СПОСОБЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ

*Карпов Д.С., Ибрагимова З.А.**

***Ключевые слова**: анонимность, анонимизация, DarkNet, шифрование, метаданные, прокси-сервер, VPN, SSL-сертификат, TOR, интернет-сервис.*

Аннотация.

Цель исследования: анализ и обоснование причин, по которым пользователи стремятся обеспечить свою анонимность в Интернете, выявление субъектов, решающих задачи деанонимизации пользователей, определение наиболее эффективных способов и средств обеспечения анонимности в Интернете.

Методы и материалы. Использовались: результаты научных исследований в области анонимизации действий пользователей в Интернете, опубликованные в открытых источниках, включая результаты авторов; материалы, полученные авторами в ходе планирования, подготовки и проведения лабораторных и практических занятий со студентами, обучающимися по направлению подготовки «Информационная безопасность»; комплексный анализ и материалы исследований в данной предметной области.

Результаты: научное исследование и обоснование причин, по которым пользователи стремятся обеспечить свою анонимность в Интернете; определение субъектов, решающих задачи деанонимизации пользователей в Интернете; определение наиболее эффективных и часто используемых способов и средств обеспечения анонимности в Интернете.

Полученные результаты могут быть использованы для совершенствования научной и методической базы исследований в сфере информационной безопасности в областях, связанных с обеспечением анонимности и деанонимизации пользователей глобальной сети Интернет.

DOI: 10.21681/1994-1404-2021-3-60-67

Под *анонимностью* в сети Интернет можно понимать отсутствие личных данных о пользователях. На сегодняшний день существует множество причин, по которым пользователи хотят скрывать свои данные. Это стремление полностью защититься от возможных противоправных действий со стороны третьих лиц, осуществление противоправных действий в Интернете (например, *Internet scam*), доступ к *DarkNet* и др.

Есть и иные причины, по которым пользователи стремятся к своей анонимности, это, в частности:

Свобода выражения мнения. Многие боятся говорить то, что они действительно думают, поэтому прячутся за своим ником в социальной сети. Кто-то даже создает по несколько аккаунтов, что помогает им общаться так открыто, как они никогда не смогли бы в реальной жизни.

Конфиденциальность. Многие не хотят, чтобы другие что-то знали об их личной жизни, но рассказать о ней хочется. Поэтому они могут создавать аккаунты от другого имени и скрываться за ником.

Низкая самооценка. Многие в Интернете совсем не такие, какие в жизни. Они часто боятся показаться глупыми, нелепыми. Пытаются сохранить свою анонимность, ведь так они смогут обрести полную свободу, быть собой, не стесняться, что другие воспримут их странными.

Возможность решать «деликатные» вопросы анонимно. Есть еще одна важная категория людей, которые извлекают выгоду из анонимности — это те, кому нужно больше информации по какой-то теме, но они не хотят, чтобы их поймали на поиске этой информации.

Стеснение. Почти каждому человеку присуще стеснение. Кто-то просто не хочет, чтобы другие знали, что это именно он выставил какой-то текст или фотографию. Они не готовы рассказать всем о своих симпатиях, взглядах на жизнь, поэтому и пытаются спрятаться за всевозможными аккаунтами.

Злость. К сожалению, вымещение злости и ненависти на людей — одна из причин, по которой люди действуют анонимно. Такие люди хотят вылить грязь на других, не неся при этом за это ответственности. Они

* ***Карпов Дмитрий Сергеевич,*** *кандидат технических наук, доцент, доцент Российского экономического университета им. Г. В. Плеханова, г. Москва, Российская Федерация.*
E-mail: kds-zn@mail.ru

Ибрагимова Заира Анзоровна, *студент Российского экономического университета им. Г. В. Плеханова, г. Москва, Российская Федерация.*
E-mail: z.ibragimova.z02@mail.ru

запугивают других, выражают свою ненависть, хамят, сквернословят и делают это анонимно и безнаказанно.

Самовыражение. В Интернете легко «самовыражаться». Далеко не всем нужна слава и пиар, и многие пытаются сохранить анонимность из нежелания, чтобы все знали, что какое-то произведение создали именно они.

В глобальной сети за пользователями могут следить такие субъекты, как интернет-провайдеры, государственные органы, владельцы интернет-сервисов и даже иностранные специальные службы (например, проект *Prism*[1] АНБ США). Отслеживание интернет-провайдерами — это практика, с помощью которой интернет-провайдеры записывают информацию об онлайн-подключениях и действиях. Это означает, что все — от истории поиска до переписки по электронной почте — отслеживается и регистрируется интернет-провайдером. Он может видеть онлайн-поиски, незашифрованную переписку по электронной почте, данные социальных сетей; пароли и информацию, которую вводят на незашифрованных веб-сайтах; информацию о сайтах, на которые заходят пользователи; о файлах/торрентах, которые они скачивают; криптовалютные транзакции; географическое местоположение при использовании мобильных устройств.

