КУЛЬТУРОЛОГИЯ

ДАРКНЕТ - ТЕМНАЯ СТОРОНА ИНТЕРНЕТА ИЛИ НЕУЖЕЛИ ТАК ВСЕ ПЛОХО?

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

DARKNET - THE DARK SIDE OF THE INTERNET OR IS IT REALLY SO BAD?

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.2413-5291.2021.1.71.470

АННОТАЦИЯ

Основной целью данной статьи является изучение основных аспектов, касающихся такого сегмента современного Интернета, как черная сторона Интернета - DarkNet. В работе проанализированы виды, формы, особенности, положительные и отрицательные стороны Даркнета, а также проведено сравнение с открытым Интернетом. Исследованы характеристики анонимности. Кроме этого в статье выяснены основные моменты, касающиеся неправомерности использования и отрицательных особенностей DarkNet и предложены способы информационной безопасности.

ABSTRACT

The main purpose of this article is to study the main aspects concerning such segment of the modern Internet as the black side of the Internet-the DarkNet. The author analyzes the types, forms, features, positive and negative aspects of the Darknet, and also compares it with the open Internet. The characteristics of anonymity are investigated. In addition, the article clarifies the main points concerning the illegality of the use and negative features of the DarkNet and suggests ways of information security.

Ключевые слова. DarkNet, Интернет, информационная безопасность, информационные технологии, прокси-сервисы, преступность, анонимность, криптовалюта, алиасы, VPN, TOR

Keywords. DarkNet, Internet, information security, information technologies, proxy services, crime, anonymity, cryptocurrency, aliases, VPN, TOR

Интернет – всемирная сеть для хранения и обмена информацией. Получить доступ к этой сети в настоящее время может каждый.

Внедрение данного вида технологий в различные сферы жизнедеятельности человека, сделало жизнь людей более комфортной, но с другой стороны, открыла занавес для развития новых путей преступности, так как существует другая, черная, сторона всемирной сети, под названием – «DarkNet» [1].

«Darknet» (Даркнет) - 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 Интернета», использующая специальные домены. Почти все сайты «Даркнета» скрывают персональные данные с помощью инструментов шифрования «TOR» («The Onion Router», некоммерческая организация, занимающаяся исследованиями и созданием инструментов конфиденциальности и анонимности в Интернете).

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 сложившиеся сложившаяся ситуация предоставляет опасность, ведь на «другой стороне» Интернета могут быть, как любопытные «обыватели», так и опасные преступники.

Прообраз «DarkNet» появился еще в 70-х годах прошлого столетия. Случилось это во времена создания сети ARPANet (Advanced Research Projects Agency Network) (рис.1), которая впоследствии и стала прародителем современного Интернета.

Уже несколько десятилетий назад было очевидным, что кроме общедоступной части сети, которая предназначена для всех, необходимо было создать скрытый сектор, который как бы изолирован и доступен лишь для «своих».

