумышленник в данной ситуации помешать клиентам подключиться к приоритетной точке доступа [23].

Проанализировав результаты предыдущих этапов исследования, можно сделать вывод, что точка становится приоритетной для клиента, если ее RSSI имеет наибольшее значение [24, 25]. Следующим этапом исследования была проверка гипотезы о том, что злоумышленнику для достижения своей цели достаточно задать для точки доступа 2 значение RSSI больше, чем у точки доступа 1, с использованием собственного ПО, описанного выше. На рисунке 6 наглядно показано, что исследование подтвердило гипотезу: когда ПО отправляет в эфир пакеты, содержащие сигнальные фреймы от точки доступа 2, устройства клиентов при анализе полученного пакета устанавливают соответствие между ними и пакетами от точки доступа 2, а затем отображают значение RSSI, принятое от ПО.

Рис. 6. Усиление сигнала точки доступа 2

Fig. 6. Gain signal of an access point 2

В таблице 4 приведены результаты исследования для анализируемых клиентов.

Таблица 4. Информация о подключенной точке доступа на этапе 4

Table 4. Information about the connected access point in step 4

Промежуток времени	Свойства точки	Клиент 1	Клиент 2
T1	SSID	Test	Test
	BSSID	04:BF:6D:0D:EA:BA	04:BF:6D:0D:EA:BA
	RSSI	-36	-37
T2	SSID	Test	Test
	BSSID	04:BF:6D:0D:EA:BA	04:BF:6D:0D:EA:BA
	RSSI	-21	-23

Результатом, наблюдаемым со стороны монитора, является отсутствие переподключения клиентов при их переносе от точки доступа 2 к точке доступа 1.

Из-за подключения ПО, характеристики всей сконфигурированной сети изменились. Таким образом, в отличие от результатов предыдущего аналогичного исследования, при перезагрузке Wi-Fi модулей клиентов, а также при отправке фреймов деаутентификации с MAC-адресом отправителя, совпадающим с MAC-адресом точки доступа 2, наблюдаемое поведение клиентов отличается от предыдущих результатов. Несмотря на то, что физическое расположение точки доступа 1 ближе, чем точки доступа 2, переподключение клиентов происходит не к ближайшей точке доступа, так как значение её RSSI оказалось ниже из-за вмешательства собственного ПО.

На рисунке 7 представлен результат переподключения клиента 1 на точку доступа 2, сигнал которой был усилен с помощью ПО.