Хотя провайдер не всегда отслеживает интернет-активность пользователя, у него в центре обработки данных есть сервер, куда «зеркалируется» определенный трафик — сервер системы оперативно-розыскных мероприятий (СОРМ)[2]. Владельцы сервисов также следят за пользователями. Необходимо быть осторожным при использовании *Google Mail* в качестве рабочей/личной почты или браузера *Chrome*. Ведь в этом случае *Google* будет очень удобно и легко собирать информацию. Это касается и российских сервисов, например, ЯндексКрипта[3], *VK* и др.

Для обеспечения анонимности пользователю нужно стараться не использовать реальные имена/фамилии/даты рождения. В разных сервисах нужно использовать разные пароли. Иначе если взломают одно — взломают все. Пользователь должен заводить несколько аккаунтов с разными никами и разным типом активности. При получении письма от сайта с паролем в открытом виде важно понимать, что это ненадежный сайт, поскольку он хранит пароль пользователя в незашифрованном виде. Так пароль может быть продан либо украден. Нельзя забывать переходить в режим инкогнито[4] при регистрации, входе на важные сайты, а при необходимости передачи секретных данных по открытому каналу связи выполнять предварительное шифрование с помощью *PGP*. Пользователь также может разбить информацию на части и передать их по разным каналам. Например, пароль сказать при встрече, логин в *Telegram*, адрес отправить в *Instagram*. Регистрация и совершение входа в сервис пользователем должны происходить только в случае, если есть *https*. При регистрации или входе обязательно использование *VPN* (*virtual private network*). Так пользователь не засветит свой *IP*-адрес. Перед тем как выложить очередное фото в Интернет, важно проверить, не осталось ли там деанонимизирующих метаданных.

Метаданные фотографий — это информация, которая часто бывает полезной, однако опасной для тех, кто хочет обеспечить максимальную анонимность. Так называемые данные *EXIF* доступны для каждой фотографии независимо от того, с какого устройства она была сделана. Они рассказывают, как было создано изображение, где и когда. Они могут рассказать о параметрах камеры/смартфона. Они также показывают, как изображение было отредактировано в редакторе. Информацию о владельце кадра и не только может узнать любой желающий, потратив на это всего несколько минут.

По данным лаборатории Касперского[5] *Facebook*, *eBay*, *Instagram*, *Twitter*, *Craigslist*, *ВКонтакте* метаданные из фотографий удаляют; *Flickr, Google Photo, Google+, Tumblr,* ЦИАН — не удаляют.

Чтобы не распространить личную информацию вместе с фотографией, пользователю необходимо отключить функцию геолокации для камеры, а прежде чем разместить свою фотографию в Интернете, удалить метаданные. Для этого можно использовать *XnView*, потому что встроенный механизм *Windows* «Удаление свойств и личной информации» оставляет под контролем как миниатюру, так и блоки *EXIF*. Необходимо также запретить сохранение метаданных в настройках конфиденциальности сервисов. Однако если пользователю действительно есть что терять, лучше не публиковать то, что может сыграть против него в будущем.

Говоря об анонимности в Интернете, не стоит забывать о правильной настройке браузера. Есть несколько простых правил. *Во-первых*, нельзя сохранять свои пароли в браузере, необходимо заходить и регистрироваться в различных сервисах только через режим инкогнито. *Во-вторых*, браузер не должен устанавливать связь между пользовательскими файлами *cookie*/паролями/историей браузера и любой другой инфор-

[1] Проект *PRISM*. URL: https://www.securitylab.ru/news/tags/PRISM (дата обращения: 29.07.2021).

[2] Приказ Минкомсвязи России от 16 апреля 2014 г. № 83 (ред. от 15.04.2019) «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий» // Демоверсия СПС «КонсультантПлюс» (дата обращения: 29.05.2021).

[3] Ресурс ЯндексКрипта основан на методе машинного обучения и анализирует характерное поведение пользователей в Интернете. Для удачного исследования достаточно проанализировать поведение не менее 30 000 пользователей.

[4] Режим «инкогнито» в браузерах — это специальный режим, при котором не сохраняется история просмотров, загрузок и др.

[5] Эксперимент: проверяем, что интересного можно узнать из метаданных фотографий в Интернете. URL: https://www.kaspersky.ru/blog/exif-privacy/13506 (дата обращения: 29.05.2021).

мацией с неизвестными серверами в сети. *В-третьих*, браузер не должен сохранять *cookie* при перезапусках.

