# DEEP WEB – ГЛУБОКАЯ ПАУТИНА. ЧТО МЫ НЕ ЗНАЕМ ОБ ИНТЕРНЕТЕ ИЛИ ЧТО ОТ НАС ХОРОШО СКРЫВАЮТ

***Дворянкин Олег Александрович,***
*старший преподаватель кафедры информационной безопасности*
*Учебно-научного комплекса информационных технологий*
*Московского университета МВД России имени В.Я. Кикотя*
*кандидат юридических наук*

# DEEP WEB – HIDDEN WEB. WHAT WE DON'T KNOW ABOUT ON THE INTERNET OR WHAT IS WELL HIDDEN FROM US

***Oleg A. Dvoryankin,***
*candidate of legal sciences,*
*lecturer at the chair of information security of*
*the Moscow MUR RS Kikot university.*
DOI: 10.31618/nas.2413-5291.2021.1.71.471

**АННОТАЦИЯ**

В настоящей статье проведено изучение Глубокой паутины – «Deep Web». В работе исследованы особенности появления и распространения настоящей сети, рассмотрены положительные и отрицательные стороны, изучены такие вопросы, как: понятие, виды, формы и характеристики, а также проведено сравнение с сокрытым Интернетом и «черным Интернетом» (DarkNet) и предложены методы личной информационной безопасности.

**ABSTRACT**

In this article, the study of the Deep Web – "Deep Web" is carried out. The article examines the way how this network appeared and spread, considers its positive and negative sides, studies such issues as: the concept, types, forms and characteristics, as well as compares it with the hidden Internet and the "black Internet" (DarkNet) and suggests methods of personal information security.

**Ключевые слова.** Deep Web, Интернет, TOR, DarkNet, контент, информационная безопасность, информационные технологии, киберпространство, кибервойны.

**Keywords**. Deep Web, Internet, TOR, DarkNet, content, information security, information technologies, cyberspace, cyberwarfare.

В настоящее время Интернет (Глобальная сеть) стал неотъемлемой частью реальной жизни большинства современных людей.

Посредством сети Интернет человек каждый день удовлетворяет свои различные потребности: общение, образование, развлечение, занятие бизнесом и т.д.

Являясь виртуально изменённой и дополненной копией существующей действительности, Глобальная сеть впитала в себя как позитивные, так и негативные её проявления. К числу последних можно в первую очередь отнести преступность, которая в кратчайшие сроки взяла на вооружение новейшие информационные технологии. В результате возникли неизвестные до этого виды преступности: хакерство, кибертерроризм, киберэкстремизм, кибервойны, компьютерное мошенничество и другие виды киберпреступности. Поэтому остро встал вопрос о безопасности информационных систем (технологий) и личной информационной безопасности каждого человека осуществляющего свою деятельность в Интернете.

Однако при этом большинство людей даже и не подозревает, что сеть Интернет или Глобальная сеть – это только маленькая частичка всего интернет пространства или Глубокой паутины (Deep Web) с еще и «черным Интернетом» (Darknet).

В настоявшей работе рассмотрим «Deep Web» (Глубокую паутину).

Теневой, глубинный («hidden» перевод с англ. «скрытый») Интернет - «Deep Web» – многие специалисты даже не могут дать точное название и определение для этой части Интернета.

В этой связи эксперты «Deep Web» часто называют «Скрытым Интернетом», «Невидимая сеть», «Глубокая паутина» или «Глубокий Интернет».

История «Deep Web» началась с 1970-х годов, когда разрабатывалась сеть «ARPANet», созданная в 1969 году в США Агентством Министерства обороны США по «перспективным исследованиям» и явившаяся прототипом сети Интернет. Наибольшее распространение термин «Deep Web» получил после публикации работы «The Darknet and the Future of Content Distribution» в 2002 году, авторами которой являются Peter Biddle, Paul England, Marcus Peinado and Bryan Willman, сотрудники компании «Microsoft». [1].

В течение последних десятилетий Интернет, как отрытое пространство для общения, а вместо с ним и «Deep Web», стали переживать колоссальные перемены: модернизацию и развитие. Параллельно с этим образы Интернета и «Deep Web» стали отслеживаться в иных индустриях современного мира, таких как: книги, фильмы, компьютерные игры и т.д.