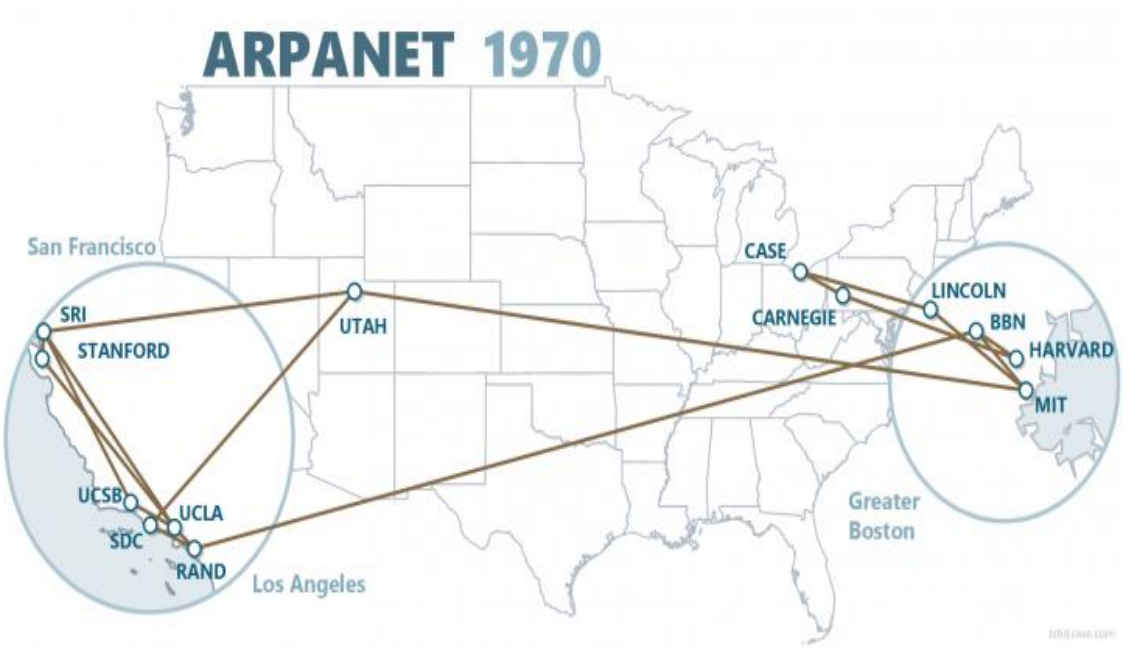

Рис. 1. Сеть ARPANet

Стоит сказать, что до начала 2000-х годов о существовании скрытой части международной веб-сети практически никто не знал.

Одни из первых сведений касательно «DarkNet» были опубликованы в сети «Freenet» (одноранговая сеть, предназначенная для децентрализованного распределённого хранения данных), где говорилось о том, что члены научной лаборатории «US Naval Research Lab» разработали особый инструмент, который позволяет находиться в сети Интернет анонимно. Как можно догадаться, речь идет о «TOR» или «The Onion Router».

Необходимо отметить, что «DarkNet» (теневая сеть, темная сеть) основывается на соединениях и протоколах сети Интернет, но не видна обычным пользователям, кроме того, любое соединение в «DarkNet» гораздо труднее отследить, что обеспечивается за счет сложной маршрутизации соединения и многократного шифрования информации.

Любопытно, что созвучные расширения в адресах «DarkNet» используются и в настоящее время. Данная система представляет собой сеть из большого количества прокси-серверов, используемых в том числе и для установки соединения, которое защищено от прослушивания извне. В результате, из такой сети получается огромная сеть виртуальных и в то же время анонимных «тоннелей», которые могут быть использованы для передачи зашифрованной информации. Таким образом, необходимо отметить, что пользователя сложно и даже «невозможно» отследить, что стало способствовать развитию преступности на просторах «DarkNet». [2]

Таким образом количество новых пользователей ресурса «DarkNet» стало быстро возрастать, т.е. увеличивается примерно на 100 миллионов в год, и часть из них криминальные структуры, которые скрывается в его тени от государственных структур, ведь просторы изучаемого ресурса являются анонимными и зашифрованными.

При этом большинство сайтов «Даркнета» скрывают персональные данные с помощью инструментов шифрования «TOR». Принцип работы заключается в следующем:

Анонимность трафика обеспечивается за счет использования распределенной 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 узнает, куда отправить пакет дальше. Второй и третий сервер поступают аналогичным образом. В то же время, программное обеспечение прокси-сервера предоставляет «SOCKSинтерфейс» (SOCKS – это сетевой протокол, который позволяет пересылать пакеты от клиента к серверу через прокси-сервер прозрачно (незаметно) для них). Внутри сети «TOR» 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 «TOR».

При этом в «Даркнете» все устроено так, как и в обычном Интернете: есть новостные сайты, маркеты, сайты, на которых торгуют какими-либо одними товарами. Главное отличие в том, что на большинстве сайтов занимаются чем-то

нелегальным или противозаконным. Если это новости, то они запрещенные, товары нелегальные или краденные, а на форумах обсуждают все, что способно нанести ущерб психическому здоровью человека.

Теневая сеть предлагает пользователям товары на любой вкус: там можно купить диплом любого высшего учебного заведения или оригинальный паспорт любого государства. Там же в наши дни осуществляется торговля людьми, оружием, наркотическими средствами и психотропными веществами [3].