Для безопасной передачи файла пользователю необходимо использовать шифрование, например, *GPG* или *PGP*. *PGP* (*Pretty Good Privacy*) — система шифрования, используемая как для отправки зашифрованных писем, так и для шифрования конфиденциальных файлов. При отправке письма или файла, которые были зашифрованы и подписаны с помощью *PGP*, пользователь может быть уверен, что письмо не поддельное, и только получатель, указанный отправителем, сможет его прочитать. Таким образом, даже если почта будет взломана, злоумышленник не сможет получить доступ к электронным письмам и файлам.

Для шифрования любого файла с помощью *GPG* пользователю необходимо использовать команду «*gpg-c file*». Система дважды запросит пароль, и после шифрования рядом с пользовательским исходным файлом появится новый с расширением *.gpg*, например, 1.*gpg*. Для того чтобы расшифровать отправленный файл, необходимо воспользоваться командой «*gpg file*», потом ввести пароль и получить исходный файл. Однако у *gpg* шифрования есть свой недостаток: помимо передаваемых файлов и писем нужно передавать пароль. Поэтому гарантий того, что его не перехватит злоумышленник, нет. Эту проблему решает *асимметричная криптография* [11]. Она использует частные и открытые ключи для шифрования/дешифрования данных. Открытый ключ — один из ключей в паре, который может быть общим для всех, тогда как закрытый ключ — ключ в паре, который хранится в секрете. Хотя *открытый* ключ доступен каждому, *закрытый* ключ, необходимый для расшифровки данных, сохраняется у владельца.

Но что бы ни делал пользователь, если он все еще использует календарь *Google*, сохраняет свою переписку в почте Яндекса или хранит файлы в *Dropbox*, он не добьется своей анонимности. Чтобы интернет-серверы не могли следить за пользователем, необходимо навсегда ограничить их использование. Заменой *Dropbox* можно считать довольно много приложений с открытым исходным кодом (*open source*): *Seafile*, *OwnCloud*, *Sparkleshare*, *Pydio*.

Также важно построить защищенную операционную систему (ОС) на компьютере. Для этого необходимо перейти на *Linux* или другую ОС с открытым исходным кодом[6], использовать шифрование дисковых разделов и всегда создавать криптостойкий пароль (будет еще лучше, если аутентификация будет проходить по отпечатку пальца [14]).

Если пользователь хочет обеспечить свою анонимность при использовании телефона, ему необходимо: заменить стандартную прошивку *Android* на *Replicant/Cyanogenmod/Paranoid Android*, всегда использовать шифрование файловой системы и *VPN* для доступа в Интернет, переключиться с *Google Play* на *F-Droid*. Также необходимо использовать «длинный» криптографический пароль и следить за активностью телефона (при помощи приложения-трекера для слежения за своим телефоном онлайн, например, *Self-Hosted GPS Tracker* для Андроид).

В обеспечении анонимности может помочь сервер синхронизации *Firefox*. Например, когда у пользователя есть файл, который находится в двух или более местах, и он хочет, чтобы файл был одинаковым везде и всегда, необходимо синхронизировать его. Это происходит с помощью механизма *синхронизации*. Когда что-то изменяется в этом файле, механизм синхронизации будет реплицировать изменения во всех местах, где есть файл.

Учетная запись *Firefox* позволяет синхронизировать данные, такие как закладки, история, пароли, открытые вкладки и установленные дополнения на всех устройствах. Можно отключить синхронизацию в любое время, также как и изменить список данных, которые пользователь хочет синхронизировать. Однако нельзя включать синхронизацию на чужих, а тем более общедоступных устройствах, необходимо использовать на них режим инкогнито.

Создание корневого *SSL*[7]-сертификата позволит веб-сайтам переходить с *HTTP* на *HTTPS*, что более безопасно. *SSL*-сертификат — это файл данных, размещенный на исходном сервере веб-сайта. *SSL*-сертификаты делают возможным шифрование *SSL/TLS* и содержат открытый ключ и удостоверение веб-сайта. Устройства, пытающиеся связаться с исходным сервером, будут ссылаться на этот файл, чтобы получить открытый ключ и проверить личность сервера. Закрытый ключ хранится в секрете и защищен.

Проведенный анализ опубликованных научных работ [3—10, 15, 20, 21] в области анонимизации пользователей глобальной сети Интернет показал, что наиболее эффективными и часто используемыми в настоящее время являются такие способы обеспечения анонимности, как использование технологий *проксификации*, *VPN*, *Tor* и *I2P*, опирающихся на соответствующие программно-аппаратные средства. Рассмотрим их подробнее.