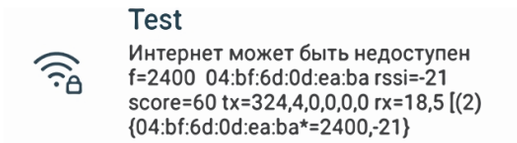

Рис. 7. Результат переподключения клиента 1

Fig. 7. Is the result of client reconnection 1

6320	45.153351368	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	44 Deauthentication, SN=2053, FN=0, Flags=........
6651	47.958168081	ZyxelCom_0d:e1:f8	SamsungE_50:80:4a	802.11	369 Probe Response, SN=2441, FN=0, Flags=........, BI=100, SSID=Test
6653	47.961472931	ZyxelCom_0d:e1:f8	SamsungE_50:80:4a	802.11	369 Probe Response, SN=2442, FN=0, Flags=........, BI=100, SSID=Test
6655	47.964667902	ZyxelCom_0d:e1:f8	SamsungE_50:80:4a	802.11	369 Probe Response, SN=2443, FN=0, Flags=........, BI=100, SSID=Test
6660	47.990805012	ZyxelCom_0d:e1:f8	SamsungE_50:80:4a	802.11	369 Probe Response, SN=2446, FN=0, Flags=........, BI=100, SSID=Test
6662	47.994217275	ZyxelCom_0d:e1:f8	SamsungE_50:80:4a	802.11	369 Probe Response, SN=2447, FN=0, Flags=........, BI=100, SSID=Test
6667	48.045164660	SamsungE_50:80:4a	Broadcast	802.11	118 Probe Request, SN=762, FN=0, Flags=........, SSID=Wildcard (Broadcast)
6668	48.047944521	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	352 Probe Response, SN=2086, FN=0, Flags=........, BI=100, SSID=Test
6671	48.054662697	ZyxelCom_0d:e1:f8	SamsungE_50:80:4a	802.11	369 Probe Response, SN=2448, FN=0, Flags=........, BI=100, SSID=Test
6673	48.058041031	ZyxelCom_0d:e1:f8	SamsungE_50:80:4a	802.11	369 Probe Response, SN=2449, FN=0, Flags=........, BI=100, SSID=Test
6675	48.061313983	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	352 Probe Response, SN=2088, FN=0, Flags=........, BI=100, SSID=Test
6677	48.064690987	ZyxelCom_0d:e1:f8	SamsungE_50:80:4a	802.11	369 Probe Response, SN=2450, FN=0, Flags=........, BI=100, SSID=Test
6681	48.077753377	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	352 Probe Response, SN=2089, FN=0, Flags=........, BI=100, SSID=Test
6683	48.081218148	ZyxelCom_0d:e1:f8	SamsungE_50:80:4a	802.11	369 Probe Response, SN=2452, FN=0, Flags=........, BI=100, SSID=Test
7522	54.910482514	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	352 Probe Response, SN=2177, FN=0, Flags=........, BI=100, SSID=Test
7524	54.920455103	ZyxelCom_0d:e1:f8	SamsungE_50:80:4a	802.11	369 Probe Response, SN=2594, FN=0, Flags=........, BI=100, SSID=Test
7526	54.923653835	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	352 Probe Response, SN=2178, FN=0, Flags=........, BI=100, SSID=Test
7528	54.927103077	ZyxelCom_0d:e1:f8	SamsungE_50:80:4a	802.11	369 Probe Response, SN=2595, FN=0, Flags=........, BI=100, SSID=Test
7530	54.934783878	SamsungE_50:80:4a	Broadcast	802.11	118 Probe Request, SN=841, FN=0, Flags=........, SSID=Wildcard (Broadcast)
7532	54.938667984	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	352 Probe Response, SN=2179, FN=0, Flags=........, BI=100, SSID=Test
7544	54.952670955	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	352 Probe Response, SN=2180, FN=0, Flags=........, BI=100, SSID=Test
7546	54.955934068	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	352 Probe Response, SN=2181, FN=0, Flags=........, BI=100, SSID=Test
7548	54.959232364	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	352 Probe Response, SN=2182, FN=0, Flags=........, BI=100, SSID=Test
7644	55.616599337	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	352 Probe Response, SN=2202, FN=0, Flags=........, BI=100, SSID=Test
7646	55.619967250	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	352 Probe Response, SN=2203, FN=0, Flags=........, BI=100, SSID=Test
7652	55.651797657	SamsungE_50:80:4a	ZyxelCom_0d:ea:ba	802.11	48 Authentication, SN=847, FN=0, Flags=........
7653	55.652676882	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	48 Authentication, SN=2204, FN=0, Flags=........
7655	55.655811570	SamsungE_50:80:4a	ZyxelCom_0d:ea:ba	802.11	127 Association Request, SN=848, FN=0, Flags=........, SSID=Test
7657	55.657977148	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	802.11	211 Association Response, SN=2205, FN=0, Flags=........
7881	57.856011857	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	EAPOL	151 Key (Message 1 of 4)
8002	58.856087544	ZyxelCom_0d:ea:ba	SamsungE_50:80:4a	EAPOL	151 Key (Message 1 of 4)

