Метод защиты трафика от вмешательства DPI-информационных систем вузов на базе использование DOH и DOT протоколов

Владимир Владимирович Фигурчиков
студент
Московский Политехнический университет
Москва, Россия
Soufigurch@gmail.com
0000-0000-0000-0000

Гамзат Абдуллаевич Салихов
студент
Национальный исследовательский университет ИТМО
Москва, Россия
Salihhhhhh@mail.ru
0000-0000-0000-0000

Ксения Олеговна Блохина
студент
Национальный исследовательский университет ИТМО
Москва, Россия
kseniablokhina99@gmail.com
0000-0000-0000-0000

Идель Фаритович Хакимов
студент
Уфимский государственный авиационный технический университет
Уфа, Россия
idel2000xf@gmail.com
0000-0000-0000-0000

Алина Руслановна Хакимова
студент
Российский государственный аграрный университет — МСХА им. К. А. Тимирязева
Москва, Россия
Aruahaxxx@ya.ru
0000-0000-0000-0000

Поступила в редакцию 27.04.2022
Принята 26.05.2022
Опубликована 20.06.2022

10.25726/d7888-7143-4235-q

Аннотация

Вопрос обеспечения информационной безопасности и конфиденциальности пользователей в интернете очень многогранен и сложен. С одной стороны, глобальная сеть становится все более защищенной: ведущие ИТ-компании мира разрабатывают и активно внедряют новые сетевые стандарты и протоколы, что делает Интернет более безопасным, быстрым и эффективным как для обычных среднестатистических пользователей, так и для корпоративных клиентов. Первые получают

возможность в любой момент времени быстро получить доступ к необходимой информации или ресурсам для удовлетворения собственных потребностей. Корпорации же, в свою очередь, благодаря разного рода статистическим данным имеют возможность более четко и эффективно планировать свои бизнес-процессы, коррелируя их с потребностями клиентов. С другой стороны, такая глобализация и структуризация информационных процессов имеет и негативные последствия. На основе данных, собираемых ИТ корпорациями и провайдерами можно полностью скомпрометировать не только отдельно взятого человека, но и крупные предприятия. Поэтому проблема защиты персональных данных в Интернете обостряется с каждым годом, ведь чем более доступной и распространенной становится глобальная сеть, тем меньше шансов на сохранение анонимности остается у среднестатистических пользователей, а конфиденциальные данные разного рода компаний и организаций становятся более уязвимыми для несанкционированного доступа к ним, нарушения их целостности и доступности. Системы DPI все чаще используются для контроля и фильтрации трафика, а также для блокировки протоколов.

Ключевые слова
информационная безопасность, взлом, кибер-атака, DPI.

Введение

Анализ последних исследований и публикаций. Как и в книге (Антонова, 2020), в данной статье рассматриваются и анализируются общие принципы применения DPI систем с целью контроля и фильтрации трафика в современных компьютерных системах и сетях. Анализ отчетов и публикаций о выявленных уязвимостях современных сетевых протоколов, а особенно протокола DNS дают понять дальнейшие направления усовершенствования обеспечения безопасности информационной системы (Восканян, 2018; Глобальное, 2021; Гусева, 2021).

В публикациях (Астахова , 2013; Бузальская , 2018; Восканян , 2018; Глобальное 6 2021; Гусева , 2021; Лабзова , 2017; Логинова , 2021) представлены направления решения проблем сетевого протокола DNS с использованием процедур шифрования, но данные подходы в полной мере не обеспечивают конфиденциальность информации при ее передаче по открытым компьютерных системах и сетях. Это приводит к перехвату и спуфингу трафика. Авторами в данной работе будут более детально проанализированы и систематизированы методы обеспечения конфиденциальности информации при ее передаче в открытом виде в современных компьютерных системах и сетях.

Учитывая анализ последних исследований и публикаций, актуальным является вопрос защиты сетевого трафика от вмешательства DPI систем, принцип действия которого основывается на исследовании уязвимых мест стандартов, а именно DNS-запросов с учетом особенностей функционирования типовых сетевых протоколов, с которыми имеет дело большинство пользователей сети Интернет.