Если пользователь использует прокси-сервер [15], трафик проходит через него по пути к запрошенному адресу. Затем запрос возвращается через тот же прокси-сервер, а после прокси-сервер отправляет данные, полученные с веб-сайта. Возможно использование цепочек (каскадов) прокси-серверов (рис. 1).

[6] Анонимизация в Интернете и использование *self-hosted* сервисов. URL: https://habr.com/ru/post/237335 (дата обращения: 29.05.2021).

[7] *SSL* (*secure sockets layer* — уровень защищенных сокетов) — криптографический протокол для безопасной связи. С версии 3.0 *SSL* заменен на *TLS* (*transport layer security* — безопасность транспортного уровня), но название предыдущей версии прижилось, поэтому сегодня под *SSL* чаще всего подразумевают *TLS*. Любой веб-сайт с *https*-адресом использует *SSL/TLS*.

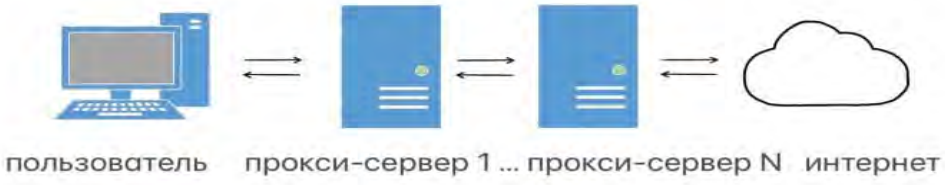

Рис. 1. Использование каскада прокси-серверов для анонимизации

Рис. 2. Использование технологии VPN для анонимизации

По обеспечению анонимности прокси-серверы можно разделить на *HTTP*-(веб)-прокси-серверы, *HTTPS*-(веб)-прокси-серверы, *SOCKS*[8]-прокси-серверы, *CGI*-прокси.

HTTP-(веб)-прокси-серверы — наиболее распространенный тип прокси, предназначенный в первую очередь для посещения веб-сайтов, загрузки и передачи файлов. Как следует из названия, прокси работают по протоколу *HTTP*, что позволяет быстро и эффективно работать с веб-страницами. *HTTPS*-прокси являются модификацией *HTTP*-прокси. Буква «*s*» в конце означает «безопасный». Такие прокси поддерживают шифрование данных для повышения безопасности данных в Интернете. Это достигается с помощью криптографических протоколов *SSL* и *TLS*. У *SOCKS*-прокси-серверов самый универсальный протокол, когда дело доходит до прокси-серверов. Эти прокси не передают никаких *HTTP*-заголовков, что делает их анонимными по умолчанию, скрывая реальный *IP*-адрес клиента и факт использования прокси. *CGI*-прокси — это веб-страница, которая схожа со страницами поисковых систем. Но вместо поисковых фраз в поле ввода пользователь вписывает *URL* того сайта, на который хочет перейти. После нажатия кнопки *Submit/Go* он автоматически попадает на страницу, *URL* которой указал.

Преимуществом прокси-серверов является то, что они очень дешевы, а иногда и вовсе бесплатны. Однако есть и свои *недостатки*: прокси-серверы используют данные кэша и могут запоминать всю личную информацию, включая пароли. Кроме того, нужно настраивать прокси-сервер под каждое приложение.

Технология *VPN* — это технология, которая создает логическую сеть поверх другой сети [2, 16—19]. *VPN* создает зашифрованный туннель между пользователем и удаленным сервером. Весь интернет-трафик направляется через этот туннель, так что пользовательские данные защищены от посторонних глаз на этом пути. Поскольку трафик выходит из *VPN*-сервера, истинный *IP*-адрес скрыт, маскируя личность и местоположение (рис. 2). В зависимости от применяемых протоколов и назначения, *VPN* поддерживает соединения трех видов: «клиент-клиент», «клиент-сеть» и «сеть-сеть». Говоря о *VPN*, не стоит забывать о *SSH*[9]-туннелях. Хотя между ними и есть различия, принцип работы у них очень схож.

Сейчас провайдерами предлагаются *PPTP*, *L2TP/IPSec*, *OpenVPN* и *SSTP* протоколы *VPN*. *PPTP* является наиболее широко используемым, быстрым, простым в настройке, однако устаревшим, отчего защита данных подвергается серьезному риску. У протокола *L2TP/IPSec* *L2TP* отвечает за транспорт, а *IPSec* за шифрование [13]. Используемые вместе *L2TP* и *IPSec* гораздо более безопасны, чем *PPTP*, но все же больше подходят для анонимизации [1], чем для обеспечения безопасности [12]. *OpenVPN* — это относительно новый и легко настраиваемый протокол. Самое лучшее в *OpenVPN* то, что он имеет открытый исходный код. В сочетании с сильным алгоритмом шифрования он является одним из самых безопасных доступных протоколов *VPN*, однако требует отдельного программного клиента. *SSTP* — это

[8] *SOCKS* (сокращение от «*SOCKet Secure*») — интернет-протокол, который используется для передачи пакетов с данными от сервера к клиенту с помощью промежуточного прокси-сервера. На сегодня это наиболее продвинутая массовая технология для организации прокси.