Рис. 8. Процесс переподключения клиента 1

Fig. 8. Client reconnection process 1

На рисунках 8 и 9 приведен скриншот работы сниффера Wireshark, с помощью которого можно наглядно наблюдать результаты исследования. На рисунке 8 наблюдается переподключение (процесс «рукопожатия») клиента 1 с точки доступа 2 на точку доступа 2. На рисунке 9 можно наблюдать аналогичный результат для клиента 2.

```
7171 52.201563687  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11    44 Deauthentication, SN=2149, FN=0, Flags=........
7590 55.310810400  HuaweiTe_02:34:33  Broadcast          802.11   100 Probe Request, SN=1106, FN=0, Flags=........, SSID=Wildcard (Broadcast)
7591 55.313772089  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2189, FN=0, Flags=........, BI=100, SSID=Test
7593 55.323556296  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2190, FN=0, Flags=........, BI=100, SSID=Test
7595 55.327030791  ZyxelCom_0d:e1:f8  HuaweiTe_02:34:33  802.11   369 Probe Response, SN=2605, FN=0, Flags=........, BI=100, SSID=Test
7597 55.328242925  HuaweiTe_02:34:33  Broadcast          802.11   100 Probe Request, SN=1108, FN=0, Flags=........, SSID=Wildcard (Broadcast)
7598 55.331325542  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2191, FN=0, Flags=........, BI=100, SSID=Test
7600 55.334702487  ZyxelCom_0d:e1:f8  HuaweiTe_02:34:33  802.11   369 Probe Response, SN=2606, FN=0, Flags=........, BI=100, SSID=Test
7601 55.340851012  ZyxelCom_0d:e1:f8  HuaweiTe_02:34:33  802.11   369 Probe Response, SN=2608, FN=0, Flags=........, BI=100, SSID=Test
7604 55.346489026  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2192, FN=0, Flags=........, BI=100, SSID=Test
7606 55.352971562  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2193, FN=0, Flags=........, BI=100, SSID=Test
7608 55.356293115  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2194, FN=0, Flags=........, BI=100, SSID=Test
7610 55.360141424  D-LinkIn_91:8d:98  HuaweiTe_02:34:33  802.11   426 Probe Response, SN=965, FN=0, Flags=........, BI=100, SSID=dlink22
7611 55.366972264  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2195, FN=0, Flags=........, BI=100, SSID=Test
7612 55.369878333  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2196, FN=0, Flags=........, BI=100, SSID=Test
7613 55.372830141  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2197, FN=0, Flags=........, BI=100, SSID=Test
7614 55.375777896  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2198, FN=0, Flags=........, BI=100, SSID=Test
7615 55.378849023  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2199, FN=0, Flags=........, BI=100, SSID=Test
7616 55.381856738  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2200, FN=0, Flags=........, BI=100, SSID=Test
7996 58.813229838  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2224, FN=0, Flags=........, BI=100, SSID=Test
7997 58.816235230  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2225, FN=0, Flags=........, BI=100, SSID=Test
7999 58.822425517  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11   352 Probe Response, SN=2226, FN=0, Flags=........, BI=100, SSID=Test
8006 58.865325235  HuaweiTe_02:34:33  ZyxelCom_0d:ea:ba  802.11    48 Authentication, SN=1111, FN=0, Flags=........
8008 58.866156846  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11    48 Authentication, SN=2227, FN=0, Flags=........
8024 59.067932767  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  EAPOL    151 Key (Message 1 of 4)
8129 60.072389252  HuaweiTe_02:34:33  ZyxelCom_0d:ea:ba  EAPOL    173 Key (Message 2 of 4)
8251 61.068072646  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  EAPOL    151 Key (Message 1 of 4)
8375 62.068087014  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  EAPOL    151 Key (Message 1 of 4)
8377 62.070530868  HuaweiTe_02:34:33  ZyxelCom_0d:ea:ba  EAPOL    173 Key (Message 2 of 4)
8786 65.073571771  ZyxelCom_0d:ea:ba  HuaweiTe_02:34:33  802.11    44 Deauthentication, SN=2297, FN=0, Flags=........
```

Рис. 9. Процесс переподключения клиента 2

Fig. 9. Client reconnection process 2

В таблице 5 приведены данные о переподключении клиентов, где наглядно указаны различия в поле RSSI для пакета деаутентификации, полученного от адаптера, используемого программой, и пакета аутентификации, полученного от настоящей точки доступа.