Под понятием DPI система будем понимать такую систему, которая выполняет, так называемый, глубокий анализ сетевых пакетов на верхних уровнях модели OSI. Традиционный анализ пакетов обычно проверяет информацию в заголовках пакетов сетевого и транспортного уровней, DPI направлен также на поведенческий анализ трафика прикладного уровня в режиме реального времени, то есть такой, что позволяет распознавать пользовательские программы, для которых заранее не определено известные заголовки протоколов и структуры данных (Антонова , 2020; Астахова , 2013; Бузальская , 2018; Восканян, 2018; Глобальное , 2021).

Материалы и методы исследования

Выделяют два вида подключения DPI:

1. Пассивный. Система подключена параллельно к сети провайдера с помощью сплиттера (разделитель сигнала) либо с использованием зеркалирования трафика. Так как DPI обычно работает в режиме реального времени, то такой тип подключения не будет узким местом при большом объеме трафика. Но такой тип подключения не имеет возможности сразу пресечь попытку получения доступа к

запрещенным ресурсам, но только выявить ее. Хотя есть возможность подделки ответа от сайта провайдером с помощью подмены IP-адреса отправителя и структуры TCP пакета.

2. Активный. Система, подключенная к сети провайдера напрямую, как и другие сетевые устройства.

Провайдер или администратор системы настраивает DPI систему, будто файервол, на проверку различных типов трафика (входящего, исходящего или обоих одновременно), а система на базе различных правил принимает решение о блокировке трафика или его пропуск.

DPI был разработан для использования в следующих ситуациях:

1. Блокирование сетевых ресурсов. Одно из главных направлений использования этих систем с целью недопущения пользователей к пользованию определенными ресурсами и чаще всего используется в комплексных системах вместе с системами хранения всего трафика.

2. Оптимизация и приоритизация. Улучшение качества обслуживания для конечных абонентов провайдер может достичь либо путем увеличения собственной ширины канала, или оптимизировав трафик, например, снизив или увеличив приоритет определенных протоколов во время повышенной нагрузки на сеть, которое обычно бывает прогнозируемое и привязано к временным рамкам.

3. Построение поведенческой модели абонента. Так как все люди уникальны, то их поведение как в жизни, так и в сети отличается. Провайдер может собирать информацию, когда и кто выходит в онлайн, какими приложениями пользуется и какие сайты посещает, что позволяет создать некий цифровой отпечаток пользователя и использовать его для оптимизации в своих целях или продавать третьим лицам.

4. Защита. Так как DPI системы могут анализировать протоколы и сигнатуры трафика или выявлять его аномалии, это позволяет строить решения, которые предотвращают атаки типа ddos, а также использоваться в IPS (Intrusion Prevention System – система предотвращения вторжений) для обнаружения атак в реальном времени.

5. Кэширование. Для более оптимального использования интернет трафика и увеличение скорости доступа к часто используем информации (контента популярных сайтов, обновления или интересных файлов) настраивают кэш серверы.

Обычно оборудование для систем DPI похоже на обычные серверы размером 1U для монтирования, где главную роль в аппаратных характеристиках играет сетевая составляющая, например, наличие специального режима для сетевых интерфейсов, что позволяет соединять их на самом низком уровне OSI – физическом и в случае проблем с системой продолжать пропускать трафик без его полной остановки, и скорость обработки (особенно важно для активного подключение) с возможностью распараллеливания задач. А для организации кэширования или хранения статистики пользования или вообще всего трафика к системе может быть подключена внешняя система хранения данных.

Крупнейшими поставщиками аппаратной реализации DPI является Cisco, Sandvine, Procera Networks и Allot Communications, а также стремительно набирают популярность интегрированные возможности в маршрутизаторы, производителями и поставщиками такой продукции являются Cisco, Ubiquiti и Juniper. Кроме аппаратных решений существуют также и программные, которые предоставляются на бесплатной и платных основах. Наиболее популярными и развитыми проектами, которые распространяются на безвозмездной основе являются: - ndpi-продолжение развития уже неподдерживаемой библиотеки opendpi компанией ntop, является проектом с открытым исходным кодом и распространяется по лицензии lgplv3.

Поддерживает более 200 протоколов и позволяет определять протоколы приложений прикладного уровня, анализируя характер сетевой активности без привязки к определенным портам, а также позволяет просматривать зашифрованный трафик с помощью MITM; - joy – программный продукт компании Cisco, который лицензируется под свободной лицензией BSD и основан на пакете libpcap с возможностью захвата трафика в режиме реального времени, используя потоко-ориентированную модель и предоставляя результаты в удобном формате JSON.