[9] *SSH* — сетевой протокол прикладного уровня, предназначенный для «туннелирования» сетевого трафика с использованием зашифрованного соединения.

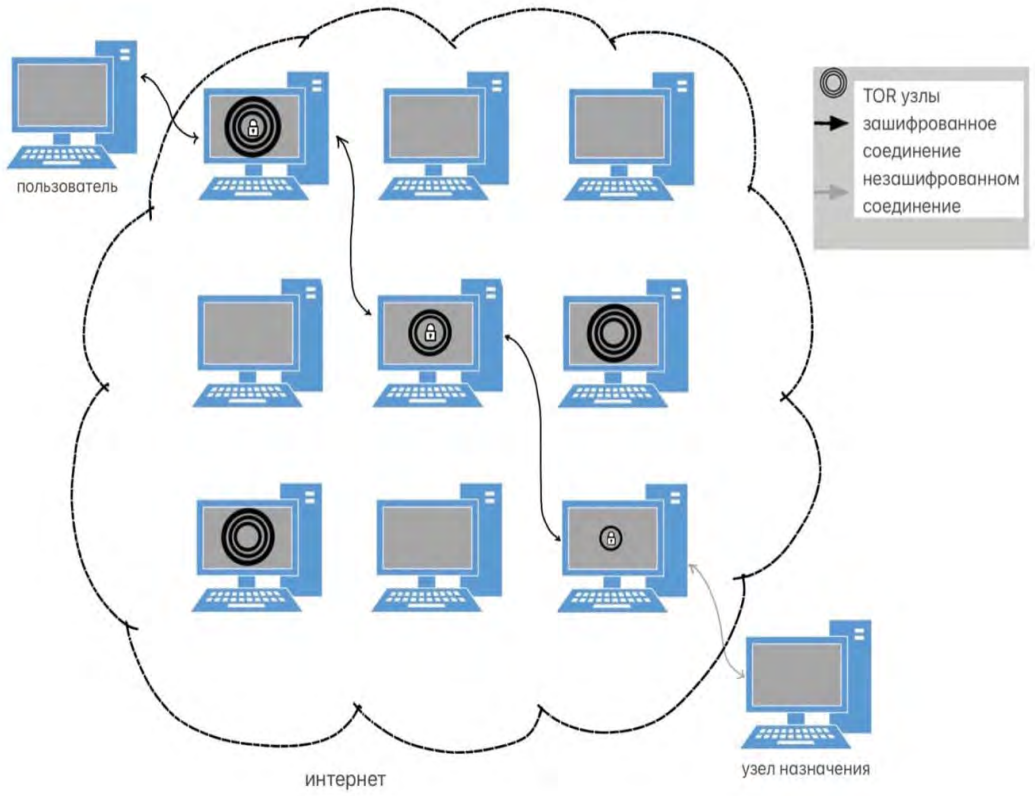

Рис. 3. Использование технологии TOR для анонимизации

VPN-протокол, который разработан *Microsoft*. Протокол предназначен для защиты данных и трафика и считается более безопасным, чем *PPTP* или *L2TP/IPSec*.

К преимуществам *VPN/SSH* относится то, что использовать их быстро и удобно, а также не требуется отдельная настройка приложений. Однако, как и в случае с прокси-серверами, нужно доверять *VPN/SSH*-серверу/провайдеру.

Когда пользователь подключается к *TOR*, его *исходящий* интернет-трафик перенаправляется через случайную серию, состоящую по крайней мере из трех узлов (ретрансляторов), прежде чем достичь места назначения (веб-сайта, который пользователь хочет посетить) [3, 5, 10]. Компьютер подключен к узлу входа; конечным узлом, через который проходит трафик, является узел выхода, после чего он достигает места назначения. *Входящий* трафик перенаправляется аналогичным образом. Помимо прохождения через несколько узлов, трафик многократно шифруется. Он теряет уровень шифрования на каждом узле, но никогда полностью не расшифровывается, пока не покинет выходной узел для назначения (рис. 3). *TOR* решает главную задачу: довольно-таки высокий уровень анонимности пользователя при передаче только *http*-трафика. Однако, как и все другие реально существующие анонимизирующие сети с малыми задержками, *TOR* не может защитить от глобального наблюдателя [4].