Таблица 5. Информация о характеристике сети на этапе 5

Table 5. Information about the network characteristics in step 5

Свойства точки	Клиент 1	Клиент 2
SSID	Test	Test
BSSID	04:BF:6D:0D:EA:BA	04:BF:6D:0D:EA:BA
RSSI (деаутентификация)	-21	-23
RSSI (аутентификация)	-58	-63

Таким образом, можно наблюдать, что с помощью сгенерированных сигнальных фреймов, которые выполняют вспомогательную функцию для усиления сигнала точки доступа 2, можно установить подключение со слабой точкой доступа.

Полученные результаты

В результате исследования был изучен вопрос безопасности беспроводных клиентов. Полученные результаты подтверждают возможность для злоумышленника переключать клиентов к точке доступа, необходимой самому злоумышленнику. Так как радиус действия беспроводной сети может достигать 50 метров, точки доступа зачастую находится вне зоны видимости клиента. Так, в исследовании предусмотрена возможность использования злоумышленником нескольких помещений: между точкой доступа и клиентом находилось две бетонных стены толщиной 10 см.

Успешность злоумышленника в данном случае зависит от того, с какими настройками работает его программное обеспечение для отправки сигнальных фреймов, а также от его физического расположения относительно клиентов и точек доступа, от которых ему необходимо отключить клиентов, мощности передатчика используемого им адаптера для отправки фреймов и коэффициента усиления антенн этого адаптера.

В ходе исследования была собрана статистика по успешности проведенного эксперимента, а также проведен анализ необходимых условий для успешной атаки на различных беспроводных клиентов. Данные для статистики были собраны для разной частоты отправки сигнального фрейма. Результаты собранной статистки по усилению сигнала слабой точки доступа приведены в таблице 6. Результаты собранной статистики по переподключению клиентов к слабой точке доступа и использованием усиления ее сигнала приведены в таблице 7.

Таблица 6. Статистика по усилению сигнала

Table 6. Signal Strength Statistics

Частота отправки фрейма	Клиент 1			Клиент 2		
	Количество проверок сети	Количество успешного усиления сигнала	Относительный показатель, %	Количество проверок сети	Количество успешного усиления сигнала	Относительный показатель, %
5 Гц	20	0	0	20	0	0
10 Гц (beacon interval)	20	2	10	20	1	5
25 Гц	20	3	15	20	3	15
50 Гц	20	6	30	20	5	25
75 Гц	20	10	50	20	11	55
100 Гц	20	18	90	20	19	95

Таблица 7. Статистика по переподключению клиентов
Table 7. Client Reconnect Statistics

Частота отправки фрейма	Клиент 1			Клиент 2		
	Количество попыток переподключения	Количество успешного переподключения	Относительный показатель, %	Количество попыток переподключения	Количество успешного переподключения	Относительный показатель, %
10 Гц (beacon interval)	20	0	0	20	0	0
50 Гц	20	1	5	20	2	10
75 Гц	20	4	20	20	5	25
100 Гц	20	14	70	20	15	75
125 Гц	20	16	80	20	18	90
150 Гц	20	16	80	20	18	90

Исходя из статистических данных, можно сделать вывод о том, что злоумышленнику необходимо отправлять сигнальный фрейм с частотой, в 10 раз превышающей частоту появления в сети сигнальных фреймов от настоящей точки доступа.

Более низкий показатель переподключения клиентов, по сравнению с показателем по усилению сигнала, объясняется тем, что во время процессов аутентификации и обмена ключами шифрования между слабой точкой доступа и клиентом есть вероятность разрыва связи, так как сила сигнала слабой точки доступа в действительности намного ниже, чем считает клиент.