В фантастических американских блокбастерах киностудии Голливуда начали часто использовать различные сюжеты о параллельных мирах, при этом активно применяя информационные технологии Интернета и «Deep Web», чем активно вовлекая в информационные сети различных людей и пропагандируя среди них виртуальные технологии. А вот после выхода легендарной книги К. Шермана и Г. Прайса «Невидимый интернет», «Deep Web» стал легендой для компьютерщиков и просто манящим Эльдорадо как для конкурентных разведчиков, так и для аналитиков и исследователей [2].

В результате открытая часть Интернета и закрытая часть «Deep Web» стали развиваться на космических скоростях. В «гонку вооружения» включились все индустриальные и информационно-развитые страны мира, так как большинство руководителей стран поняли, что в настоящем, а тем более в будущем мировое влияние и контроль над обществом будет зависеть от доминирования в информационной среде (в сфере информационных технологий), где год идет за десять лет, а может и еще быстрее.

При этом одни страны и IT-компании сосредоточились на открытом Интернете, а другие серьезное внимание обратили и на скрытую часть Интернета «Deep Web» (стали проводить основательные разработки), которая занимает, по мнению экспертов, значительное количество виртуального пространства, в том числе поглощая Интернет, а также «Darknet» («черная сторона Интернета» или Даркнет).

Специалисты «Deep Web», так же по мнению исследователей, в ходе своей работы с Глубокой паутиной стараются лишний раз не афишировать свои разработки, а активно их применять на практике, так они очень часто связаны с деятельностью спецслужб и политический деятельностью.

Таким образом в настоящее время о наличии параллельного «Скрытого Интернета» или «Невидимой сети» сейчас мало кто знает, а ведь это не сюжет для очередного фильма или книги, а суровая действительность.

По сути, это та же Всемирная паутина, и в большинстве своем англоязычная, а для того, чтобы попасть туда, существуют специальные ключи и программы. Проникнуть туда можно только пользователю, который вооружен специальными знаниями и программами. И что самое тут неприглядное – с этой закрытой частью Интернета мало что могут сделать правоохранительные органы, как за рубежом, так и в России. А вот количество его пользователей стремительно растет изо дня в день, что пугает не только контролирующие Интернет органы, а даже правительства многих стран.

Глубокая сеть содержит в себе множество веб-страниц Всемирной паутины, не индексируемых поисковыми системами. Термин произошёл от соответствующего (англ. - invisible web.) Наиболее значительной частью Глубокой паутины является Глубинный веб (от англ. deep web, hidden web), состоящий из веб-страниц, динамически генерируемых по запросам к онлайн-базам данных. Не следует смешивать понятие «Глубокая паутина» с понятием «Тёмная паутина» (от англ. Dark web), под которым имеются в виду сетевые сегменты, хотя и подключённые к общей сети Интернет, но требующие для доступа определённые программные средства.

В Глубокой паутине находятся веб-страницы, не связанные с другими гиперссылками (например, тупиковые веб-страницы, динамически создаваемые скриптами на самих сайтах, по запросу, на которые не ведут прямые ссылки), а также сайты, доступ к которым открыт только для зарегистрированных пользователей и интернет-страницы, доступные только по паролю (рис. 1).