Преимущества *TOR* — обеспечение высокого уровня безопасности пользователя; любой пользователь может легко воспользоваться *TOR* , для этого достаточно скачать *TOR Browser Bundle*. Недостатки *TOR* — прослушивание выходного трафика, низкая скорость работы и наличие управляющих серверов.

I2P — это децентрализованная анонимизирующая сеть, построенная с использованием *Java* на тех же принципах, что и *TOR*, но изначально задуманная как автономный *DarkNet*.

В *I2P* есть два главных понятия:

- «туннель» — временный однонаправленный путь через некоторый список узлов;
- «сетевая база *NetDb*» — документирование группы точек входа в туннель (*leases*) для конкретного клиентского назначения, которая хранит в себе *RouterInfos* — контактная информация маршрутизатора (клиентов) и *LeaseSets* — контактная информация назначения.

Таким образом, определены причины, по которым пользователи стремятся обеспечить свою анонимность в сети Интернет, субъекты, решающие задачи деанонимизации пользователей в Интернете, наиболее эффективные и часто используемые способы и средства обеспечения анонимности в Интернете. Важно заметить, что ни один из приведенных способов не гарантирует полной анонимности, но их вполне достаточно, чтобы значительно усложнить задачу деанонимизации.

Полученные результаты можно использовать для совершенствования научной и методической базы исследований в сфере информационной безопасности в областях, связанных с обеспечением анонимности и деанонимизации пользователей глобальной сети Интернет.

Литература

1. Борисов Р.С., Ефименко А.А. Регламент обработки наборов данных для их публикации в открытых источниках // Правовая информатика. 2021. № 2. С. 59—70. DOI: 10.21681/1994-1404-2021-2-59-70 .
2. Карпов Д.С., Микрюков А.А., Козырев П.А. Повышение качества подготовки специалистов по направлению подготовки «Информационная безопасность» // Открытое образование. 2019. Т. 23. № 6. С. 22—29. DOI: 10.21686/1818-4243-2019-6-22-29 .
3. Карпов Д.С., Спивак А.И. Об одном способе воздействия на информационные ресурсы, имеющие выход в сеть Интернет // Труды Междунар. науч.-прак. конф. «Ценности и интересы современного общества». Часть 3: «Современные парадигмы информационных технологий в развитии общества» / МЭСИ. М. : МЭСИ, 2015. С. 88—93.
4. Карпов Д.С., Спивак А.И. Разработка модели угроз безопасности информации в системе информационного обмена на основе технологии анонимизации TOR // Труды XXXVII Всеросс. науч.-техн. конф. «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» / Филиал ВА РВСН. Серпухов : ФВА РВСН им. Петра Великого, 2018. С. 97—101.
5. Карпов Д.С., Спивак А.И. Использование технологий анонимизации трафика для воздействия на информационные ресурсы // Труды Междунар. науч.-прак. конф. «Актуальные задачи математического моделирования и информационных технологий» / Сочинский ГУ. Сочи : Соч. гос. ун-т, 2015. С. 93—97.
6. Карпов Д.С., Спивак А.И. Создание математической модели обеспечения достаточного уровня анонимности в системах передачи данных с сохранением целостности и конфиденциальности передаваемой информации // Проблемы обеспечения информационной безопасности в ВС РФ : сб. науч. тр. № 1. Краснодар : КВВУ, 2016. С. 133—143.
7. Карпов Д.С., Спивак А.И. Обеспечение достаточного уровня анонимности отправителя в распределенной компьютерной системе информационного обмена // «Известия» № 265 : науч.-техн. сб. Часть I «Перспективные АСУ и робототехнические комплексы военного назначения». Балашиха : ВА РВСН, 2016. С. 155—164.
8. Карпов Д.С., Спивак А.И. Разработка алгоритма анонимного обмена информацией в системах передачи данных с сохранением ее целостности и конфиденциальности // Проблемы обеспечения информационной безопасности в ВС РФ : сб. науч. тр. № 1. Краснодар : КВВУ, 2016. С. 112—121.
9. Карпов Д.С., Спивак А.И. Реализация способа обеспечения анонимности отправителя в информационно-телекоммуникационной сети международного информационного обмена // Труды Междунар. науч.-прак. конф. «Информационная безопасность: вчера, сегодня, завтра» / РГГУ. М. : РГГУ, 2018. С. 127—135.
10. Киселенко В.А. Анонимизация работы в глобальной компьютерной сети Internet // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2005. № 1. С. 43—51.
11. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : Рос. гос. ун-т правосудия, 2021. 276 с. ISBN 978-5-93916-896-0.
12. Ловцов Д.А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74.
13. Ловцов Д.А. Обеспечение информационной безопасности в российских телематических сетях // Информационное право. 2012. № 4. С. 3—7.
14. Ловцов Д.А., Князев К.В. Защищённая биометрическая идентификация в системах контроля доступа. I. Математические модели и алгоритмы // Информация и космос. 2013. № 1. С. 100—103.
15. Маркин Д.О., Архипов П.А., Галкин А.С. Исследование устойчивости анонимной сети на основе технологий веб-прокси // Вопросы кибербезопасности. 2016. № 2 (15). С. 21—27.
16. Наполова Е.И., Кожевников С.В. Защита компьютерных сетей на основе технологии virtual private network // Экономика и качество систем связи. 2018. № 2. С. 80—85.
17. Росляков А. Виртуальные частные сети VPN. Модели и методы анализа. LAP, 2011. 328 с.
18. Росляков А.В. Виртуальные частные сети: основы построения и применения : монография. М. : Эко-Трендз, 2006. 300 с.
19. Рябко Е.И. Калейдоскоп VPN-технологий // T-Comm. 2009. Спецвып. по ИБ. С. 16—20.
20. Сергеев С.М. Некоторые проблемы противодействия использованию в преступной деятельности средств обеспечения анонимизации пользователя в сети Интернет // Вестник СПб. ун-та МВД России. 2017. № 1 (73). С. 137—140.
21. Karpov D.S., Spivak A.I. The use of technology for traffic anonymization exposure to information resources // European Journal of Computer Science. 2015. № 1 (1). Pp. 34-40.