Результаты и обсуждение

При использовании DPI могут возникнуть следующие проблемы:

Уязвимость к ddos атак: хотя DPI и помогает противостоять атакам такого типа, но при неправильной конфигурации преступники, наоборот, могут использовать особенности системы для создания подобных атак;

Повышение сложности управления сетью: в дополнение к настройкам межсетевого экрана нужно правильно настроить DPI, а также проводить работы с политиками для повышения эффективности;

Необходимость прослушивать трафик в обоих направлениях: для детектирования трафика, обычно основанного на эвристической модели, DPI система должна иметь доступ к обоим типам трафика для наиболее точного детектирования.

Среди блокировок, использующих DPI системы при перехвате и фильтрации трафика можно выделить: подмена DNS-ответов; перенаправление обращений к сторонним DNS-серверов на серверы, принадлежащие провайдеру; блокировка за IP-адресом; блокировка всех поддоменов заблокированного домена; фильтрация URL на отдельных или всех IP-адресах и/или портах; подмена SSL сертификата для прослушивания HTTPS-трафика (Лабзова , 2017; Логинова , 2021; Мартынова , 2006; Моргун , 2020; Найок , 2020).

Использование особенностей протоколов для обхода DPI

Используя особенности протоколов можно выделить такие способы обхода DPI-блокировок: добавление пробелов или других символов табуляции между методом HTTP (GET, POST и т. п) и URI; смешения букв регистра значение заголовка хоста; удалить пробел между названием заголовка и значением в заголовке хоста; фрагментация на уровня TCP для первого пакета данных; фрагментация на уровне TCP для постоянных сеансов HTTP; отправка поддельных пакетов HTTP с низким значением времени жизни или неправильной контрольной суммой. Таким образом в данном разделе исследованы теоретические возможности использования DPI систем до прослушивания и перехвата DNS трафика. Далее рассмотрим проблемы и возможные подходы по обеспечению защиты DNS трафика.

Современный веб и некоторые другие сетевые протоколы защищены с помощью TLS, но DNS запросы всю свою историю передают в незашифрованном виде. Компании или государства используют это в своих интересах, например, для сбора информации о посещаемые сайты или фильтрации трафика или даже проводить атаки на DNS трафик, так называемый спуфинг запросов с целью перенаправления их на собственный сервер. Даже использование защищенных VPN туннелей не дает стопроцентную гарантию защиты, так как в рамках этой сессии могут использоваться запросы DNS, которые могут отправляться за пределами туннеля и приводить к утечке DNS информации.

DNS проектировался для использования распределенными высоконагруженными сетями доставки контента и не обеспечивает на сегодня достойного уровня защиты трафика пользователей. Это привело к появлению некоторых векторов атак:

– спуфинг DNS запросов: подмена настоящего IP-адреса в кэше сервера вредоносной с целью установления соединения с сервером злоумышленника;

– перехват DNS запросов: перенаправление на вредоносные сайты или с целью сбора статистики и показа рекламы;

– перевязка DNS: установление контроля над сервером, который обслуживает вредоносный домен, с последующей загрузкой и выполнением скриптов в приложении пользователя при посещении других сервисов.

В рамках расширения функций DNS было предложено использование DNSSEC-протокола цифровой подписи DNS записей. При использовании этого подхода к определенным типам записей прилагается подпись, который позволяет рекурсивным резолверам установить, действительно ли именно владелец домена создал эту запись. Данное расширение не использует шифрование, лишь подтверждая подлинность записи, а все DNS-запросы передаются в открытом виде, как и ранее (Астахова , 2013; Бузальская , 2018; Восканян , 2018; Глобальное , 2021; Гусева , 2021). Таким образом, подобные расширение никак не используют шифрование данных, и, соответственно, не решают проблему конфиденциальности информации, передаваемой во время выполнения DNS-запросов, чем и

пользуются, например, производители DPI оборудования, провайдеры, злоумышленники и государственные органы, так как подобные логи с серверов позволяют создать некий цифровой отпечаток пользователя.

Поэтому с целью решения проблемы шифрования DNS предлагаются такие протоколы (Бузальская, 2018; Восканян, 2018; Глобальное, 2021): dnscrypt; DNS-over-TLS (dot); DNS-over-HTTPS (doh); DNS-over-SSH (dos); DNS-over-QUIC (doq).