Стоит также отметить, что на некоторых сайтах можно приобрести поддельные и фальшивые купюры самых разных стран, а на других - краденную технику, стоимость которой в 2 раза меньше закупочной. Однако все поддельные свидетельства, дипломы и паспорта, а также оружие и наркотики - это лишь вершина айсберга. Самое страшное начинается в форумах, где можно постичь искусство угона автомобиля и получить рекомендации других опытных автоугонщиков. Форумы в «Даркнете» объединяют людей абсолютно разных интересов и, главное, психических заболеваний. Самым неожиданным является то, что торговля людьми, контрабанда, продажа документов – всё это делается «уполномоченными людьми», а наличие в «Даркнете» личной информации о политиках и их переписок обусловлено «сливом информации» их самыми «близкими» людьми, которые непосредственно имеют доступ к их мобильному телефону или компьютеру.

Несомненно, у «Даркнета» есть определенные достоинства. Их не очень много, но все же недостатки во много раз превышают все плюсы. К положительным проявлениям «Даркнета» можно отнести, что он - это целая энциклопедия знаний о компьютерной, сетевой и информационной безопасности.

Также он содержит множество полезных форумных веток, где общаются между собой хакеры на тему цифровой безопасности. Данные форумы могут быть содержательны и познавательны для тех, кто заинтересован в поддержании компьютерной и информационной безопасности. Для экспертов в области программирования порой интересно узнать новые, креативные, усовершенствованные идеи. Однако стоит отметить тенденцию подростков использовать такую информацию в неправомерных целях.

Учитывая их азартность, любознательность и стремление к познанию всего запрещенного, а также неспособность нести ответственность за свои поступки, можно предположить, что подростки, зная способы поддержания цифровой и информационной безопасности, способны нанести вирусными атаками значительный ущерб правам граждан, использовав их персональные данные.

Изучая вопрос перехода на темную сторону Интернета, необходимо начать с небольшой истории.

Для посещения сайтов «Даркнета» нужен специальный софт, назовем его «Х». Такой софт изобрели американские военные в середине 1990-х, заботясь о безопасной передаче разведданных. Он шифрует и передает данные через несколько узлов. При этом, что именно смотрит и какие сайты посещает человек через этот софт (браузер), Интернет-провайдер не знает. Для сайтов пользователь тоже остается анонимом, только если не светится сам.

К «Даркнету» можно подключиться и через обычный браузер, используя специальные расширения, но их качество и ваша анонимность будут под вопросом. [4].

«Х» подключается к сайтам через несколько узлов по всему миру. Юзера, который заходит на ресурс, например, из Китая, браузер может повести через Канаду, ЮАР и Чили. Исходя из этого, пользователи «Даркнет» получают полную анонимность при использовании его ресурсов.

Сайты Даркнета расположены очень часто в псевдодоменной зоне «.onion», а их названия прогоняются через ключ шифрования и выглядят как 16-значная комбинация букв и цифр. Такие сайты работают на виртуальных выделенных серверах, то есть они сами себе хостинг-провайдеры. Вычислить администраторов сайтов в зоне «.onion» сложно, но можно, поэтому часто люди, занимающиеся коммерческой деятельностью, чтобы себя обезопасить в «Даркнете» заводят новые площадки, не дожидаясь проблем на старых, чтобы наверняка обезопасить себя от потенциальных проблем или иных вопросов.

Таким образом, на сегодняшний день на «DarkNet» функционирует огромное множество магазинов и иных бизнесов (коммерческих предложений). Многие люди, понимая, что на данных ресурсах они будут иметь практически полную анонимность начинают пользоваться данной возможностью не в благих намерениях.

Магазины «DarkNet» - это не бизнес одного направления. Разные люди продают здесь «незаконные» товары и услуги, которых не найти на обычном рынке.

По данным экспертов, магазины «Даркнета» работают по 100%-ной предоплате. Чтобы сделки были честными, площадки замораживают квоты и депозиты дилеров, при сделках на большие суммы администраторы могут выступать гарантом. Мелкие магазины работают как кофе-автоматы: ты ему деньги - он тебе закладку.