Рецензент: ***Марков Алексей Сергеевич,*** *доктор технических наук, старший научный сотрудник, генеральный директор НПО «Эшелон», профессор кафедры информационной безопасности МГТУ им. Э. Н. Баумана, г. Москва. E-mail: a.markov@bmstu.ru*

WAYS AND MEANS TO ENSURE ANONYMITY IN THE GLOBAL INTERNET NETWORK

Dmitrii Karpov, *Ph.D. (Technology), Associate Professor at the Plekhanov Russian University of Economics, Moscow, Russian Federation.*
E-mail: kds-zn@mail.ru

Zaira Ibragimova, *student at the Plekhanov Russian University of Economics, Moscow, Russian Federation.*
E-mail: z.ibragimova.z02@mail.ru

Keywords: *anonymity, anonymisation, DarkNet, encryption, metadata, proxy server, VPN, SSL certificate, TOR, Internet service.*

Abstract.

Purpose of the study: analysing and justificating the reasons why users seek to ensure their anonymity on the Internet, identifying subjects solving the tasks of deanonymising users, finding the most efficient ways and means of ensuring anonymity on the Internet.

Methods and materials used: results of research in the field of anonymisation of user actions on the Internet published in open sources, including the results obtained by the authors, materials obtained by the authors in the course of planning, preparing and carrying out laboratory and practical training of students studying in the subject of information security, multi-faceted analysis and materials of research in this subject area.

Results obtained: a research study and justification of reasons why users seek to ensure their anonymity on the Internet, identification of subjects solving the tasks of deanonymising users on the Internet, finding the most efficient and frequently used ways and means of anonymisation on the Internet.

The obtained results can be used to improve the research and methodological basis for research in the field of information security in areas related to anonymisation and deanonymisation of users in the global Internet network.

