

DARKNET – ТЁМНАЯ СТОРОНА ИНТЕРНЕТА

Шеллер Игорь Анатольевич

студент 1 курса

Сибирский институт управления – филиал РАНХиГС, г.Новосибирск

Аннотация. В статье рассматриваются суть и принципы работы анонимной сети – Darknet. Приводятся основные цели использования данной сети. А так же, изучаются её характерные особенности, которые служат полем для совершения преступлений.

Ключевые слова: даркнет, темная сторона интернета, преступления, криптовалюта, биткоин.

Интернет – всемирная сеть для хранения и обмена информацией. Получить доступ к этой сети может каждый. Внедрение данного вида технологий в различные сферы, однозначно сделало жизнь людей более комфортной, но с другой стороны, открыла занавес для развития новых путей преступности, так как существует другая, чёрная, сторона всемирной сети, под названием – «Darknet». Так же можно встретить название – «Dark Web».

Darknet — термин, относящийся к некоторой группе определенных вебсайтов, которые существуют в зашифрованном сетевом пространстве. Их невозможно обнаружить традиционными поисковыми механизмами с помощью обычных браузеров. Даркнет, по сути, — это «сеть поверх другой сети интернет», использующая специальные домены. Почти все сайты Даркнета скрывают персональные данные с помощью инструментов шифрования Tor. Эта сеть популярна, благодаря своей способности прятать идентификационные данные и сетевую деятельность пользователя. Соответственно, чтобы получить доступ к сайтам, которые являются запрещенными, человеку необходимо подключиться к сети Tor. Сайты Даркнета может посетить любой пользователь, который найдет «правильный» путь к нему. Именно по этой причине это предоставляет опасность, ведь на другой стороне интернета могут быть как любопытные «обыватели», так и опасные преступники[1].

Факт того, что пользователя невозможно отследить и способствовал развитию преступности в данной среде. Количество пользователей данной сети увеличивается примерно на 100 миллионам новых пользователей в год, значит можно говорить и о развитии преступности, которая скрывается в тени от государственных структур.

Большинство сайтов Даркнета скрывают персональные данные с помощью инструментов шифрования Tor. Принцип работы заключается в следующем:

Анонимность трафика обеспечивается за счёт использования распределённой сети серверов – узлов. В этой системе используется многоуровневое шифрование. Каждый пакет данных, попадающий в систему, проходит через три различных прокси-сервера – узла, которые

выбираются случайным образом. Перед отправлением пакет последовательно шифруется тремя ключами: сначала для третьего узла, потом для второго и в конце, для первого. Когда первый узел получает пакет, он расшифровывает «верхний» слой шифра и узнаёт, куда отправить пакет дальше. Второй и третий сервер поступают аналогичным образом. В то же время, программное обеспечение «лукового» прокси-сервера предоставляет SOCKS-интерфейс (SOCKS – это сетевой протокол, который позволяет пересылать пакеты от клиента к серверу через прокси-сервер прозрачно (незаметно) для них). Внутри сети Тог трафик перенаправляется от одного маршрутизатора к другому и окончательно достигает точки выхода, из которой чистый (нешифрованный) пакет данных уже доходит до изначального адреса получателя (сервера). Трафик от получателя обратно направляется в точку выхода сети Тог[2].

Но какие цели преследуют люди пользуясь тёмной стороной интернета? Как правило, основной целью использования Даркнета является незаконная торговля. Ниже будут приведены основные разделы торговли сети Даркнет:

1. Продажа наркотиков — одна из главных причин популярности Dark Web. В анонимной сети этому нелегальному виду торговли посвящены крупные разделы на разных форумах и множество отдельных сайтов. На одном из самых больших русскоязычных форумов по продаже наркотиков зарегистрировано свыше 90 тысяч пользователей. Купить на этих сайтах можно практически все виды наркотиков. Схема продажи следующая: покупатель связывается с продавцом через мессенджер с включенным шифрованием, оплачивает товар через интернет и получает наркотики в скрытом виде. На дальние расстояния товар отправляют курьерскими службами или по почте. Лично продавец и покупатель в подавляющем большинстве случаев не встречаются.

2. Продажа оружия. В отличие от западного сегмента Dark Web, где продажа оружия ведется в больших объемах и на крупных торговых площадках Даркнета, в России же этот вид торговли не так популярен. На крупнейших форумах можно найти лишь несколько продавцов и простеньких сайтов с каталогом оружия. Схемы продажи у них примерно одинаковые. Сначала предоплата — от 50 до 100 % через биткоины или фейковые платежные аккаунты, потом — получение оружия через курьерскую службу. Для того, чтобы не вызвать подозрения у правоохранительных органов, оружие разбирают и пересылают по частям.

3. Заказные убийства. На Западе заказу убийств через Тог посвящено множество сайтов. В русскоязычном же сегменте Dark Web можно найти лишь малую долю подобных объявлений. Как правило, продавцы предлагают разные виды убийств, цена за которые соответственно разнится. Оплата также принимается в биткоинах, исполнение заказа обещается в срок от 21 недели.

4. Другие организации преступлений. Также в Тог можно найти объявления о смежных с убийствами услугах. Например, о слежке, поджогах машин, ограблениях и избиениях. Если жертвой должна стать публичная личность, то цена устанавливается для конкретного человека. При этом исполнители уверяют, что берутся за «наказание» только тех, кто действительно этого заслуживает[3].

Но как произвести оплату необходимой услуги? Для того чтобы оставить эту зону без контроля и сохранить анонимность пользователя был придуман Биткоин. Биткоин – это вид криптовалюты, пиринговая платёжная система, использующая одноимённую единицу для учёта операций. Для функционирования и защиты биткоина используются криптографические методы.

При использовании биткоина участники транзакции не имеют никакой информации друг о друге. Анонимность и децентрализованность биткоина часто интерпретируются государствами как угроза, что приводит к борьбе с его использованием. Тем не менее его используют даже в тех странах, где он запрещен, в том числе для расчета в «теневых» сетях (Darknet). Одной из основных причин широкого использования биткоина является беспрецедентная надежность расчетов с автоматической защитой от мошеннических и прерванных операций[4]. Это означает, что криптовалюты обеспечивают анонимный, но при этом безопасный с точки зрения возможности обмана способ.

Благодаря такой системе, преступность в Даркнете продолжает развиваться. Процент раскрытых преступлений с использованием данной сети очень мал. В связи с этим нужно более основательно подойти к данной проблеме. Для того чтобы реально повлиять на динамику и структуру преступности в полностью анонимной сети, необходимы новые подходы, новые кадры и осознание масштаба данной проблемы. Возможно, одним из решений станет объединение стран, в которых Даркнет процветает, для совместной борьбы, ведь это может стать начальной точкой для создания абсолютно нового, полностью законного и открытого интернет пространства.

Список литературы:

1. Мэтт Иган. На темной стороне интернета: Что такое Dark Web и Deep Web? URL: https://www.dgl.ru/articles/na-temnoy-storone-interneta-cto-takoe-dark-web-i-deep-web_11677.html
2. Голик Дарья Игоревна, Ганжа Евгения Андреевна, Коломоец Анна Валерьевна. Темная сторона интернета. Ее суть и принцип работы. URL: <https://elibrary.ru/item.asp?id=31877134>

3. Мерзликин П.А. Что продают в русскоязычном Dark Web? URL: <https://paperpaper.ru/dark/>
4. Garman, C., Green, M., Miers, I. Accountable privacy for decentralized anonymous payments // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9603 LNCS, 2017. С. 81–98.