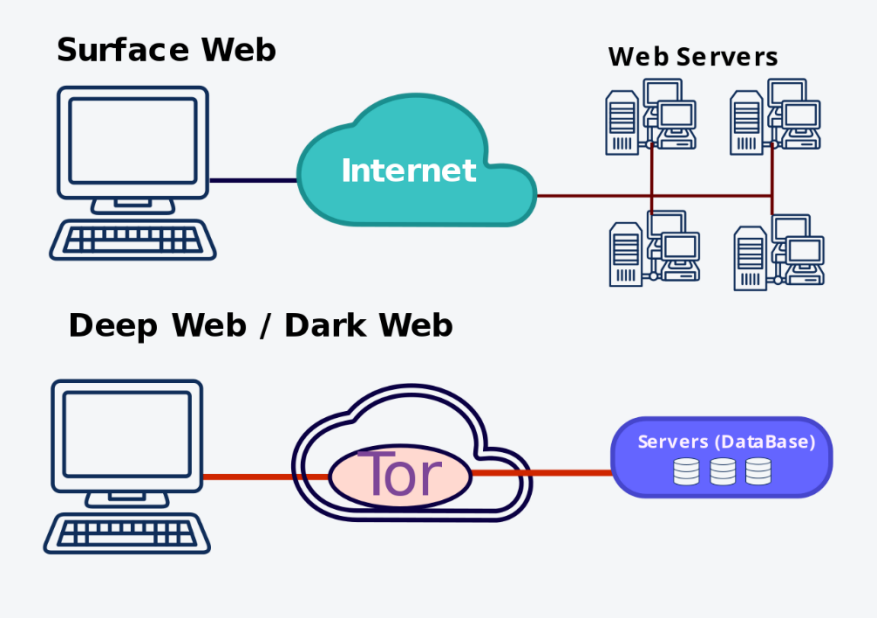


*Рис. 1. Пример видимой и невидимой сети*

Поисковые системы используют специальных поисковых роботов (ботов), которые переходят по гиперссылкам и индексируют содержимое веб-страниц, на которых они оказываются, занося их содержимое и гиперссылки на них в свои базы данных. Найдя на проиндексированной веб-странице ссылки на другие страницы, поисковый бот переходит по ним и индексирует содержимое каждой из найденных страниц, находит новые гиперссылки и переходит по ним для индексации; в результате переходов по ссылкам, ведущим за пределы индексируемых страниц, количество проиндексированных веб-страниц постоянно увеличивается. Попасть на веб-страницы, на которые нет ссылок с других страниц, поисковый бот не может, в силу чего содержимое этих страниц не индексируется. Как следствие, не зная URL сайта или веб-страницы «Глубокой сети», обычный пользователь попасть на них не сможет [3].

Так, одним из примеров технологий, позволяющих перейти на ресурсы Глубокой сети, является «Tor». («*Tor» — свободное и открытое программное обеспечение для реализации второго поколения так называемой луковой маршрутизации. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания.)*

«TOR» – это разработка американских военных, выпущенная в 2003 году.

Она использует так называемую «луковую» маршрутизацию, которая представляет собой технологию анонимного обмена информацией, осуществляемую через компьютерную сеть. Эта система, которая позволяет устанавливать анонимное сетевое соединение, защищённое от прослушивания.

Так сообщения несколько раз шифруются и отсылаются через несколько сетевых узлов, которые называются луковыми маршрутизаторами. Каждый маршрутизатор удаляет слой шифрования (будто луковый слой), чтобы открыть трассировочные инструкции и отследить последовательность выполнения команд, и отсылает сообщение на следующий маршрутизатор, где всё повторяется. Так, промежуточные узлы не знают ни источник, ни пункт назначения, ни содержание сообщения. Это лишь своеобразный портал в параллельный мир, мир уголовных элементов, запрещённых веществ, работорговли и секретных данных.

«TOR» также используется, по данным экспертов, для безопасного общения журналистов с информаторами и диссидентами. Юридические лица создают сайты для приёма компромата, для сбора информации о деятельности преступных структур и информации о злоупотреблениях чиновников.

Однако сеть «TOR» также является площадкой для развития теневой, преступной экономики. Именно поэтому наиболее часто звучащими обвинениями в её адрес является возможность её широкого использования для отмывания денег, компьютерного терроризма, незаконного оборота наркотиков, нелегального оборота оружием и организации хакерских атак и заказных убийств. С точки зрения поддержания безопасности Интернета «TOR» позволяет управлять программами-вымогателями и троянскими конями.

Сейчас «TOR» – это одно из самых лучших клиент-серверных приложений, использующих технологию анонимного обмена информацией. Суть этой технологии заключается в том, что изначально пакет подвергается многократному шифрованию и случайным образом распределяется между участниками сети, что позволяет с уверенностью сказать, что ни один из пользователей узловых машин не обладает полной информацией о передаваемых данных. Самым незащищенным местом в цепочке передачи является путь от отправителя пакета до первого сервера [4].

