ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.771

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ВЫХОДА В ИНТЕРНЕТ ПОСРЕДСТВОМ WI-FI РОУТЕРА

Нуждин Виктор Владимирович
Студент бакалавриата 4 курс, факультет «Сети и системы связи»
Кафедра «Сети и системы связи», Московский технический университет связи и информатики, Москва, Россия
e-mail: nuzhdinvictor2404@gmail.com

Томильченко Лев Русланович
Студент бакалавриата 4 курс, факультет «Сети и системы связи»
Кафедра «Сети и системы связи», Московский технический университет связи и информатики, Москва, Россия
e-mail: tomilchenko.lev@bk.ru

Чигрина Анастасия Сергеевна
Студент бакалавриата 4 курс, факультет «Сети и системы связи»
Кафедра «Сети и системы связи», Московский технический университет связи и информатики, Москва, Россия
e-mail: achigrina04@gmail.com

Аннотация

В данная статья посвящена обеспечению безопасности выхода в интернет посредством Wi-Fi роутера, поскольку совместное использование Wi-Fi сети с кучей незнакомых людей – не лучший способ сохранить пользовательские данные в тайне. В данной статье будут перечислены меры предосторожности при использовании бесплатной Wi-Fi сети, а также при предоставлении собственной.

Ключевые слова: Wi-Fi, VPN, пользователь, безопасность, защита, сеть, роутер.

ENSURING THE SECURITY OF ACCESS TO THE INTERNET VIA A WI-FI ROUTER

Victor V. Nuzhdin
Undergraduate student 4th year, Faculty of "Networks and Communication Systems" Department of "Networks and Communication Systems", Moscow Technical University of Communications and Informatics, Moscow, Russia

Lev R. Tomilchenko
Undergraduate student 4th year, Faculty of "Networks and Communication Systems" Department of "Networks and Communication Systems", Moscow Technical University of Communications and Informatics, Moscow, Russia

Anastasia S. Chigrina
Undergraduate student 4th year, Faculty of "Networks and Communication Systems" Department of "Networks and Communication Systems", Moscow Technical University of Communications and Informatics, Moscow, Russia

ABSTRACT

This article is devoted to ensuring the security of accessing the Internet via a Wi-Fi router, since sharing a Wi – Fi network with a bunch of strangers is not the best way to keep user data secret. This article will list the precautions when using a free Wi-Fi network, as well as when providing your own.

Keywords: Wi-Fi, VPN, user, security, protection, network, router

Введение.

Совместное использование сети Wi-Fi с кучей незнакомых людей - не лучший способ сохранить пользовательские данные в тайне. Принять необходимые меры предосторожности легко, когда пользователь использует свой ноутбук в бесплатном Wi-Fi кафе. Но если пользователь проживает в месте, где делится сетью со своими соседями, все начинает усложняться, поскольку за симпатичной внешностью людей могут стоять хакеры (рис. 1).

Рисунок 1. Раздача Wi-Fi

Многие многоквартирные дома связывают интернет-сервис с арендой, помещая всех в здании в единую, легкодоступную сеть. Иногда это открытые сети, к которым может

присоединиться любой желающий, с порталом, через который пользователь должен войти, чтобы получить доступ в интернет. В других случаях они используют стандартный пароль WPA2, как в обычной домашней сети. Некоторые арендодатели могут пойти дальше, например, они создают отдельные сети Wi-Fi для каждой квартиры—определенно предпочтительный вариант - но так как пользователь не может настроить их, то сети могут иметь легко угадываемые пароли или другие дыры в безопасности. Другими словами, если у пользователя нет контроля над сетью Wi-Fi, которую он использует дома, он может быть в опасности.

"Совместное использование сети Wi-Fi с неизвестными людьми, как правило, небезопасно", - говорит Эйприл К. Райт (https://ru.omatomeloanhikaku.com/secure-your-601) консультант по безопасности в компании ArchitectSecurity.org. Райт также сообщает, что в многоквартирном доме есть хорошие способы организовать подобную сеть, но пользователь может не догадываться, что сделал его домовладелец, поскольку будет большой удачей, если сеть организована качественно и безопасно. Есть также хороший шанс, что арендодатели даже не знают, каким образом организована сеть Интернет в их доме, поскольку это та работа, которая обычно передается на аутсорсинг.

Что еще хуже, у пользователя может не быть возможности получить свой собственный отдельный интернет-план: кабельная компания может иметь дело со всем зданием. И если арендная плата очень выгодна, а квартира хорошая, трудно отказаться от отличного места для жизни только из-за Wi-Fi.

