ДАРКНЕТ КАК ЯВЛЕНИЕ ИНТЕРНЕТА

Мукимов Д.В., студент 4 курса ПИ

Мухаметшина Г.С., к. э. н., доцент

г. Бирск, ФГБОУ ВО Бирский филиал БашГУ

Deep web часто называют невидимой или скрытой сетью, потому что найденные здесь веб-страницы недоступны для стандартных поисковых систем. Сайты Deep Web содержат более сфокусированные и содержательные материалы, чем сайты Surface. Доступ к материалам в Deep Web часто требует навыков, усилий и настойчивости со стороны пользователя. Ресурсы в глубокой паутине часто остаются незамеченными из-за неопытности пользователя в поиске, иначе известной как «когнитивная невидимость».

Изучение Deep Web имеет важное значение, поскольку оно раскрывает скрытую информацию, чтобы пользователи могли получить доступ к ресурсам, которые в основном игнорируются популярными поисковыми системами. Пользователи баз данных регулярно взаимодействуют с Deep Web, но могут не знать об этом. 90% трафика в

Интернете поступает из Deep Web. Текущие академические исследования в значительной степени опираются на Deep Web. Deep Web часто содержат динамически генерируемые страницы, страницы с большим объемом данных, а также чувствительные ко времени или недолговечные страницы. Хотя технически невозможно точно измерить размер Deep Web, по некоторым оценкам, он в 500 раз превышает размер Surface Web, в то время как другие исследователи считают, что Deep Web в 5000 раз больше. Обычные поисковые системы индексируют менее 16% Surface Web и 0,03% всей информации, которая существует в Интернете. Доступ к Darknet можно получить через базы данных и каталоги, используя специализированные поисковые системы, которые обеспечивают более точные результаты поиска по более конкретным темам.

Эти расширенные инструменты поиска позволяют пользователю изменять и настраивать поиск для улучшения результатов. Поскольку большинство библиотек предлагают своим пользователям доступ к сотням различных баз данных, специалисту в области информации следует понимать Deep Web и то, как использовать его функции для поиска точной информации. Библиотечные и информационные специалисты обучены находить соответствующие ресурсы в глубокой сети быстрее и эффективнее, чем случайные искатели информации.

Darknet работает на более глубоком уровне Интернета, который процветает на анонимности. Эти сайты не являются общедоступными, поскольку в Интернете адреса протоколов скрыты для обеспечения конфиденциальности и анонимности. Интернет адреса протокола (IP) - это числовые строки, которые идентифицируют устройства в сетях, позволяют распознавать их другими системами. Темные веб-страницы обычно ненадежные, приходят и уходят регулярно, оставляя каталоги, заваленные мертвыми ссылками, когда веб-сайты исчезают или меняют местоположение. Обнаружение скрытых веб-сайтов, а также строгая анонимность укрепляют атмосферу таинственности.

Сама фраза Darknet производит впечатление незаконности, хотя законные цели для его использования существуют. Например, жители стран с высокой цензурой, иммигранты без документов имеют право на доступ к информации и нуждаются в защите конфиденциальности. Dark Web предоставляет все способы защиты их личной информации и конфиденциальности в условиях вторжения в практику сбора данных. Хотя некоторые могут поэкспериментировать с доступом к Dark Web из любопытства, анонимный характер и свобода выражения мнений становятся поддерживающим фактором в его долгосрочном использовании. В основе Darknet лежит сложный массив маршрутизации, который обеспечивает анонимность для пользователей, обращающихся к нему. В отличие от Surface Web и большинства частей Deep Web, Darknet включает в себя специальные технологии для доступа к размещенным веб-сайтам. Чтобы получить доступ к этим анонимным сайтам, необходимо использовать браузер Tor. Tor - это аббревиатура от The Onion Router. Темные веб-сайты работают на специальном сервере, который доставляет контент в браузеры Tor. Tor, модифицированная версия Firefox браузер, остается наиболее популярным инструментом пользователей Dark Web. Он использует набор инструментов, служб и узлов шифрования, которые скрывают и изменяют IP.

Deep Web и Darknet как инструмент защиты частной жизни и конфиденциальности стала ценным ресурсом в цифровую эпоху. Способность защищать интеллектуальную свободу эволюционировала благодаря новым и постоянно меняющимся информационным технологиям. Угрозы конфиденциальности информации по-прежнему вызывают озабоченность в любой сфере. Пользователи могут информировать посетителей об угрозах конфиденциальности и доступных защитных мерах. Эффективное информирование о рисках, связанных с обнаружением информации в интернете, является ключевым фактором. Изучение Deep Web, а по ассоциации и Darknet, требует специальных инструментов и техник, с различными средствами достижения различных уровней глубины. Анонимность и защита безопасности, предоставляемые преступникам, могут быть использованы для защиты тех, кто живет в странах с тираническим правительством, где существует законный риск судебного преследования, тюремного заключения или смерти за утечку информации или наличие несогласных мнений. Существует потенциал для дальнейших исследований того, как библиотеки используют технологии Darknet для защиты частной жизни посетителей. Темные веб-платформы разделяют основные ценности конфиденциальности, интеллектуальной свободы и доступа к информации.

Литература

1. «Дилемма даркнета» Эрик Жардин 2016 г.

2. «Конфиденциальность в Интернете» Уильям Роули, 2016 г.

3. «TOR и Deep Web» Леонард Эддисон, 2018 г.