МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ВСЕРОССИЙСКАЯ ГРУППА ТЕОРИИ ИНФОРМАЦИИ IEEE
АКАДЕМИЯ ИНФОРМАТИЗАЦИИ ОБРАЗОВАНИЯ
ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ООО «ОТКРЫТЫЕ РЕШЕНИЯ»
ОБЩЕСТВО «ЗНАНИЕ» РОССИИ
ПРИВОЛЖСКИЙ ДОМ ЗНАНИЙ

XXII Международная
научно-техническая конференция

ПРОБЛЕМЫ ИНФОРМАТИКИ В ОБРАЗОВАНИИ, УПРАВЛЕНИИ, ЭКОНОМИКЕ И ТЕХНИКЕ

Сборник статей

Декабрь 2022 г.

Пенза

УДК 004
ББК 32.81я43+74.263.2+65.050.2я43
П781

П781 **ПРОБЛЕМЫ ИНФОРМАТИКИ В ОБРАЗОВАНИИ, УПРАВЛЕНИИ, ЭКОНОМИКЕ И ТЕХНИКЕ :**
сборник статей XXII Международной научно-технической конференции. – Пенза: Приволжский Дом знаний, 2022. – 356 с.

ISBN 978-5-8356-1800-2
ISSN 2311-0406

Под редакцией ***В.И. Горбаченко,*** доктора технических наук, профессора;
В.В. Дрождина, кандидата технических наук, профессора

Информация об опубликованных статьях предоставлена в систему Российского индекса научного цитирования (РИНЦ) по договору № 573-03/2014К от 18.03.2014.

ISBN 978-5-8356-1800-2
ISSN 2311-0406

XXII International
scientific and technical conference

PROBLEMS OF INFORMATICS IN EDUCATION, MANAGEMENT, ECONOMICS AND TECHNICS

December, 2022

Penza

политическое развитие России в условиях глобализации и цифровизации: сборник статей по материалам Международной научно-практической очной конференции. – Пенза: Пензенский государственный университет, 2022. – С. 7-12.

7. Абрамова, Т. А. Характеристики актуальных угроз безопасности веб-приложений / Т. А. Абрамова, С. Н. Катков, Д. А. Голдуева, А. Г. Петренко // Управление и экономика: исследование и разработка : сборник статей VI Международной научно-практической конференции. – Пенза: АННОО «Приволжский Дом знаний», 2021. – С. 131-135.

Галактионова Божена Андреевна
Катков Сергей Николаевич
Пензенский государственный университет,
г. Пенза, Россия

GalaktionovaB.A.
Katkov S.N.
PenzaStateUniversity,
Penza, Russia

УДК 004.7

СПОСОБЫ ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ В ИНТЕРНЕТЕ

Р.Р. Гатин, В.В. Лебедев, Ю.Н. Матвеев

METHODS OF ANONYMITY ON THE INTERNET

R.R. Gatin, V.V. Lebedev, Y.N. Matveev

Аннотация. В статье рассматриваются способы, с помощью которых можно стать анонимным в Интернете.

Ключевые слова: прокси-сервер, сети Интернет, IP-адрес, идентификация, VPN.

Abstract. The article discusses the ways in which you can become anonymous on the Internet.

Key words: proxy server, internet networks, IP address, identification, VPN.

Каждый пользователь Интернета хоть раз задумывался о том, чтобы стать скрытным в сети. Анонимность в сети Интернет призвана обеспечить конфиденциальность, защиту персональных сведений, снижение контроля

за своей личной жизнью. Для этого существует два способа: прокси-серверы, VPN.

Прокси-сервер. Прокси – это промежуточный сервер между пользователем Интернета и серверами, откуда запрашивается информация. Прокси меняет ваш IP-адрес и местоположение, из-за чего сложно отследить, кто делает запрос.

Рис. 1. Иллюстрация работы прокси-сервера

Достоинства:

1. Вы скрываете свой IP-адрес при базовой проверке;
2. Используя прокси-серверы, вы скрываете свое географическое положение. Сайты и сервисы, которые вы посещаете, видят только местоположение прокси-сервера;
3. Прокси-серверы могут повысить вашу безопасность путем блокирования сайтов, распространяющих вредоносное программное обеспечение. Они также могут проверять контент на наличие вредоносных элементов перед его отправкой на ваш компьютер;
4. Прокси-серверы могут быть использованы для доступа к географически ограниченным сервисам;
5. В интернете есть много открытых бесплатных прокси-серверов, и некоторые из них предоставляют разнообразные полезные услуги.

Недостатки:

1. Прокси-серверы не шифруют ваш интернет-трафик;
2. Ни ваш IP-адрес, ни ваше реальное местоположение не скрыто от более продвинутых методов обнаружения.
3. При использовании прокси-сервера ваш интернет-трафик проходит через него. Это означает, что вредоносный прокси-сервер может видеть и контролировать все, что вы делаете в интернете.
4. Прокси-серверы, как правило, отслеживают и фиксируют действия своих пользователей. В определенных случаях это может иметь негативные последствия;
5. Многие бесплатные прокси-серверы являются ненадёжными, а некоторые вредоносными.