На сайтах-маркетплейсах, продавцы платят покупателям или «онлайн площадкам» комиссию с каждой сделки. При этом самыми крупными площадками были и остаются: «Silk Road», «AlphaBay», «Hansa» и др., при том что их владельцы, администраторы, ряд продавцов и клиенты уже за решеткой, например, Россу Ульбрихту, основателю «Silk Road», дали целых два пожизненных срока за торговлю наркотиками, хакерство, отмывание денег и заказ шести убийств.

В тоже время наряду с представленными действиями в «Даркнете» появились новые информационные технологии, связанные с произведением сделок, оплата и отмыв денег. Одним из наиболее эффективных и подходящих выходов в данной ситуации стало появление криптовалют.

В результате начали активно создаваться новые нелегальные торговые площадки: продавать и покупать стало безопаснее. Данный фактор связан с тем, что площадки, занимающиеся обработкой криптовалют не подразумевают сбор конфиденциальных данных.

При этом заработанные деньги дилеры и прочие «барыги» «Даркнета» отмывают через «биткойн-прачечные». «Прачечные» обналичивают криптовалюту за свой процент. Таким образом, криптовалюты стали инструментом практически всех торговцев, предоставляющих свои услуги на площадках «Даркнета».

Однако в последнее время серьезную роль стала играть криптовалюта - BitCoin (Биткоин).

Биткоин – это вид криптовалюты, пиринговая платежная система, использующая одноименную единицу для учета 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.

Преимуществом BitCoin является то, что он может быть не связан ни с каким государством или конкретным банком, что обеспечивает беспрецедентную анонимность и неотслеживаемость прохождения платежа. У системы отсутствует какой-либо административный центр или узел администрирования, поэтому собрать сводку о проводимых транзакциях трудно, кроме того, из-за высокой трансграничности системы вряд ли юрисдикция какого-либо государства распространяется на контроль таких платежей.

Однако, при этом необходимо отметить, что «Даркнет» является не единственным ресурсом сети Интернет, использующимся в преступных целях. Современные ресурсы Всемирной сети, открытый Интернет, имеет множество преимуществ и особенностей, посредством которых и процветает преступность.

Таким образом возникает вопрос: «Есть ли связь между обычным открытым Интернетом и «Даркнетом»?»

Так, например, по данным экспертов, в обычной сети Интернет простые люди и преступники пользуются следующими преимуществами:

Во-первых, Интернет имеет глобальную трансграничную природу, что вызвано архитектурой самой сети. Это способствует развитию и росту всей интернет-преступности независимо от ее видов и категорий. Интернет позволяет совершать многочисленные общественно опасные деяния на территории любой страны в мире с домашнего компьютера, находящегося в другом государстве. Кроме этого, Глобальная сеть способствует кооперации и консолидации международных организованных преступных группировок и сообществ независимо от вида совершаемых преступлений [5].

Во-вторых, одним из принципов интернет-технологии является анонимность, что, в первую очередь, обеспечивает преимущества для всех форм мошенничества и обмана. Анонимность позволяет публиковать информацию любого свойства с минимальным риском понести уголовную или иную ответственность. Анонимность не только дает преимущества в размещении преступной информации, но и влияет на увеличение спроса на нее. Так, например, востребованная некоторой категорией лиц детская порнография может анонимно воспроизводиться, тиражироваться и просматриваться педофилами в Интернете без угрозы огласки и наступления для них негативных последствий. Выходит, что анонимность Интернета способствует созданию устойчивого спроса на информацию аморального, безнравственного, антиобщественного и преступного характера.

В-третьих, Интернет имеет огромный потенциал для охвата глобальной аудитории, делая возможным совершать беспрецедентные по количеству потерпевших преступления. Использование Интернета для совершения преступлений зачастую позволяет многократно увеличить наносимый вред и причинить негативные последствия, которые будут проявляться на протяжении длительного времени, что несравнимо с обычными общественно опасными деяниями.

В-четвертых, сложности в борьбе с преступностью и правовом регулировании интернет-пространства дают определенные преимущества преступникам, использующим Глобальную сеть, создают распределение основных узлов сети и их взаимозаменяемость. Например, несмотря на все усилия китайского правительства по ограничению доступа на своей территории к нежелательной экстремистской, террористической, антисоциальной информации, существует достаточно много общеизвестных возможностей по обходу запрета.

Перечисленные характеристики подходят и для сети «DarkNet».