Заключение

По итогу исследования, можно сделать вывод о том, что для беспроводных клиентов существует уязвимость, согласно которой злоумышленник может отключить клиентов от точек доступа, к которым они подключены, и подключить к другой точке доступа, менее безопасной. Подключив клиента к другой точке доступа, злоумышленник получит возможность перехватывать данные, отправляемые клиентом. Это могут быть личные данные, пароли или иная информация, утрата которой опасна для клиентов.

Особенно актуальной эта проблема является в случае использования открытых беспроводных сетей, не защищенных шифрованием. Такие сети используются во многих общественных местах. В этом случае данные, передаваемые клиентом, не зашифрованы, а значит риск попадания личных данных третьим лицам резко возрастает.

Чтобы обезопасить себя от таких ситуаций, пользователю следует по возможности избегать использования открытых точек доступа, не защищенных шифрованием. Защита данных шифрованием в рассматриваемом случае значительно усложнит задачу злоумышленника, но не исключит возможность утечки данных. Безусловно, поставщики услуг стремятся повысить степень безопасности предоставляемых ими сетей, но пользователям необходимо помнить о существующей угрозе и также принимать необходимые меры для защиты своих личных данных.

Список использованных источников

[1] *Buttyán L., Dóra L.* WiFi Security – WEP and 802.11i // EURASIP Journal on Wireless Communications and Networking. 2006. Vol. 2006, issue 1. Pp. 1-13. URL: http://www.hit.bme.hu/~buttyan/publications/ButtyanD06ht-en.pdf (дата обращения: 26.09.2018).

[2] *Reddy S.V., Ramani K.S., Rijutha K., Mohammad Ali S., Reddy C.P.* Wireless hacking – a WiFi hack by cracking WEP // Proceedings of 2010 2nd International Conference on Education Technology and Computer. Shanghai, 2010. Pp. V1-189-V1-193. DOI: 10.1109/ICETC.2010.5529269

[3] *Goncharov D.E., Zareshin S.V., Bulychev R.V., Silnov D.S.* Vulnerability analysis of the Wifi spots using WPS by modified scanner vistumbler // Proceedings of 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). Moscow, 2018. Pp. 48-51. DOI: 10.1109/EIConRus.2018.8317027

[4] *Zareshin S.V., Shustova L.I., Shestakova N.Y.* Comprehensive analysis of wireless networks security in Moscow Central District // Proceedings of 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). St. Petersburg, 2017. Pp. 240-241. DOI: 10.1109/EIConRus.2017.7910537

[5] *Anastasia A.V., Zareshin S.V., Rumyantseva I.S., Ivanenko V.G.* Analysis of security of public access to Wi-Fi networks on Moscow streets // Proceedings of 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). St. Petersburg, 2017. Pp. 105-110. DOI: 10.1109/EIConRus.2017.7910505

[6] *Rowan T.* Negotiating WiFi security // Network Security. 2010. Vol. 2010, issue 2. Pp. 8-12. DOI: 10.1016/S1353-4858(10)70024-6

[7] *Egupov A.A., Zareshin S.V., Yadikin I.M., Silnov D.S.* Development and implementation of a Honeypot-trap // Proceedings of 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). St. Petersburg, 2017. Pp. 382-385. DOI: 10.1109/EIConRus.2017.7910572

[8] *Peng H.* WIFI network information security analysis research // Proceedings of 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet). Yichang, 2012. Pp. 2243-2245. DOI: 10.1109/CECNet.2012.6201786

[9] *Hole K.J., Dyrnes E., Thorsheim P.* Securing Wi-Fi networks // Computer. 2005. Vol. 38, no. 7. Pp. 28-34. DOI: 10.1109/MC.2005.241

[10] *Arbaugh W.A.* Wireless security is different // Computer. 2003. Vol. 36, no. 8. Pp. 99-101. DOI: 10.1109/MC.2003.1220591