References

1. Borisov R.S., Efimenko A.A. Reglament obrabotki naborov dannykh dlia ikh publikatsii v otkrytykh istochnikakh. Pravovaia informatika, 2021, No. 2, pp. 59-70. DOI: 10.21681/1994-1404-2021-2-59-70 .
2. Karpov D.S., Mikriukov A.A., Kozyrev P.A. Povyshenie kachestva podgotovki spetsialistov po napravleniiu podgotovki "Informatsionnaia bezopasnost'". Otkrytoe obrazovanie, 2019, t. 23, No. 6, pp. 22-29. DOI: 10.21686/1818-4243-2019-6-22-29 .
3. Karpov D.S., Spivak A.I. Ob odnom sposobe vozdeistviia na informatsionnye resursy, imeiushchie vykhod v set' Internet. Trudy Mezhdunar. nauch.-prak. konf. "Tsennosti i interesy sovremennogo obshchestva". Chast' 3: "Sovremennye paradigmy informatsionnykh tekhnologii v razvitii obshchestva", MESI. M. : MESI, 2015, pp. 88-93.
4. Karpov D.S., Spivak A.I. Razrabotka modeli ugroz bezopasnosti informatsii v sisteme informatsionnogo obmena na osnove tekhnologii anonimizatsii TOR. Trudy XXXVII Vseross. nauch.-tekhn. konf. "Problemy effektivnosti i bezopasnosti funktsionirovaniia slozhnykh tekhnicheskikh i informatsionnykh sistem", filial VA RVSN. Serpukhov : FVA RVSN im. Petra Velikogo, 2018, pp. 97-101.
5. Karpov D.S., Spivak A.I. Ispol'zovanie tekhnologii anonimizatsii trafika dlia vozdeistviia na informatsionnye resursy. Trudy Mezhdunar. nauch.-prak. konf. "Aktual'nye zadachi matematicheskogo modelirovaniia i informatsionnykh tekhnologii", Sochinskii GU. Sochi : Soch. gos. un-t, 2015, pp. 93-97.
6. Karpov D.S., Spivak A.I. Sozdanie matematicheskoi modeli obespecheniia dostatochnogo urovnia anonimnosti v sistemakh peredachi dannykh s sokhraneniem tselostnosti i konfidentsial'nosti peredavaemoi informatsii. Problemy obespecheniia informatsionnoi bezopasnosti v VS RF : sb. nauch. tr. No. 1. Krasnodar : KVVU, 2016, pp. 133-143.
7. Karpov D.S., Spivak A.I. Obespechenie dostatochnogo urovnia anonimnosti otpravitelia v raspredelennoi komp'iuternoi sisteme informatsionnogo obmena. "Izvestiia" No. 265 : nauch.-tekhn. sb. Chast' I "Perspektivnye ASU i robototekhnicheskie kompleksy voennogo naznacheniia". Balashikha : VA RVSN, 2016, pp. 155-164.
8. Karpov D.S., Spivak A.I. Razrabotka algoritma anonimnogo obmena informatsiei v sistemakh peredachi dannykh s sokhraneniem ee tselostnosti i konfidentsial'nosti. Problemy obespecheniia informatsionnoi bezopasnosti v VS RF : sb. nauch. tr. No. 1. Krasnodar : KVVU, 2016, pp. 112-121.
9. Karpov D.S., Spivak A.I. Realizatsiia sposoba obespecheniia anonimnosti otpravitelia v informatsionno-telekommunikatsionnoi seti mezhdunarodnogo informatsionnogo obmena. Trudy Mezhdunar. nauch.-prak. konf. "Informatsionnaia bezopasnost': vchera, segodnia, zavtra", RGGU. M. : RGGU, 2018, pp. 127-135.

10. Kiselenko V.A. Anonimizatsiia raboty v global'noi komp'iuternoi seti Internet. Vestnik MGTU im. N.E. Baumana, ser. "Priborostroenie", 2005, No. 1, pp. 43-51.
11. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : Ros. gos. un-t pravosudiia, 2021. 276 s. ISBN 978-5-93916-896-0.
12. Lovtsov D.A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66-74.
13. Lovtsov D.A. Obespechenie informatsionnoi bezopasnosti v rossiiskikh telematicheskikh setiakh. Informatsionnoe pravo, 2012, No. 4, pp. 3-7.
14. Lovtsov D.A., Kniazev K.V. Zashchishchennaia biometricheskaia identifikatsiia v sistemakh kontrolia dostupa. I. Matematicheskie modeli i algoritmy. Informatsiia i kosmos, 2013, No. 1, pp. 100-103.
15. Markin D.O., Arkhipov P.A., Galkin A.S. Issledovanie ustoichivosti anonimnoi seti na osnove tekhnologii veb-proksi. Voprosy kiberbezopasnosti, 2016, No. 2 (15), pp. 21-27.
16. Napolova E.I., Kozhevnikov S.V. Zashchita komp'iuternykh setei na osnove tekhnologii virtual private network. Ekonomika i kachestvo sistem sviazi, 2018, No. 2, pp. 80-85.
17. Rosliakov A. Virtual'nye chastnye seti VPN. Modeli i metody analiza. LAP, 2011. 328 s.
18. Rosliakov A.V. Virtual'nye chastnye seti: osnovy postroeniia i primeneniia : monografiia. M. : Eko-Trendz, 2006. 300 s.
19. Riabko E.I. Kaleidoskop VPN-tekhnologii. T-Comm, 2009, spetsvyp. po IB, pp. 16-20.
20. Sergeev S.M. Nekotorye problemy protivodeistviia ispol'zovaniiu v prestupnoi deiatel'nosti sredstv obespecheniia anonimizatsii pol'zovatelia v seti Internet. Vestnik SPb. un-ta MVD Rossii, 2017, No. 1 (73), pp. 137-140.
21. Karpov D.S., Spivak A.I. The use of technology for traffic anonymization exposure to information resources. European Journal of Computer Science, 2015, No. 1 (1), pp. 34-40.