Также в «Глубокую сеть» попадают сайты, владельцы которых добровольно отказались от индексации поисковыми системами (например, с помощью файла «robots.txt»), а также сайты и веб-страницы, защищённые авторизацией от просмотра информации третьими лицами. В таком случае, не зная логин и (или) пароль к веб-странице, невозможно в полной мере просмотреть её содержимое или пользоваться веб-сайтом.

Однако по большей части, контент в «Глубоком Интернете» очень похож на контент на обычных сайтах, которые можно найти, например, в поисковой системе «Google».

«Deep Web» – это просто поиск контента, который, по мнению также разных экспертов, нельзя найти через обычную поисковую систему. К этому контенту относится, например, личная информация в вашей учетной записи в какой-нибудь социальной сети, ваши сообщения на электронной почте, закрытые страницы частных сайтов и т.д. То, что можно найти в поиске, называется «surface web», или «поверхностный Интернет». Отличия между поверхностным и глубоким Интернетом заключается в том, что некоторая защита препятствует к свободному доступу информации из «Deep Web», а к «surface web» может получить доступ любой пользователь.

Более 96% контента находящаяся в «Deep Web», т.е. это большая часть информации, к которой мы получаем доступ в Интернете только после аутентификации: банковский счет, электронная почта, аккаунт в социальной сети. Представьте только, если бы любой мог получить доступ к этой информации, просто погуглив ваше имя. В результате ваша личная информация была бы доступна всему миру. Веб-сайты не позволяют индексировать защищенные страницы, потому что лишь определенные лица должны иметь доступ к информации, размещенной на них. Хоть и не всегда возможно напрямую найти контент определенного веб-сервера, чтобы он мог быть проиндексирован, всё же можно получить доступ к такому сайту (из-за компьютерных уязвимостей) (рис. 2).

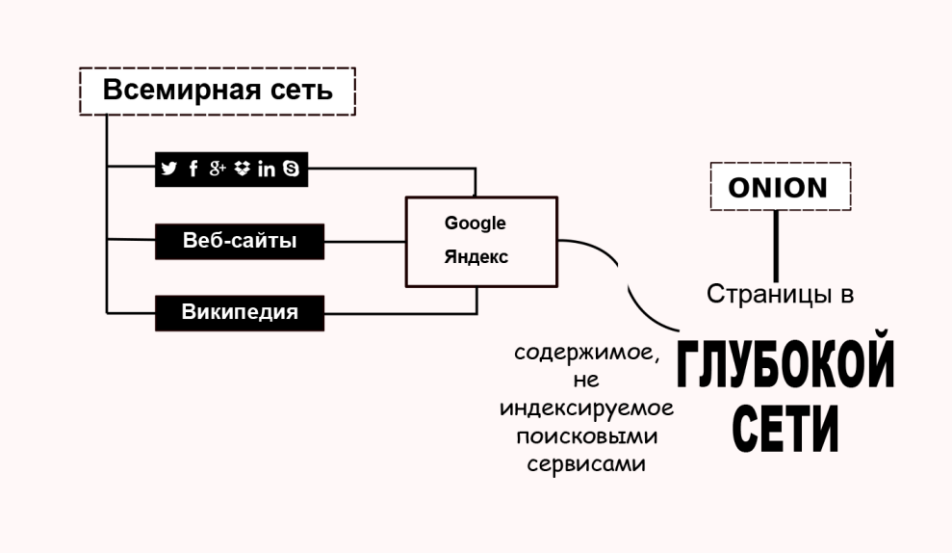


*Рис. 2. Пример неиндексируемого содержимого сети*

Чтобы обнаружить контент в Интернете, поисковые системы используют веб-сканеры, которые следуют за гиперссылками через известные номера виртуальных портов протокола. Этот метод идеально подходит для обнаружения контента во «Всемирной сети», но зачастую неэффективен при поиске контента «Глубокой сети». Например, поисковые роботы не ищут динамические страницы, которые являются результатом запросов к базе данных из-за неопределенного количества этих самых запросов. Такие действия могут быть (частично) преодолены путем предоставления ссылок на результаты запроса, но это может непреднамеренно раздуть популярность для члена «Глубокой сети» [5].

