1	Вывод итогов								
2									
3	Регрессионная статистика								
4	Множественный R	0,230953144							
5	R-квадрат	0,053339355							
6	Нормированный R-квадрат	-0,058032486							
7	Стандартная ошибка	4,935553302							
8	Наблюдения	20							
9									
10	Дисперсионный анализ								
11		df	SS	MS	F	Значимость F			
12	Регрессия	2	23,33318623	11,66659311	0,478930349	0,62755493			
13	Остаток	17	414,1146688	24,3596864					
14	Итого	19	437,447855						
15									
16		Коэффициенты	Стандартная ошибка	t-статистика	P-значение	Нижние 95%	Верхние 95%	Нижние 95,0%	Верхние 95,0%
17	Y-пересечение	9,30399599	1,309866983	7,103008254	1,7713E-06	6,540418225	12,06757375	6,540418225	12,06757375
18	Переменная X 1	-1,420435228	1,494261259	-0,950593626	0,355130778	-4,57305091	1,732180454	-4,57305091	1,732180454
19	Переменная X 2	0,051563008	0,081330261	0,633995362	0,534522414	-0,120028843	0,223154859	-0,120028843	0,223154859
20									
21									

Рисунок 1 – Регрессионный анализ

Коэффициент детерминации и коэффициент корреляции соответственно равны $R^2 = 0,0533$, $R = 0,2309$. Следовательно, корреляционная связь между переменными практически отсутствует, т.к. показатель меньше 0,3. Коэффициент детерминации близок к 0, поэтому данная модель имеет низкую значимость. Другими словами, входная переменная плохо «объясняет» поведение выходной, т.е. линейная зависимость между ними отсутствует.

После этого окончательная функция примет вид:

$$Y(t) = 9,3039 - 1,4204x_1 + 0,0515x_2.$$

Следует понимать, что полученные результаты нельзя считать окончательными. Их оценка и применение должны учитывать факторы, условия или ограничения, которые не были приняты во внимание при разработке статистической модели, и должны корректировать статистические характеристики в соответствии с ожидаемым изменением обстоятельств их формирования.

1. Горелова Г. В. Теория вероятностей и математическая статистика в примерах и задачах с применением Excel: учеб. пособие / Г. В. Горелова, И.А.Кацко. – Ростов-на-Дону : Феникс, 2005. – 480 с.
2. Гулай Т. А. Элементы теории вероятностей и математической статистики : учеб. пособие/ Т. А. Гулай, А. Ф. Долгополова, В. А. Жукова, С.В.Мелешко, И. А. Невидомская. – Ставрополь: Сервисшкола, 2017. – 116 с.
3. Лукашин Ю. П. Адаптивные методы краткосрочного прогнозирования временных рядов / Ю. П. Лукашин. – М. : Финансы и статистика, 2003. – 414 с.
4. Чашкин Ю. Р. Математическая статистика. Анализ и обработка данных: учеб. пособие / Ю. Р. Чашкин, С. Н. Смоленский. – Ростов-на-Дону : Феникс, 2010. – 236 с.

Смирнов В.М., Гулабян А.О.

Угрозы, исходящие из открытых сетей Wi-Fi, их последствия и меры безопасности

*Московский университет МВД имени В. Я. Кикотя
(Россия, Москва)*

doi: 10.18411/lj-06-2021-69

Аннотация

В статье рассмотрены угрозы, которые исходят из открытых сетей Wi-Fi, для пользователей всего мира. Указаны негативные последствия в случае несанкционированного доступа к сети Wi-Fi и проанализированы меры безопасности, которые должны быть реализованы.

Ключевые слова: угрозы, беспроводные сети, безопасность, Wi-Fi, информационная безопасность.

Abstract

The article examines the threats posed by open Wi-Fi networks for users around the world. The negative consequences in case of unauthorized access to the Wi-Fi network are indicated and the security measures to be implemented are analyzed.

Keywords: threats, wireless networks, security, Wi-Fi, information security.