Так, к примеру, как обычный пользователь, так и мошенник без всякого труда имеет доступ к теневому интернету «DarkNet» благодаря некоторым следующим технологиям:

- **Зеркало сайта**. Точная копия сайта, расположенная по другому адресу. Такое решение часто используют для распределения нагрузок: если нужно, чтобы больше людей могли скачивать один и тот же файл без потери в скорости скачивания, его загружают на несколько зеркал. Другой повод установить зеркало — необходимость увеличить число источников информации. Например, какой-нибудь сайт могут заблокировать, но его зеркало в это время останется доступным. Это все равно как квартира, в которую можно попасть через несколько разных дверей — «meduza.io» и «mdza.io».

- **Алиасы.** Алиасы, это дополнительные адреса для сайтов, псевдонимы и они нужны по разным причинам — от желания обладать правами на созвучное доменное имя или похожее по написанию до необходимости завести более короткий адрес сайта. Например, адреса с другими доменными именами «.ru» вместо «.com» или с опечатками — «Amozon» вместо «Amazon». Они повсеместно используются вебмастерами для управления схожими доменами, чтобы их никто не украл. Иногда алиасы называют синонимами доменных имен. Например, человек захотел зайти на ваш сайт «moysait.com», но не вспомнил суффикс и написал «moysait.org», то в этом случае с алиасом произойдет одно из двух: посетитель увидит контент, хранящийся на основном сайте, но в адресной строке будет ссылка с «ошибкой» (как с «зеркалом») или будет перенаправлен на главную страницу.

- **Прокси-сервер**. Промежуточный сервер, который выступает посредником между пользователем и целевым сервером. Применяется для обхода блокировки сайтов, подмены настоящего местоположения пользователя. Представьте, что вы звоните со своего телефона другу, но не хотите, чтобы ваш номер определился у него на экране. Для этого вы используете посредника, который подменит ваш номер на свой. Так и работает прокси-сервер — он скрывает ваш IP-адрес и заменяет на другой. Обычные пользователи могут воспользоваться как открытыми прокси-серверами (чаще всего с различными ограничениями по качеству соединения), так и платными. Кстати, в компаниях прокси-серверы используют для того, чтобы предоставлять или, наоборот, ограничивать доступы сотрудников к выбранным ресурсам.

- **VPN (Virtual Private Network).** Это название целого ряда технологий, которые позволяют настроить одну сеть поверх другой. Для большинства пользователей на практике это означает, что при помощи VPN можно подключиться к одному узлу Интернета посредством другого. Например, в вашей стране заблокировали какой-то мессенджер, но вам очень нужно им воспользоваться. Можно использовать прокси-сервер или VPN. Ваш компьютер или смартфон будет пропускать все соединения через еще один компьютер, расположенный, например, в другой стране. Существует много компаний, которые предоставляют VPN как сервис: вы оплачиваете подписку, а вам дают адрес и пароль (это похоже на настройку электронной почты) либо дают приложение, которое можно установить на компьютер или смартфон. Еще одна причина использования VPN — создание защищенных каналов коммуникации.

Как правило, различие между использованием прокси и VPN состоит в том, что в первом случае это применяется на уровне отдельной программы, а во втором — ко всем соединениям [6].

Итак, подытоживая, техническую сторону Интернета и «DarkNet» встают вопросы: «Какие цели преследуют люди пользуясь темной стороной Интернета «DarkNet»? Хорошо это или плохо?»

По мнению некоторых экспертов, хотя компьютерные технологии в целом нейтральны и не могут быть деструктивными, тем не менее, возможности, предоставляемые «DarkNet», способствуют проявлению их антисоциального и криминального характера. В данной сети процветают расистские сайты, наркоторговля, онлайн проституция, терроризм, а также распространение информации и средств для кибервзлома. В «теневом Интернете» свободно распространяется порнография, в том числе детская, продаются оружие и боеприпасы, доступны украденные данные кредитных карт и т. д.

Исследования показывают, что «DarkNet» привлекателен не только для незаконного распространения наркотических средств и психотропных веществ, но и для осуществления террористической и экстремистской деятельности.