Существует несколько поисковых систем, которые получили доступ к «Глубокой сети».

Так, например, в 2001 году исследователи Стэнфордского университета (США) Шрирам Рагхаван и Гектор Гарсия-Молина представили архитектурную модель скрытой поисковой системы, которая использовала ключевые слова, предоставленные пользователями или собранные из интерфейсов запросов, для запроса и сканирования «Глубокого Интернета».

Таким образом, в результате деятельности этих и ряда других исследователей в данной сфере были разработаны протоколы и методы сканирования Глубокого интернета. Отмечу некоторые из них.

Коммерческие поисковые системы начали изучать альтернативные методы для сканирования «Глубокого Интернета». Протокол «Sitemap» (впервые разработанный и внедренный «Google» в 2005 году) и «mod_oai» — это механизмы, которые позволяют поисковым системам и другим заинтересованным сторонам обнаруживать ресурсы «Глубокого Интернета» на определенных веб-серверах. Оба механизма позволяют веб-серверам размещать на них доступные URL-адреса, что позволяет автоматически обнаруживать ресурсы, которые напрямую не связаны со «Всемирной сетью». Система навигации по «Глубокому Интернету» от «Google» вычисляет представления для каждой HTML-формы и добавляет полученные HTML-страницы в индекс поисковой системы «Google». Полученные результаты учитывают тысячу запросов в секунду для глубокого веб-контента. В этой системе предварительное вычисление представлений выполняется с использованием трех алгоритмов:

- выбор входных значений для текстового поиска, которые принимают ключевые слова;
- определённые входные данные, которые принимают только значения определенного типа (например, даты);
- выбор небольшого количества комбинаций ввода, которые генерируют URL-адреса, подходящие для включения в индекс поиска в Интернете.

При этом необходимо отметить, что у «Intute» прекратилось финансирование и теперь он является временным архивом по состоянию на июль 2011 года, а «Scirus» закрылся в конце января 2013 года.

Однако появились другие поисковые системы, которые в настоящее время применяются различными юзерами. Так, исследователи сообщили, в виде одного из вариантов, как можно автоматически сканировать «Глубокую паутину», включая контент, доступ к которому можно получить только с помощью специального программного обеспечения, такого как, например, «TOR».

С учетом изложенного, раз «Deep Web» является большим и живым организмом, в который просто так не войдешь, а если начнешь в нем работать, то потребуются особые навыки и в первую очередь – это анонимность.

Таким образом вопрос анонимности в Интернете или точнее в «Deep Web» становится не маловажным, а очень часто и основополагающим. Ведь как было отмечено выше: это персональные данные пользователя, поисковые системы, программы–шпионы, деятельность спецслужб и т. д. [6].

Исходя из этого возникает ряд вопросов, связанных с личной информационной безопасностью в «Deep Web»: «Анонимность в Интернете – норма или исключение? Что такое подлинная онлайн свобода? Как обеспечить безопасность в «Deep Web?»

Мнения экспертов по этому поводу существуют разные, но их собрав и обобщив, можно прийти к следующим положениям.

Так, например, видимо с коммерческой целью некоторые «специалисты» внушают наивным юзерам, что «Deep Web» один из последних «истинных бастионов свободы» в Интернете (эксперты говорят, что миф), а также что в данном киберпространстве существующие хакеры, которые могут забрать ваши персональные данные, но вам при этом ни чего плохого не сделают, в отличии интернет-поисковика «Google», который в автоматическом режиме собирает информацию о вас с каждым запросом.

При этом говорится, что «Google» знает о вас «все»: географическое местоположение компьютера (стационарного или мобильного), день рождения, размер вашей обуви, рецепт любимой пиццы и другие ваши вкусы и предпочтения.

При этом, также «специалисты» сообщают, что в отношении «комфортных» и «добропорядочных» обывателей-пользователей действуют интернет форумы, социальные медиа для того, чтобы незаконно применять в своих коварных целях персонализированную конфиденциальную информацию, чтобы потом манипулировать массовым сознанием благодаря изощренным современным схемам (информационным технологиям).