[11] *Zàruba G.V., Huber M., Kamangar F.A.* et al. Indoor location tracking using RSSI readings from a single Wi-Fi access point // Wireless networks. 2007. Vol. 13, issue 2. Pp. 221-235. DOI: 10.1007/s11276-006-5064-1

[12] *Zafft A., Agu E.* Malicious WiFi networks: A first look // Proceedings of the 37th Annual IEEE Conference on Local Com-

puter Networks - Workshops. Clearwater, FL, 2012. Pp. 1038-1043. DOI: 10.1109/LCNW.2012.6424041

[13] *Karpowicz M.P., Arabas P.* Preliminary results on the Linux libpcap model identification // Proceedings of 2015 20th International Conference on Methods and Models in Automation and Robotics (MMAR). Miedzyzdroje, 2015. Pp. 1056-1061. DOI: 10.1109/MMAR.2015.7284025

[14] *Garcia L.M.* Programming with Libpcap – Sniffing the Network From Our Own Application // Hackin9. Computer Security Magazine. 2008. Vol. 3, no. 2. Pp. 38-46. URL: https://www.kapravelos.com/teaching/csc574-f16/readings/libpcap.pdf (дата обращения: 26.09.2018).

[15] *Banerjee U., Vashishtha A., Saxena M.* Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection // International Journal of Computer Applications. 2010. Vol. 6, no. 7. 5 p. URL: http://citeseerx.ist.psu.edu/viewdoc/download?-doi=10.1.1.206.4345&rep=rep1&type=pdf (дата обращения: 26.09.2018).

[16] *Musa A.B.M., Eriksson J.* Tracking Unmodified Smartphones Using Wi-Fi Monitors // Proceedings of the 10th ACM conference on embedded network sensor systems. ACM, 2012. Pp. 281-294. DOI: 10.1145/2426656.2426685

[17] *Shin S., Forte A.G., Rawat A.S., Schulzrinne H.* Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs // Proceedings of the second international workshop on Mobility management & wireless access protocols. ACM, 2004. Pp. 19-26. DOI: 10.1145/1023783.1023788

[18] *Chandra R., Bahl P., Bahl P.* MultiNet: connecting to multiple IEEE 802.11 networks using a single wireless card // Proceedings of IEEE INFOCOM 2004. Hong Kong, 2004. Vol. 2. Pp. 882-893. DOI: 10.1109/INFCOM.2004.1356976

[19] *Chandra R., Padhye J., Ravindranath L., Wolman A.* Beacon-Stuffing: Wi-Fi without Associations // Proceedings of the Eighth IEEE Workshop on Mobile Computing Systems and Applications. Tucson, AZ, 2007. Pp. 53-57. DOI: 10.1109/HotMobile.2007.16

[20] *Freudiger J.* How talkative is your mobile device?: an experimental study of Wi-Fi probe requests // Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '15). ACM, New York, NY, USA, 2015. Article 8, 6 p. DOI: 10.1145/2766498.2766517

[21] *Cunche M.* I know your MAC Address: Targeted tracking of individual using Wi-Fi //Journal of Computer Virology and Hacking Techniques. 2014. Vol. 10, issue 4. Pp. 219-227. DOI: 10.1007/s11416-013-0196-1

[22] *Lui G., Gallagher T., Li B., Dempster A.G., Rizos C.* Differences in RSSI readings made by different Wi-Fi chipsets: A limitation of WLAN localization // Proceedings of 2011 International Conference on Localization and GNSS (ICL-GNSS). Tampere, 2011. Pp. 53-57. DOI: 10.1109/ICL-GNSS.2011.5955283

[23] *Koo J., Cha Y.* Localizing WiFi Access Points Using Signal Strength // *IEEE Communications Letters*. 2011. Vol. 15, no. 2. Pp. 187-189. DOI: 10.1109/LCOMM.2011.121410.101379

[24] *Xue W., Qiu W., Hua X., Yu K.* Improved Wi-Fi RSSI Measurement for Indoor Localization // IEEE Sensors Journal. 2017. Vol. 17, no. 7. Pp. 2224-2230. DOI: 10.1109/JSEN.2017.2660522

[25] *Kim M., Kotz D.* Modeling users' mobility among WiFi access points // Papers presented at the 2005 workshop on Wireless traffic measurements and modeling (WiTMeMo '05). USENIX Association, Berkeley, CA, USA, 2005. Pp. 19-24. URL: https://dl.acm.org/citation.cfm?id=1072434 (дата обращения: 26.09.2018).