Dnscrypt является древнейшей попыткой имплементации защиты DNS запросов. Он аутентифицирует связь между DNS клиентом и DNS-резолвером, предотвращает некоторым видам атак и использует криптографические подписи для проверки ответа. К сожалению, хотя и существует достаточно большое количество серверов, которые реализуют поддержку этого протокола, но поддержка для конечных устройств так и не получила широкого распространения, для мобильных клиентов требуется установка дополнительного программного обеспечения, а для мобильных – права суперпользователя. В то же время самым современным протоколом является DNS-over-QUIC, но он, вместе с другими протоколами, на которые он полагается, находятся только на начальной стадии, а их спецификации часто обновляются, чтобы можно было целесообразно имплементировать поддержку для конечных устройств. DNS-overSSH базируется на одном из наиболее часто используемых протоколов прикладного уровня – SSH (Secure Shell – безопасная оболочка), который по умолчанию использует шифрование без использования TLS, но требует TCP. Реализация DNS, работающий на базе SSH приводит к созданию двойного TCP, то есть TCP over TCP, что приводит к значительному снижению быстродействия, а также сложности синхронизации и гарантии доставки.

Согласно проведенного анализа авторами предлагается использование сочетанных методов dot и doh, которые позволяют сразу, без внедрения новых протоколов, с обеспечением обратной совместимости реализовать защищенную передачу трафика. Первый метод большее распространение приобретает на мобильных устройствах, например, входит в реализации Android 9. В то же время второй метод более широкое распространение получил в системах, уже реализуют использование HTTPS, например, браузеры. В данном разделе были рассмотрены наиболее значимые аспекты работы сети, основные понятия и принципы ее построения, обнаружено до сих пор уязвимые места определенных протоколов, а именно, DNS, который базируется на протоколе UDP и не полагается на использование криптографических алгоритмов. Этим пользуются поставщики услуг, государства и злоумышленники в своих целях, используя некоторые схемы атак, а также оборудование DPI. Таким образом, далее будет показан усовершенствованный подход по сокрытию данных, до сих пор передаваемых в открытом виде в сети Интернет, на базе внедрения криптографических методов.

Как можно видеть, этот процесс является рекурсивным: сначала запрос попадает на локальный DNS-резолвер, что может обслуживаться на рабочей станции, дальше, так как, обычно рабочие станции находятся за NAT, то есть за маршрутизатором, то последний отвечает за перенаправление запроса, а также может выступать в роли локального кэширующего DNS-сервера при соответствующих настройках, далее маршрутизатор перенаправляет запрос на некоторый публичный сервер, например, Интернет провайдера или другой компании, обслуживающей соответствующие решения. Если сервер не может найти у себя нужный ответ, запрос будет передан следующему серверу, вплоть до корневого. Как было указано в первом разделе, DPI оборудование обычно устанавливается, в соответствии с текущей схемой, на третьем шаге, и, в соответствии с оригинальной спецификацией DNS-весь трафик на пути своего следования передается в открытом виде.

Согласно поставленной цели, авторы считают целесообразным разработку такого метода доставки DNS запросов к доверенных резолверов, который бы обеспечил конфиденциальность данных, передаваемых и сделал невозможным или существенно затруднило выявление этого типа трафика DPI системами.

Авторы предлагают разработку полноценного локального проксирующего сервера, который может обращаться к доверенным публичным DNS резолюторам с помощью протоколов doh и dot. Практическая ценность полученных результатов в данной статье заключается в программной реализации методов защиты трафика от вмешательства DPI систем в среде Visual Studio Code за счет

использования языка программирования Python 3.8, что позволило обеспечить криптографическую защиту трафика. С практической точки зрения для понимания принципов взаимодействия предложенных протоколов авторы предлагают развернуть упрощенную локальную модель, которая состоит из: веб-сервера, сервера, отвечающего за сокрытие DNS запросов и локального DNS-сервера.

Предложенная авторами архитектура, представленная в виде собственного локального проксующего DNS серверу, который может отправлять DNS трафик хоста к вверенного публичного резолвера посредством формирования соответствующих запросов и получения ответов с поддержкой doh и dot. Таким образом данная реализация может быть использована для обеспечения криптографической защиты трафика, что обычно передается в открытом виде, между локальным устройством и доверенным публичным резолвером.