В результате создается ложное представление о «Deep Web». [7].

Однако несмотря на все это, «Deep Web» имеет некоторые достоинства и преимущества.

Необходимо отметить, что ссылки на страницы в «Глубоком Интернете» работают в особом формате «.onion», так что открыть их обычным браузером не получится. Для доступа в «Глубокую сеть» нужны, как было сказано выше, особые программы, сохраняющие анонимность пользователей и шифрующие трафик.

«Глубокий Интернет» — это единая сеть, скрытая от поисковых систем, а вот технологий Даркнета может быть несколько, и к каждой из них нужен особый доступ. Так, чтобы попасть в каждый из популярных даркнетов — «Freenet», «RetroShare» или др. - нужно установить отдельное программное обеспечение.

Причин для создания страниц в «Глубоком Интернете» или в одном из даркнетов может быть много. Главное преимущество закрытых сетей по сравнению с поверхностными, конечно, анонимность. Поэтому «Скрытый Интернет» нередко используют для незаконной деятельности.

«Глубокий интернет» и «Даркнет» получили дурную славу из-за того, что они часто используются преступниками. Тем не менее, нелегальная деятельность — не единственное применение скрытых сетей.

Там, например, создают свои страницы правозащитники и журналисты из тоталитарных и авторитарных государств. В «Даркнете» им не страшны ни цензура, ни власти.

«Глубокий интернет» — отличная площадка для борьбы за свободу слова и использовать его можно не только в незаконных целях.

В «Глубокой сети» есть не только сайты для преступников, а также для добропорядочных пользователей.

В таблице 1 представлены несколько ссылок, которые могут быть полезны и рядовым законопослушным гражданам [8].

Табл. 1.

**Полезные ресурсы в «Deep Web»**

| | |
|---|---|
| Библиотеки | После того как русскоязычную библиотеку «Флибуста» заблокировали в поверхностном Интернете, она переехала на «глубину». Там можно найти тысячи книг на русском языке. У «Флибусты» есть свои страницы в «Глубоком Интернете» и в Даркнете. Среди других известных книжных ресурсов «Deep Web»— «Словесный богатырь» и «Imperial Library of Trantor». |
| Росправосудие | База данных общедоступных судебных решений со всей России. |
| Хостинг картинок | Анонимный хостинг картинок, куда можно бесплатно загрузить файлы «jpg», «png» или «gif» размером до 20 мегабайт. |
| Научные статьи | Глубокое «зеркало» портала «Sci-Hub», который позволяет бесплатно скачивать научные статьи. |
| Сообщество борцов с цензурой | Мультиязычное сообщество «We Fight Censorship» публикует материалы, которые по тем или иным причинам были признаны запрещенными в разных странах. |
| Сервис вопросов и ответов | Англоязычный сервис «Hidden Answers» работает по тому же принципу, что и «Ответы Mail.ru». Одни пользователи задают вопросы, а другие на них отвечают. Главное отличие от аналогичных «поверхностных» площадок — тематика вопросов. В основном они посвящены кибербезопасности и «Глубокому Интернету». Хотя есть и вполне обычные тематические разделы, например, об отношениях или еде. |
| Поисковик | Если захотите сами поискать что-то в «Deep Web», можно воспользоваться системой, которая позволяет искать работающие сайты в «Глубоком Интернете». |

**Как видно из таблицы 1 «Deep Web» используется и во множестве благих целей, некоторые из которых могут пригодиться и обычному пользователю для решения своих индивидуальных задач.**

**Рассмотрим некоторые советы для поиска информации в «Deep Web»:**

- Менять ракурс поиска в обычном поисковике. Подумать не только о самом предмете поиска, но и о том, где такой контент может находиться и к каким категориям данных он относится. Если вы ищите в Интернете контакты человека, подумайте, в каких базах данных может быть информация о нем. Необходимо понять, кто может быть заинтересован в создании и наполнении базы с нужными вам данными. Например, если вам нужны контакты архитектора из «Германии», можно искать в – «Google» не только его имя, но и базу данных всех архитекторов «Германии».