Поступила 26.09.2018; принята в печать 10.10.2018;
опубликована онлайн 10.12.2018.

References

[1] Buttyán L., Dóra L. WiFi Security – WEP and 802.11i. *EURASIP Journal on Wireless Communications and Networking*. 2006; 2006(1):1-13. Available at: http://www.hit.bme.hu/~buttyan/publications/ButtyanD06ht-en.pdf (accessed 26.09.2018).

[2] Reddy S.V., Ramani K.S., Rijutha K., Mohammad Ali S., Reddy C.P. Wireless hacking – a WiFi hack by cracking WEP. *Proceedings of 2010 2nd International Conference on Education Technology and Computer*. Shanghai, 2010, pp. V1-189-V1-193. DOI: 10.1109/ICETC.2010.5529269

[3] Goncharov D.E., Zareshin S.V., Bulychev R.V., Silnov D.S. Vulnerability analysis of the Wifi spots using WPS by modified scanner vistumbler. *Proceedings of 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. Moscow, 2018, pp. 48-51. DOI: 10.1109/EIConRus.2018.8317027

[4] Zareshin S.V., Shustova L.I., Shestakova N.Y. Comprehensive analysis of wireless networks security in Moscow Central District. *Proceedings of 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. St. Petersburg, 2017, pp. 240-241. DOI: 10.1109/EIConRus.2017.7910537

[5] Anastasia A.V., Zareshin S.V., Rumyantseva I.S., Ivanenko V.G. Analysis of security of public access to Wi-Fi networks on Moscow streets. *Proceedings of 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. St. Petersburg, 2017, pp. 105-110. DOI: 10.1109/EIConRus.2017.7910505

[6] Rowan T. Negotiating WiFi security. *Network Security*. 2010; 2010(2):8-12. DOI: 10.1016/S1353-4858(10)70024-6

[7] Egupov A.A., Zareshin S.V., Yadikin I.M., Silnov D.S. Development and implementation of a Honeypot-trap. *Proceedings of 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. St. Petersburg, 2017, pp. 382-385. DOI: 10.1109/EIConRus.2017.7910572

[8] Peng H. WIFI network information security analysis research. *Proceedings of 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*. Yichang, 2012, pp. 2243-2245. DOI: 10.1109/CECNet.2012.6201786

[9] Hole K.J., Dyrnes E., Thorsheim P. Securing Wi-Fi networks. *Computer*. 2005; 38(7):28-34. DOI: 10.1109/MC.2005.241

[10] Arbaugh W.A. Wireless security is different. *Computer*. 2003; 36(8):99-101. DOI: 10.1109/MC.2003.1220591

[11] Zàruba G.V., Huber M., Kamangar F.A. et al. Indoor location tracking using RSSI readings from a single Wi-Fi access point. *Wireless networks*. 2007; 13(2):221-235. DOI: 10.1007/s11276-006-5064-1

[12] Zafft A., Agu E. Malicious WiFi networks: A first look. *Proceedings of the 37th Annual IEEE Conference on Local Computer Networks - Workshops*. Clearwater, FL, 2012, pp.

1038-1043. DOI: 10.1109/LCNW.2012.6424041

[13] Karpowicz M.P., Arabas P. Preliminary results on the Linux libpcap model identification. *Proceedings of 2015 20th International Conference on Methods and Models in Automation and Robotics (MMAR)*. Miedzyzdroje, 2015, pp. 1056-1061. DOI: 10.1109/MMAR.2015.7284025

[14] Garcia L.M. Programming with Libpcap – Sniffing the Network From Our Own Application. *Hackin9. Computer Security Magazine*. 2008; 3(2):38-46. Available at: https://www.kapravelos.com/teaching/csc574-f16/readings/libpcap.pdf (accessed 26.09.2018).