В качестве примера приводим элементы собственной реализации метода защиты трафика от вмешательства DPI систем на базе использования doh и dot и локального проксирующего DNS сервера. Пример реализован на Python 3.8:

```
@staticmethod
Def doh_resolver(dns_message, sender):
Ip, port, domain = parse_sender_dict(sender)
Doh = proto_senders.dohsender(ip, port, domain)
Return doh.query(dns_message)
@staticmethod
Def dot_resolver(dns_message, sender):
Ip, port, domain = parse_sender_dict(sender)
Dot = proto_senders.dotsender(ip, port, domain)
Return dot.query(dns_message)
@staticmethod
Def resolve_sender_ip(sender_address, bootstrap_ip, hosts_dict):
If sender_address in hosts_dict:
Return hosts_dict[sender_address]
Dns_query = dns.message.make_query(sender_address, dns.rdatatype.A) Response = dns.query.udp(dns_query, bootstrap_ip)
If response.answer:
Return response.answer[-1].items[0].to_text()
```

Для проведения тестирования корректности авторской разработки используются программный интерфейс на языке Python, утилита curl или веб-браузер, а для эмуляции DPI используется программа Wireshark для просмотра интернет-пакетов.

Основным элементом имплементации локальной архитектуры, отражающий возможность защиты DNS-трафика является внедрение сервера, который реализует шифрование этого типа трафика (doh и dot сервер) и выступает в роли прокси сервера между приложением, которое поддерживает генерирование запроса в нужном формате-с одной стороны, а с другой – непосредственно DNS сервером.

Авторская программа запускается посредством вызова файла main.py через интерпретатор с указанием параметром типа защищенного подключения к публичному резолвера.

Так как защищенное соединение предполагает использование доменных имен, то для первого запроса резолвинга адреса сервера, куда будут поступать защищены запросы, используется, так называемая, bootstrap адрес, то есть адрес также DNS-сервера, но в виде IP адреса. Также программа позволяет выбирать домены, для которых не нужно использовать защищенное соединение, обычно, это будет полезно для использования серверов синхронизации времени. Firefox и Google Chrome, которые могут использовать системную переменную SSLKEYLOGFILE, для того чтобы хранить ключи шифрования, которые можно будет использовать для дешифровки трафика. Сначала нужно запустить файл, содержащий следующую конфигурацию:

```
@echo off
```

```
Set SSLKEYLOGFILE=keylogfile.txt
Firefox.exe
```

Таким образом, все ключи шифрования будут храниться в указанный файл до тех пор, пока открыто окно браузера, в этом случае – Firefox. После записи трафика, для тестирования предложенного решения используем эмуляцию DPI, а именно программу Wireshark, которая будет использовать эти ключи для дешифровки трафика, что даст возможность убедиться в том, что запросы направляются на сервер cloudflare-dns.com, а также имеют соответствующую структуру и заголовки.

Последним тестом является перезапуск локального сервера в режим dot и захват трафика программой Wireshark. Как можно видеть, обмен трафиком происходит по адресу 1.1.1.1, так как на ней находится сервер компании cloudflare, обслуживающий Dot соединение, и портом 853, что соответствует описанной спецификации протокола.

Таким образом, данное тестирование позволяет утверждать, что весь DNS-трафик будет пересылаться через защищенный канал на местах, где возможно установка элементов DPI систем для прослушивания информации.

Заключение

В данной статье был проведен детальный анализ DPI системы и их основных компонентов, а также рассмотрены способы сокрытия информации от подобных систем, используя особенности протоколов и новых реализаций (Проценко, 2021). Принцип действия этих протоколов основывается на исследовании до сих пор уязвимых мест стандартов, а именно DNS-запросов с учетом особенностей функционирования типовых сетевых протоколов, с которыми имеет дело большинство пользователей сети Интернет. На базе этих исследований авторами достигнуты следующие результаты: рассмотрены и развернуть собственную локальную реализацию основных компонентов сети; исследован поток трафика от клиента к нужному ресурсу; проведен анализ взаимодействия протоколов с целью убеждения в том, что трафик между узлами с установленным оборудованием для фильтрации трафика является защищенным. Также был реализован собственный комплекс локального проксирующего сервера на языке программирования Python 3.8, и проведено его тестирование на реальной системе. Этот комплекс позволяет устанавливать защищенное соединение с другими доверенными серверами на базе использования протоколов doh и dot, и делает невозможным или значительно усложняет возможность использования DPI систем на границе обычных мест их установки. Несмотря на достижения цели работы практическая ценность этих решений является актуальной и необходимой для большинства пользователей и систем. Предложенное решение локального проксирующего сервера может быть развито и дальше (Семёнова, 2016).