- При поиске баз данных, добавьте в поисковый запрос фразу «database OR directory OR catalogue OR list» (то есть название базы данных, ее директиву и каталог). Но помните, что таким образом стоит искать только саму базу данных, а не конкретную информацию из нее.

- Для поиска списков с англоязычными базами данных, введите в поиск фразу «a * z database».

- Проверяйте раздел «Ссылки» под статьями в «Wikipedia» – там можно найти перечни некоторых нужных вам баз данных. Нужно помнить, что некоторые категории в «Wikipedia» тоже ведут к информации о базах данных.

Например:

URL:https://en.wikipedia.org/wiki/Category:Databases , https://en.wikipedia.org/wiki/Category:Digital_libraries, https://en.wikipedia.org/wiki/Category:Scholarly_databases.

- Помните о городских и университетских библиотеках: они могут иметь доступ к различным научным базам данных по подписке. А еще в библиотеках можно получить доступ к научным работам и проверить на плагиат диссертации интересующих вас людей.

**Полезные сайты для поиска в «Deep Web»:**

- «Startpage.com» – поисковая система, которая использует данные поиска «Google», но не передает поисковику информацию о пользователе.

- «bibliothek.uni-regensburg.de/dbinfo» – большой каталог баз данных на разные темы.

- «Archive.is» – сервис, позволяющий заархивировать страницу в Интернете по состоянию на определенный момент. Полезно регулярно делать такой бекап в ходе расследования, чтобы иметь доказательства на случай удаления страницы.

- «Iana.org» – сайт, на котором можно проверить владельца домена.

- «Worldcat.org» – крупнейший каталог книг, их авторов и издателей.

- «Cve.mitre.org» – база утечек данных в Интернете.

- «Ted.europa.eu» – «Tenders electronic daily» – крупнейшая база тендеров Европейского Союза.

- «Doaj.org» – база данных научных изданий.

В последнее время появились и другие сайты.

Доступ в «Глубокий Интернет» также возможен через специальный браузер «TOR». Он шифрует трафик и данные пользователей, поэтому работает медленно, зато серфить интернет через «TOR» можно абсолютно анонимно [9].

Итак, например, по данным экспертов, для того чтобы перейти через приложение «TOR» в «Глубокий Интернет», необходимо обратиться к ресурсу «Hidden Wiki» (аналог обычной Википедии). Там содержатся ссылки на сервисы и услуги «подвала» Интернета, начиная от тематических ресурсов, заканчивая торговыми площадками. В недрах невидимой сети можно без особых затруднений найти как легальный форум или блог, так и сайты противозаконных организаций. Так, например, большая утечка секретных данных АНБ США в СМИ, осуществленная бывшим сотрудником ЦРУ Эдвардом Сноуденом, производилась с использованием сети «TOR».

Наряду с этим необходимо обратить внимание и на связь **«Deep Web»** с «DarkNet» о чем выше уже говорилось.

«Глубокая паутина» заработала репутацию зловещей бездны, незаконной и вызывающей беспокойство деятельности, о которой можно услышать в СМИ, но это место называется «DarkNet».

Термины «Deep Web» и «DarkNet» часто используются как синонимы, однако это не совсем верно. «DarkNet» – это лишь крошечная часть «Deep Web», составляющая, по данным экспертов, всего 0,01% от него.

Таким образом все страшилки, которые очень часто можно слышать о «Deep Web», относятся к «DarkNet».

В этой связи необходимо дать небольшое разъяснение. (Разные специалисты по-разному трактуют положения, связанные «Deep Web» и «DarkNet», но есть некоторые точки соприкосновения).