К счастью, даже если у пользователя нет контроля над Wi-Fi, есть несколько вещей, которые он может сделать, чтобы обезопасить себя от кражи либо потери данных.

"Отделение сети Wi-Fi здания от домашней сети — это идеальная конфигурация для защиты домашних устройств", - объясняет Райт. "Для этого требуется, чтобы беспроводной мост был задействован как брандмауэр между внешними и внутренними сетями." Есть несколько способов сделать это, но лучшие варианты требуют, чтобы у пользователя был свой собственный, персональный Wi-Fi маршрутизатор.

Если у пользователя есть физический доступ к маршрутизатору здания (или порт Ethernet в его квартире, который подключается к маршрутизатору здания), он может просто подключить WAN-порт своего персонального маршрутизатора к одному из портов локальной сети на маршрутизаторе здания с помощью кабеля Ethernet. Затем пользователю необходимо настроить свою собственную сеть Wi-Fi с ПК.

Если у пользователя нет возможности подключиться напрямую, необходимо купить Wi-Fi роутер, затем подключить его к собственному зданию Wi-Fi в "клиентском режиме" с помощью веб-интерфейса, а затем соединить WAN-порт собственного персонального маршрутизатора с портом Ethernet Wi-FI роутера.

Установка маршрутизатора между собственными устройствами и остальной частью Wi-Fi здания пользователя может защитить его от любого вредоносного ПО, которое его сосед неосознанно загрузил.

В обоих этих сценариях персональный маршрутизатор пользователя в основном видит сеть здания как интернет, позволяя ему создать свою собственную сеть Wi-Fi, как и в любом другом доме или квартире. Пользователь управляет сетью в своей квартире, и в то время, как он сможет видеть устройства других жильцов здания, они не смогут видеть его - только его маршрутизатор.

Это самая большая часть головоломки, так как маршрутизатор будет выполнять преобразование сетевых адресов (NAT), действуя как своего рода брандмауэр между пользователем и остальной частью здания.

"Использование VPN всякий раз, когда вы подключены к сети Wi-Fi (даже на работе), является обязательным на телефонах и компьютерах", - говорит Райт. "Программное обеспечение VPN должно блокировать пользовательский доступ в интернет, пока оно не подключено к VPN. Пользователь может проверить некоторые из любимых VPN и узнать, как настроить один из них на своем телефоне, используя это руководство. Кроме того, если роутер поддерживает эту функцию, пользователь может настроить VPN непосредственно на нем - таким образом, весь пользовательский исходящий трафик шифруется, включая устройства, такие как smart TV, которые могут не иметь своих собственных средств шифрования.

Наконец, необходимо использовать многофакторную аутентификацию для всех своих учетных записей в интернете, настроить гостевую сеть для всех, кто посещает дом (не выдавайте пароль для домашней сети), и убедиться, что брандмауэры, встроенные в Windows и macOS, активны в любое время. Чем больше этих советов пользователь сможет реализовать, тем лучше для него - создание собственной сети Wi-Fi с вышеупомянутым мостом может помочь, но пользователю также нужны хорошие повседневные методы безопасности. Как говорит Райт: «Конечные устройства не должны полагаться исключительно на сетевую защиту, а сеть не должна полагаться исключительно на защиту конечных устройств».

Список литературы.

1. Защита в сетях Wi-Fi. Date Views 04.09.2021 ru.wikipedia.org/wiki/Защита_в_сетях_Wi-Fi.

2. 7 советов по настройке домашнего Wi-Fi-роутера. Date Views 09.09.2021 www.kaspersky.ru/blog/how-to-setup-wi-fi-router/6403/.

3. Симонов С Аудит безопасности информационных систем // Get Info. 1999. №9(76).

4. Гордейчик С. В., Дубровин В. В., Безопасность беспроводных сетей. Горячая линия — Телеком, 2008.

5. 802,11i-2004 — IEEE Standard for Local and Metropolitan Area Networks — Specific requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

References.

1. Protection in Wi-Fi networks. Date Views 04.09.2021 ru.wikipedia.org/wiki/Защита_в_сетях_Wi-Fi

2. 7 tips for setting up a home Wi-Fi router. Date Views 09.09.2021 www.kaspersky.ru/blog/how-to-setup-wi-fi-router/6403 /.

3. Simonov With Information Systems Security Audit // Get Info. 1999. №9(76).

4. Gordeychik S. V., Dubrovin V. V., Security of wireless networks. Hotline - Telecom, 2008.

5. 802.11i-2004 - IEEE Standard for Local and Metropolitan Area Networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.