Каждый день миллионы людей в мире пользуются беспроводной сетью Wi-Fi, которая предоставляет им бесплатный доступ к интернету. Открытая сеть Wi-Fi отличается доступностью и простотой использования, так любой пассажир, клиент, покупатель различного торгового центра, кафе, метро и тому подобное, может подключиться без логина и пароля. Технология Wi-Fi, которая используется в открытых сетях, обеспечивает аутентификацию и хранение данных пользователя, что как раз и представляет собой угрозу. Однако, обеспечение информационной безопасности, используемые представителями информационной безопасности в различных странах, не всегда могут защитить информацию о пользователе, а его данные могут попасть к злоумышленникам. Поэтому важно исследовать угрозы, возникающие при использовании открытыми сетями Wi-Fi, установить негативные последствия и возможные меры безопасности по их предотвращению.

Угрозами информационной безопасности открытой сети Wi-Fi являются:

1. Использование устаревших технологий шифрования конфиденциальности, которые дискредитировали себя, ввиду высокой степени уязвимости алгоритмов распределения ключей. Несмотря на то, что информационная служба безопасности защиты конфиденциальных данных утверждает, что используется только высокотехнологические точки и оборудование для доступа в Интернет [2], специалисты в сфере информационной безопасности, такие как Касперский, указывают на устаревшее оборудование и программное обеспечение, используемое допустим в метро [4, С. 89]. Существует множество программ, посредством которых злоумышленники могут подобрать WEP-ключи для взлома открытой сети Wi-Fi.

В результате несанкционированного подключения к сети Интернет через взлом сети Wi-Fi, злоумышленники получают доступ к данным информации пользователей, которые пользуются Wi-Fi. В результате другие лица могут получить доступ не только к личной информации пользователей Интернета в метро, но и к данным банковских карт, логинам и паролям, маршрутах их передвижения. Личные данные могут быть проданы мошенникам, а деньги с банковских счетов могут списать мошенники.

2. Дублирование точки доступа, которая осуществляется посредством того, что злоумышленник заменяет основной источник доступа к сети, получивший название «злой двойник» [5, С. 92]. Однако, данный метод применяется достаточно редко, так как для его реализации требуется не только высокотехнологичное оборудование, но и новейшее программное обеспечение, а также значение SSID.

3. Вместе с тем, злоумышленники могут создать вторую сеть Wi-Fi, со схожим названием, к которой могут подключиться пользователи. Например, пользователь сети Интернет не заметит, что помимо доступа к сети «MT_FREE» существуют также и другие сети – «MT-FRE» или «MT-FREE». По невнимательности человек может подключиться не к безопасной и официальной сети Wi-Fi, которую предоставляет Интернет, а к дополнительной сети, которая была создана злоумышленниками. Данная сеть создается, для того чтобы выдать ее за известную общественную Wi-Fi сеть, для отслеживания интернет-трафика, получения и кражи информации о пользователях.

Можно выделить следующие негативные последствия возможных угроз информационной безопасности при использовании незащищенной сети Wi-Fi:

- получение информации о пользователях, допустим в открытых сетях аэропорта. Данная информация может быть продана другим лицам,

которые могут использовать ее в преступных целях. Например, узнать график и маршрут передвижения конкретного человека, его увлечения, хобби и т.п.;

- получить доступ к смартфону или ноутбуку пользователя, подключившегося к сети, распространяющей угрозы. Например, в качестве исходной точки доступа для совершения другого преступления;
- установление вредоносных программ. К такому типу программ относятся: программы и утилиты, направленные на контроль мобильного устройства, использование в качестве исходной точки для совершения противоправных действий. Опасность установки подобных программ заключается в том, что они работают в фоновом режиме, а поэтому многие пользователи не смогут их обнаружить и удалить со своего телефона, смартфона или ноутбука;
- кража личной информации, такой как паспортные данные, информация о банковских картах, логины и пароли, которые использует клиент, например, развлекательных центров. Данная информация может быть использована для совершения покупок от имени и за счет пользователя, получение кредита и т.п. [6, С. 96- 97]

Поэтому необходимо применять внешние и внутренние меры безопасности для предупреждения угроз уязвимости Wi-Fi.