VPN. VPN (англ. Virtual Private Network – виртуальная частная сеть) – это безопасное зашифрованное подключение пользователя к сети, с которым он может обходить локальные ограничения и сохранять конфиденциальность.

Чтобы подключиться к VPN, достаточно установить нужное мобильное приложение и активировать эту функцию.

Когда пользователь заходит в сеть, его устройству присваивается уникальный IP-адрес. Он позволяет третьим лицам идентифицировать его и шпионить – смотреть, какие сайты он открывает, какую информацию ищет в поисковиках, что покупает и так далее.

При активации VPN оригинальный IP-адрес становится не виден. Вместо него отображается адрес виртуальной частной сети.

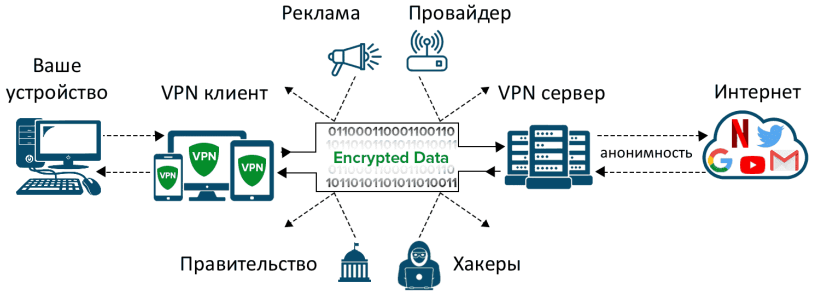

Рис. 2. Иллюстрация работы VPN

Достоинства:

1. Ваш личный трафик шифруется и безопасно передается через интернет. Это защитит вас от множества интернет-угроз
2. Если вы используете VPN-сервис, то хакерам становится крайне сложно получить доступ к вашим данным и переписке
3. Вы можете пользоваться общедоступными точками доступа WiFi, не беспокоясь на счет хакеров, вы также сможете безопасно подключаться к любым удаленным серверам.
4. Высокий уровень защиты приблизит вас к возможности по-настоящему анонимной работы в сети.

Недостатки:

1. VPN-серверы должны шифровать весь трафик, который проходит через них, и это может сказаться на производительности и скорости;
2. При подключении к VPN-серверу каждый бит данных между вами и сервером шифруется. Тем не менее, эти данные расшифровываются на сервере VPN, поэтому он знает, что вы делаете в интернете. Очень важно,

чтобы провайдеры VPN не хранили логи деятельности пользователей. В противном случае провайдер VPN будет знать, что вы делаете. Эти данные могут быть использованы другими организациями, которые получают санкционированный или несанкционированный доступ к ним;

3. Надежные VPN-сервисы, как правило, стоят дороже, чем хороший прокси-сервер. Шифрование всего трафика означает, что VPN-сервер должен иметь мощное аппаратное обеспечение.

Виртуальные частные сети лучше, чем прокси-серверы практически во всех аспектах. Виртуальные частные сети лучше в плане анонимности и безопасности. Все, что вы делаете в интернете, используя VPN-сервис, шифруется, и никто не может контролировать или отслеживать ваши действия. Единственным серьезным недостатком является то, что виртуальные частные сети стоят гораздо дороже, чем прокси-серверы.

Если все, что вам нужно, это скрыть свой IP-адрес или реальное местоположение от сайта или интернет-сервиса, который выполняет только базовую проверку, тогда используйте прокси сервер для локальных подключений. Если вам нужна анонимность, безопасность и конфиденциальность, в таком случае следует воспользоваться VPN. Тем не менее, проверьте, что выбранный вами сервис не хранит логи вашей деятельности.

Библиографический список

1. Когда использовать прокси-сервер, а когда VPN? – URL: https://www.internet-technologies.ru/articles/newbie/kogda-ispolzovat-proksi-server-a-kogda-vpn.html

2. Преимущества и недостатки VPN (всё, что вы должны знать). – URL: https://www.cactusvpn.com/ru/vpn/vpn-advantages-disadvantages/

3. Достоинства и недостатки прокси. – URL: https://socproxy.ru/blog/post/plyusy-i-minusy-proksi

4. Плюсы и Минусы Использования VPN в 2022 году. – URL: https://ru.wizcase.com/blog/плюсы-и-минусы-vpn/

Гатин
Роман Ренатович
Лебедев
Владимир Владимирович
Матвеев Юрий Николаевич
Тверской государственный
технический университет,
г. Тверь, Россия

Gatin R.R.
Lebedev V.V.
Matveev Y.N.
Tver State Technical University,
Tver, Russia