Например, внедрены реализацию локального кэширования или добавлена возможность создавать более точные правила для определенных доменов и их поддоменов, а реализован тестовый doh сервер может быть развернут на вверенном выделенном сервере за пределами возможных точек установки фильтрующего оборудования, что позволит полностью контролировать собственный трафик для резолвинга доменных имен.

Список литературы

1. Антонова Д.А., Оспенникова Е.В. Методологические основы продуктивного обучения // Пед. образование в России. 2020. № 6. С. 163-173.
2. Астахова Л.В. Понятие информационной компетенции специалиста: когнитивный подход // Вестник ЮУрГУ. Серия «Образование. Педагогические науки». 2013. Т. 5. № 4. С. 10-16.
3. Бузальская Е.В. Тест-эссе как подвид академического эссе: характеристики жанра // Азимут научных исследований: педагогика и психология. 2018. Т. 7. № 1 (22). С. 39-42.
4. Восканян С.К. Эссе как жанр письменной речи: цели и задачи // Вестник Моск. ун-та. Серия 19 «Лингвистика и межкультурная коммуникация». 2018. № 2. С. 95-102.

5. Глобальное исследование «Доверие к цифровым технологиям» 2021. Кибербезопасность вступает в пору зрелости / РЖС. https://www.pwc.ru/ru/publications/dti-2021/e-version-digital-trust-insights-2021-in-russian.pdf

6. Гусева А.Х. Формат комментированной эссе-презентации как мотивационный ресурс подготовки итоговой аттестационной работы // Инновации. Наука. Образование. 2021. № 32. С. 2116-2121.

7. Лабзова И.Ю. Теория самоопределения и её применение в зарубежной образовательной практике // Человек и образование. 2017. № 3 (52). С. 152-156.

8. Логинова М.П. Философия американского образования: от истины до мнения // Вестник Православного Свято-Тихоновского гуманитарного университета. Серия 4 «Педагогика. Психология». 2021. № 60. С. 22-36.

9. Мартынова А.Г. Обучение академическому письменному дискурсу в жанре экспозиторного эссе: дис. ... канд. пед. наук. Омск, 2006. 207 с.

10. Моргун Е.А. Академический дискурс: эссе как жанр академического письма // Профессионально-ориентированное обучение языкам: реальность и перспективы: сб. ст. участников Ежегод. всерос. науч.-практ. конф. с междунар. участием. М., 2020. С. 260-265.

11. Найок О.Б. Средства смысловой целостности и прагматического воздействия в иллюстрированном эссе // Вестник Моск. гос. лингвист. ун-та. Гуманитарные науки. 2020. № 9 (838). С. 93-107.

12. Проценко А. Работодатели оценили уровень подготовки выпускников вузов //Рос. газ. 2021. https://rg.ru/2021/09/07/rabotodateli-ocenili-uroven-podgotovki-vypusknikov-vuzov.html

13. Семёнова Т.В. Проблемы организации продуктивной образовательной деятельности студентов вуза // Наука и образование: новое время. 2016. № 3. С. 99-103.

A method of protecting traffic from interference by DPI-information systems of universities based on the use of DOT and DOT protocols

Vladimir Vl. Figurchikov
student
Moscow Polytechnic University
Moscow, Russia
Soufigurch@gmail.com
0000-0000-0000-0000

Gamzat A. Salihov
student
ITMO National Research University
Moscow, Russia
Salihhhhhh@mail.ru
0000-0000-0000-0000

Kseniya O. Blohina
student
ITMO National Research University
Moscow, Russia
kseniablokhina99@gmail.com
0000-0000-0000-0000

Idel F. Hakimov
student
Ufa State Aviation Technical University
Ufa, Russia
idel2000xf@gmail.com
0000-0000-0000-0000

Alina R. Hakimova
student
Russian State Agrarian University — K. A. Timiryazev Agricultural Academy
Moscow, Russia
Aruahaxxx@ya.ru
0000-0000-0000-0000