Во-первых, в «DarkNet» террористические группы могут найти практически любые необходимые рекомендации и улучшенные схемы для повышения эффективности своей деятельности, среди них: легализация преступно заработанных доходов, шифруемые каналы связи, наем исполнителей, включая потенциальных смертников для террористических атак в реальном мире и кибератак.

Во-вторых, «DarkNet» содержит подробную информацию по изготовлению взрывчатых веществ и оружия массового поражения, руководства по вербовке, тренировке, психологической обработке, формированию мотивации у террористов.

В-третьих, в «DarkNet» специально создаются официальные сайты для террористических групп, которые, не боясь преследования, контактируют и взаимодействуют. Так поступала, например, известная террористическая организация «Аль-Каида». Сайты террористического и экстремистского содержания предоставляют самую разную информацию – от того, как избежать излишнего внимания правоохранительных органов до способов удаления следов крови и сокрытия иных последствий совершенных преступлений [7].

И как было отмечено выше, одной из основных задач использования Даркнета является незаконная торговля, в частности:

1. **Продажа наркотиков** - одна из главных причин популярности «DarkNet». 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.

Так, к примеру, можно отметить в Даркнете российскую торговую площадку «Гидра» (уникальная торговая площадка в сети «TOR»), на которой происходит торговля наркотиками. В последнее время «Гидра» стала крупнейшей в мире по продаже наркотиков.

«Гидра» выполняет роль посредника между продавцами и покупателями. Помимо наркотиков, на площадке можно купить поддельные купюры, хакерские услуги, фальшивые документы и другие запрещенные товары [3].

На «Гидре», согласно информации, различных экспертов, зарегистрированы около 2,5 млн аккаунов, 393 тысячи из них совершили за время существования площадки хотя бы одну покупку. Число пользователей с каждым месяцем растет.

Кроме этого с 2016 года по 2019 год через «Гидру» проведено свыше 64,7 млрд рублей, при том что общий объем сделок, прошедший через зарубежный Даркнет с 2011 по 2015 год, составил 191 млн долларов США.

При этом лидером по наркотикам, которые спрятаны в «закладках» (продавец упаковывает товар и закладывает в неприметном месте), стала Москва.

На втором месте — Санкт-Петербург, где в «закладках» лежало наркотиков на 66 млн рублей. Петербург также является основной точкой ввоза наркотиков из Европы, по данным экспертов. Причем большинство «импортных» наркотиков стоят там дешевле, чем в других городах, из-за низких расходов на логистику. [3].

2. **Продажа оружия.** В отличие от западного сегмента «DarkNet», где, продажа оружия ведется в больших объемах и на крупных торговых площадках «Даркнета», в России, по данным экспертов, пока 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 [6].

3. **Заказные убийства**. На Западе заказу убийств через «TOR» посвящено множество сайтов. В русскоязычном же сегменте «DarkNet» можно найти незначительную долю подобных объявлений. Как правило, продавцы предлагают разные виды убийств, цена за которые соответственно разнятся. Оплата также принимается в биткоинах, исполнение заказа обещается в срок от 21 недели [8].

4. **Другие организации преступлений**. Также в «TOR» 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 [9].

Список деструктивного и противоправного в «DarkNet» не ограничивается только указанными видами деятельности, он продолжает увеличиваться и совершенствоваться. Например, в последнее время хакеры стали активно взламывать базы компаний и красть важные данные, затем выставлять украденную информацию на продажу в «Даркнете».

С учетом изложенного можно сделать предварительный вывод, что впитывая в себя различные информационные, технические, финансовые, программные компоненты «DarkNet» становится более анонимной, более разветвленной системой (сетью), предоставляющую возможность «юзерам» еще большую трансграничность и финансовую самостоятельность.

О повышенной анонимности такой сети свидетельствует, что Эдвард Сноуден, сотрудник Агентством национальной безопасности США (АНБ США), например, использовал ее для передачи в СМИ информации о совершенно секретном комплексе мероприятий, осуществляемых АНБ США с целью негласного массового сбора информации, передаваемой по коммуникационным сетям.

Кроме того, в сети «DarkNet» используются сложные системы шифрования, что серьезно затрудняет доступ правоохранительных органов к передаваемой информации даже при наличии полномочий [9].