Внутренние меры безопасности, осуществляют сотрудники безопасности по обеспечению защиты конфиденциальных данных и направлены на:

- использование новейших и актуальных технологий Wi-Fi Protect Access (WPA), которая поддерживает протокол TKIP (Temporal Key Integrity Protocol), который использует метод шифрования RC4 и обеспечивает защиту посредством обновления программного обеспечения. Оборудование, которое подключается к точке доступа, осуществляет декодировку интернет-трафика посредством РМК [4, С. 90].
- осуществления аутентификации пользователей в сети Wi-Fi посредством аутентификации MAC-адресов. Данная мера безопасности осуществляется сетевым администратором, которые осуществляют настройку доступа в точку посредством налаживания специальной таблицы фильтрации. Любой несанкционированный доступ к данной точке будет отклонён [1, С. 940].
- совершенствования архитектуры сети Wi-Fi, которая не позволит злоумышленникам получить доступ к личным данным пользователей.
- совершенствование методов и способов аутентификации, посредством применения модифицированных протоколов и изменение конкретных свойств протоколов. Посредством использования данного метода используется программный пакет защиты Wi-Fi и VPN, которые направлены на обеспечение высокого уровня защиты данных пользователей открытой сети Wi-Fi. Программное обеспечение и установка VPN сервера позволяет реализовать окончательную идентификацию и аутентификацию пользователей и тем самым защищает сеть Wi-Fi [4, С. 93].

Внешние меры безопасности, применяется самими пользователями открытой сети Wi-Fi и заключается в следующем:

- повышение уровня информационной грамотности пассажиров в местах с открытыми сетями, которые направлены на информирование о способах и меры защиты своих данных.

- использование средств защиты своих данных.
- использование специальных надстроек Интернет-браузеров, которые направлены на обеспечение безопасного входа и использования Интернетом.
- подключение к виртуальной частной сети (VPN), которое защитит данные пользователей открытых сетей Wi-Fi [3, С. 53-54];
- пользователи открытых сетей не должны передавать персональные либо конфиденциальные данные при использовании открытой сети Wi-Fi. Необходимо помнить, что данная сеть в первую очередь направлена на получение информации, а не на ее передачу. Поэтому также нельзя использовать интернет-банкинг.
- включать настройки фаервола и антивирусы на блокировку входящего трафика, постоянно обновлять базы вирусов, включать режим расширенного эвристического анализа.

Таким образом, комплексный подход к обеспечению безопасности открытых сетей Wi-Fi, позволит предотвратить угрозы со стороны злоумышленников и защитит данные и информацию о пользователях открытых сетей Wi-Fi в различных местах их возможной угрозы.

1. Баранова Е.А., Зарешин С.В. Анализ защищенности беспроводных клиентов//Современные информационные технологии и ИТ-образование. 2018. Т. 14. № 4. С. 938-946.
2. Бесплатный Wi-Fi в метро [Электронный ресурс] URL: <https://www.mosmetro.ru/info/wifi-v-metro/> (Дата доступа: 27.03.2021)
3. Джумагалиева А.М. О возможностях предотвращения угроз информационной безопасности сетей на основе Wi-Fi технологий//Электронный журнал. 2018. № 1. С. 51 – 59.
4. Мокану Г.С. Проблема безопасности пользователей в сетях Wi-Fi// Информационно-технологический вестник. 2020. № 4 (26). С. 89-95.
5. Куринный Ф.А., Паслён В.В. Угрозы безопасности управления информацией в беспроводных системах Wi-Fi//Современные проблемы радиоэлектроники и телекоммуникаций. 2020. № 3. С. 92.
6. Кожушко В.В. Угрозы и риски безопасности общественных Wi-Fi сетей// Конкурентоспособность территорий. 2019. С. 95 – 97.

Смирнов В.М., Сушенцев А.С.
Влияние криптовалют на мир

Московский университет МВД имени В. Я. Кикотя
(Россия, Москва)

doi: 10.18411/lj-06-2021-70

Аннотация

В данной статье хотелось бы рассмотреть, как криптовалюта влияет на экономический статус всех страны мира. В последнее время криптовалюта идет наравне с другим платежным способом, таким как оплата наличными. Многие известные компании и многие известные личности уже давно используют криптовалюту в качестве основного вида платежа. Также в данной статье будет рассмотрено:

- 1) Влияние криптовалюты на весь мир.
- 2) Виды криптовалют.
- 3) Методы добычи криптовалюты и законность данных методов.
- 4) Киберпреступления, как следствие появления криптовалюты.

Ключевые слова: криптовалюта, биткоин, киберпреступления, криптовалюты, виды криптовалют.