Received 27.04.2022
Accepted 26.05.2022
Published 20.06.2022

10.25726/d7888-7143-4235-q

Abstract

The issue of ensuring information security and user privacy on the Internet is very multifaceted and complex. On the one hand, the global network is becoming more secure: the world's leading IT companies are developing and actively implementing new network standards and protocols, which makes the Internet safer, faster and more efficient for both ordinary average users and corporate clients. The former get the opportunity at any time to quickly access the necessary information or resources to meet their own needs. Corporations, in turn, thanks to various kinds of statistical data, have the opportunity to plan their business processes more clearly and efficiently, correlating them with the needs of customers. On the other hand, such globalization and structuring of information processes has negative consequences. Based on the data collected by IT corporations and providers, it is possible to completely compromise not only an individual, but also large enterprises. Therefore, the problem of protecting personal data on the Internet is becoming more acute every year, because the more accessible and widespread the global network becomes, the less chance of anonymity remains for average users, and confidential data of various companies and organizations become more vulnerable to unauthorized access to them, violation of their integrity and accessibility. DPI systems are increasingly being used to monitor and filter traffic, as well as to block protocols.

Keywords

information security, hacking, cyber attack, DPI.

References

1. Antonova D.A., Ospennikova E.V. Metodologicheskie osnovy produktivnogo obuchenija // Ped. obrazovanie v Rossii. 2020. № 6. S. 163-173.
2. Astahova L.V. Ponjatie informacionnoj kompetencii specialista: kognitivnyj podhod // Vestnik JuUrGU. Serija «Obrazovanie. Pedagogicheskie nauki». 2013. T. 5. № 4. S. 10-16.
3. Buzal'skaja E.V. Test-jesse kak podvid akademicheskogo jesse: harakteristiki zhanra // Azimut nauchnyh issledovanij: pedagogika i psihologija. 2018. T. 7. № 1 (22). S. 39-42.
4. Voskanjan S.K. Jesse kak zhanr pis'mennoj rechi: celi i zadachi // Vestnik Mosk. un-ta. Serija 19 «Lingvistika i mezhkul'turnaja kommunikacija». 2018. № 2. S. 95-102.

5. Global'noe issledovanie «Doverie k cifrovym tehnologijam» 2021. Kiberbezopasnost' vstupaet v poru zrelosti / RZhS. https://www.pwc.ru/ru/publications/dti-2021/e-version-digital-trust-insights-2021-in-russian.pdf

6. Guseva A.H. Format kommentirovannoj jesse-prezentacii kak motivacionnyj resurs podgotovki itogovoj attestacionnoj raboty // Innovacii. Nauka. Obrazovanie. 2021. № 32. S. 2116-2121.

7. Labzova I.Ju. Teorija samoopredelenija i ejo primenenie v zarubezhnoj obrazovatel'noj praktike // Chelovek i obrazovanie. 2017. № 3 (52). S. 152-156.

8. Loginova M.P. Filosofija amerikanskogo obrazovanija: ot istiny do mnenija // Vestnik Pravoslavnogo Svjato-Tihonovskogo gumanitarnogo universiteta. Serija 4 «Pedagogika. Psihologija». 2021. № 60. S. 22-36.

9. Martynova A.G. Obuchenie akademicheskomu pis'mennomu diskursu v zhanre jekspozitornogo jesse: dis. ... kand. ped. nauk. Omsk, 2006. 207 s.

10. Morgun E.A. Akademicheskij diskurs: jesse kak zhanr akademicheskogo pis'ma // Professional'no-orientirovannoe obuchenie jazykam: real'nost' i perspektivy: sb. st. uchastnikov Ezhegod. vseros. nauch.-prakt. konf. s mezhdunar. uchastiem. M., 2020. S. 260-265.

11. Najok O.B. Sredstva smyslovoj celostnosti i pragmaticheskogo vozdejstvija v illjustrirovannom jesse // Vestnik Mosk. gos. lingvist. un-ta. Gumanitarnye nauki. 2020. № 9 (838). S. 93-107.

12. Procenko A. Rabotodateli ocenili uroven' podgotovki vypusknikov vuzov //Ros. gaz. 2021. https://rg.ru/2021/09/07/rabotodateli-ocenili-uroven-podgotovki-vypusknikov-vuzov.html

13. Semjonova T.V. Problemy organizacii produktivnoj obrazovatel'noj dejatel'nosti studentov vuza // Nauka i obrazovanie: novoe vremja. 2016. № 3. C. 99-103.