Таким образом, можно констатировать, что преступный мир быстро адаптируется к информационному и технологическому прогрессу. Преступники разных специализаций, не обремененные бюрократическими процедурами и требованиями по соблюдению прав человека, соблюдения законности, освоили «теневой Интернет» за достаточно короткий срок.

При этом законодатели, в разных странах мира, в том числе в России, не успевают своевременно создавать и формировать правовую базу, регулирующее данную сферу деятельности, по разным объективными субъективным причинам. По этим же причинам не удается должным образом осуществлять наступательность и показывать

должную результативность правоохранительным и контролирующим органам.

Однако, не смотря на трудности и сложности, есть и первые победы. С каждым годом все больше и больше контролирующими и правоохранительными органами закрываются противозаконные сайты в «DarkNet», применяются запретительные меры, и преступники уже не так вольготно и безопасно чувствуют себя в этой части информационного сегмента сети.

Наиболее громким делом стало закрытие сайта сети «DarkNet» под названием «Шелковый путь» (англ. SilkRoad), закрытый международными правоохранительными органами, который, по сути, являлся площадкой для торговли наркотиками и контрабандным товаром. Данному сайту на протяжении двух лет удавалось избегать привлечения к уголовной ответственности и быть посредником между продавцами и покупателями по всему миру, предоставляя возможность доставки наркотиков в любую точку земного шара за безналичный расчет (в основном с использованием криптовалют) [10].

В завершении необходимо отметить, что, не смотря на первые результаты, несовершенство законодательства и недостаточно эффективной работе контролирующих и правоохранительных органов преступность в Даркнете продолжает развиваться. Процент раскрытых преступлений, в настоящее время, 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 активизация работы по совершенствованию законодательства, применение новых наработок правоохранительными органами и передачи опыта профессорско-преподавательскому составу полицейских подразделений и потом быстрому и качественному обучению курсантов, и повышению квалификации действующих сотрудников, а потом применение на практике знаний и опыта по предотвращению преступлений в Даркнете.

Кроме этого необходимо объединение и передача международного опыта между правоохранительными органами разных стран, что придаст дополнительные силы и позволит осуществлять совместную борьбу, что для создания абсолютно нового, полностью законного и открытого интернет пространства [10].

Таким образом, общественная опасность данного явления очевидна и требует повышения эффективности предупредительной работы. Анализ противодействия преступности в Даркнет позволит выработать основные методы борьбы с киберпреступностью и успешно внедрять их в жизнь и обезопасить простых людей от противозаконных действий.

Но самое главное при этом - личная информационная безопасность каждого человека, когда человек будет надеяться не только на государство и его правоохранительные, контролирующие органы, но и на себя, и не будет ради хвастовства, ухарства лезть туда куда ему лезть не надо.

Берегите себя и подумайте о последствиях свой действий.

Список литературы

1. Узденов Р. М. «Новые границы киберпреступности» // Всероссийский криминологический журнал. 2016.

2. Бурцев С.Е. «Причины роста числа российских пользователей анонимной сети TOR и влияние PR-компаний на интерес к скрытым Интернет-сервисам». - журн. «ИТПОРТАЛ», №4 (16), 3 с., 2017.

3. Свищёв А. В., Лаухина А.С. «Darknet: полезный инструмент или источник угрозы» // Colloquium-journal. 2020.

4. Иванов М.Г. «О роли уголовного наказания в предупреждении служебно-экономической преступности и коррупции в современной России» // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2017.

5. 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.

6. Lacson W., Jones B. «The 21st Century DarkNet Market: Lessonsfrom the Fall of Silk Road» // International Journal of Cyber Criminology. 2016.

7. Weimann G. «Going Dark: Terrorism on the Dark Web» // Studies in Conflict & Terrorism. 2016.

8. Васильев А.А., Ибрагимов Ж.И., Васильева О.В. «Даркнет как ускользающая сфера правового регулирования» // Юрислингвистика. - 2019.

9. Полунина А.В. «Даркнет: по ту сторону Интернета». / Р.М. Магомедов. -Тюм.: Академически журнал Западной Сибири, том 15, № 3(80), с. 69-70, 2019.

10. Bancroft A. «Responsible use to responsible harm: illicit drug use and peer harm reduction in a darknet cryptomarket» // Health, Risk and Society. 2017.