[15] Banerjee U., Vashishtha A., Saxena M. Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. *International Journal of Computer Applications*. 2010; 6(7):1-5. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.206.4345&rep=rep1&type=pdf (accessed 26.09.2018).

[16] Musa A.B.M., Eriksson J. Tracking Unmodified Smartphones Using Wi-Fi Monitors. *Proceedings of the 10th ACM conference on embedded network sensor systems*. ACM, 2012, pp. 281-294. DOI: 10.1145/2426656.2426685

[17] Shin S., Forte A.G., Rawat A.S., Schulzrinne H. Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs. *Proceedings of the second international workshop on Mobility management & wireless access protocols*. ACM, 2004, pp. 19-26. DOI: 10.1145/1023783.1023788

[18] Chandra R., Bahl P., Bahl P. MultiNet: connecting to multiple IEEE 802.11 networks using a single wireless card. *Proceedings of IEEE INFOCOM 2004*. Hong Kong, 2004; 2:882-893. DOI: 10.1109/INFCOM.2004.1356976

[19] Chandra R., Padhye J., Ravindranath L., Wolman A. Beacon-Stuffing: Wi-Fi without Associations. *Proceedings of the Eighth IEEE Workshop on Mobile Computing Systems and Applications*. Tucson, AZ, 2007, pp. 53-57. DOI: 10.1109/HotMobile.2007.16

[20] Freudiger J. How talkative is your mobile device?: an experimental study of Wi-Fi probe requests. *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '15)*. ACM, New York, NY, USA, 2015. Article 8, 6 p. DOI: 10.1145/2766498.2766517

[21] Cunche M. I know your MAC Address: Targeted tracking of individual using Wi-Fi. *Journal of Computer Virology and Hacking Techniques*. 2014; 10(4):219-227. DOI: 10.1007/s11416-013-0196-1

[22] Lui G., Gallagher T., Li B., Dempster A.G., Rizos C. Differences in RSSI readings made by different Wi-Fi chipsets: A limitation of WLAN localization. *Proceedings of 2011 International Conference on Localization and GNSS (ICL-GNSS)*. Tampere, 2011, pp. 53-57. DOI: 10.1109/ICL-GNSS.2011.5955283

[23] Koo J., Cha Y. Localizing WiFi Access Points Using Signal Strength. *IEEE Communications Letters*. 2011; 15(2):187-189. DOI: 10.1109/LCOMM.2011.121410.101379

[24] Xue W., Qiu W., Hua X., Yu K. Improved Wi-Fi RSSI Measurement for Indoor Localization. *IEEE Sensors Journal*. 2017; 17(7):2224-2230. DOI: 10.1109/JSEN.2017.2660522

[25] Kim M., Kotz D. Modeling users' mobility among WiFi access points. *Papers presented at the 2005 workshop on Wireless traffic measurements and modeling (WiTMeMo '05)*. USENIX Association, Berkeley, CA, USA, 2005, pp. 19-24. Available at: https://dl.acm.org/citation.cfm?id=1072434 (accessed 26.09.2018).

Submitted 26.09.2018; revised 10.10.2018;
published online 10.12.2018.

About the authors:

Elena A. Baranova, Master Student of the Department of computer systems and technologies, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) (31 Kashirskoe shosse, Moscow 115409, Russia), ORCID: http://orcid.org/0000-0002-4439-297X, baranovaeaa@yandex.ru

Sergey V. Zareshin, Master, Assistant of the Institute of Cyber Intelligence, Systems, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) (31 Kashirskoe shosse, Moscow 115409, Russia), ORCID: http://orcid.org/0000-0002-4183-1535, svzareshin@gmail.com