*Идентификация инженерно-технических и программных границ киберпространства не позволяет выделить достаточно точно такой проблематичный в плане легитимности сегмент Интернета, который чаще всего называется Deep Web/Dark Net. Это такая интернетизированная сеть, в которой соединения между информационными ресурсами устанавливаются только между доверенными (и многократно проверенными) IP адресами, с использованием специфицированных протоколов и портов [10].*

*В киберпространстве «DarkNet» через сеть не связанных между собой виртуальных информационных потоков, предоставляет возможность передачи данных в зашифрованном виде. Обмен файлами в «DarkNet» анонимен, поскольку IP-адреса юзеров скрыты от внешнего контроля. Поэтому пользователи могут*

*надеяться, что их конфиденциальное общение происходит без государственного вмешательства.*

На основании изложенного делая предварительный вывод, можно отметить, что с развитием информационных технологий появляются новые возможности для саморазвития, новые способы коммуникации и быстрой передачи информации на любые расстояния.

«Глобальная сеть» и «Интернет» обладают большим количеством уникальных характеристик, которые позволили межчеловеческим отношениям перейти на новый уровень. Однако с появлением достоинств «Глобальной сети», появились и её недостатки, представляющие опасность для человека: распространение вирусов и вредоносных программ, публикация недостоверной информации, порой ущемляющей права человека или подрывающей безопасность государства и т.д.

При всей доступности информационных технологий в **«Deep Web»** необходимо помнить, что это достаточно опасное место, тем более, что в него входит «DarkNet». Ведь эту площадку используют не только хакеры или ученые, но и разведслужбы, полицейские, а также преступники. Может произойти такое, что переход на нежелательный сайт в лучшем случае обернется потерей денег, в худшем – уголовным преследованием, так как многие ресурсы, размещенные там являются запрещенными на территории нашей страны.

В этой связи укрепление ресурсной базы кибербезопасности обеспечивает оборонительную и наступательную функции защиты национальных интересов нашей страны, создаст возможности реального противостояния конкурирующих за обладание стратегическими информационными ресурсами стран, иногда доходит до ситуации кибервойны (cyberwarfare), как составной части перманентной информационной войны.

Экспоненциальная цифровизация экономической деятельности в современном обществе неизбежно влечет многочисленные риски, в том числе несанкционированный доступ преступников к базам данных, находящихся в труднодоступной части киберпространства - **«Deep Web»** или «DarkNet».

Таким обозом в заключение необходимо отметить, что необходимо изучать данные технологии и системы, осуществлять и наращивать информационную безопасность страны, а самое главное людям подумать о своей личной информационной безопасности, когда входите в Интернет или **«Deep Web».**

Берегите себя.

**Список литературы**

1. Узденов Р.М. «Новые границы киберпреступности» // Всероссийский криминологический журнал. 2016. [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/novye-granitsy-kiberprestupnosti (дата обращения: 03.09.2021).

2. Международный конгресс по кибербезопасности «International Cybersecurity Congress» (2018). 05.07.2018. Москва, Центр международной торговли, Конгресс-центр.

3. Тумоян Е.П., Аникеев М.В. «Сетевое обнаружение пассивных скрытых каналов передачи данных в протоколе TCP/IP // Информационное противодействие угрозам терроризма». 2006.

4. Kokoulin A. N., Andreev R. A., Badrtdinov A. S., Feofilova P. A.-«Analysis of problems of using the tor system-Technical Sciences - from theory to practice». 2015.

5. Колоколова В.И. «Ограничение доступа к сайтам в сети «Интернет», содержащими запрещённую информацию – Современные научные исследования и инновации». 2016.

6. Сушкова Ю. А., Меркулова М. С. «Киберучения. Проблемы российского Интернета». Электронный вестник Ростовского социально-экономического института. 2015.

7. Аграновский А.В. «Современные анонимные сети в электронной коммерции» // Известия высших учебных заведений. Северо-Кавказский регион. Серия: Технические науки. 2003.

8. Borodakiy Yu. V., Dobrodeev A. Yu., Butusov I. V. «Cybersecurity as the main factor of national and international security of the XXI century» (Part 1) // Cybersecurity issues. 2013.

9. Nishanov R. sh. «On the issue of possible criminalization of the spread of Tor technologies-Actual problems of the relationship between criminal law and the process-Collection of materials of the all-Russian scientific and practical conference with international participation». 2016.

10. Lekalo I. A. «Using anonymous networks to protect the Internet traffic of employees of the organization. In the book: New information technologies Abstracts of the XX International student conference-school-seminar». MIEM. Moscow, 2012.