ISSN 2311-410X

ИННОВАЦИОННАЯ ЭКОНОМИКА:
ПЕРСПЕКТИВЫ РАЗВИТИЯ И СОВЕРШЕНСТВОВАНИЯ

научно-практический журнал

экономика
право
социология
философия

№2 (28) 2018 год

УДК 34.09

ПУТИ НЕЗАКОННОГО ИСПОЛЬЗОВАНИЯ ВОЗМОЖНОСТЕЙ ИНТЕРНЕТА И ВОПРОСЫ ПРАВОВОЙ РЕГЛАМЕНТАЦИИ

***Джумадиль Екатерина Евгеньевна**, студент*
(e-mail: kit_96@list.ru)
***Макаревич Марина Леонидовна**, к.и.н., доцент*
(e-mail: makarevichm@mail.ru)
Санкт-Петербургский политехнический университет Петра Великого, г. Санкт-Петербург, Россия

В данной статье рассматриваются основные виды незаконного использования интернет-пространства, а также правовые аспекты регулирования данного вида преступности.

Ключевые слова: Интернет, Dark web, DarkNet, киберпреступность, компьютерное мошенничество, Tor-сети, хакерство, запрещённый интернет-контент, правовое регулирование.

Интернет стал неотъемлемой частью реальной жизни большинства людей. Посредством сети Интернет человек каждый день удовлетворяет различные потребности: общение, образование, развлечение и так далее.

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 хакерство, кибертерроризм, киберэкстремизм, кибервойны, компьютерное мошенничество и другие виды киберпреступности.

Поэтому остро стоит вопрос о безопасности информационных систем. В частности, вопрос о законодательном регулировании так называемого «тёмного» Интернета, Dark Web (синонимы – *DarkNet*, скрытый интернет, Теневой интернет, «Тёмная паутина»).

История Теневого интернета началась с 1970-х годов, когда разрабатывалась сеть ARPANet – прообраз будущего Интернета. Наибольшее распространение термин «Даркнет» 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. [0]

«Тёмную паутину» не следует путать с **«Глубокой паутиной»**, Deep Web (синонимы – невидимая сеть, «глубокая» сеть, глубинный интернет). *Dark Web* и *Deep Web* – два совершенно разных понятия, которые СМИ зачастую смешивают. Под Dark Web принято подразумевать тот скрытый интернет, который ценится за возможность анонимно пользоваться благами Всемирной Сети. Основная же часть Глубинного интернета абсолютно

легальная, страницы здесь хоть и не индексируются, но пребывают в ведении законопослушных пользователей и легитимных предприятий.

На аккаунты «Даркнета» приходится до 0,1% Интернета. Кроме того, DarkNet базируется на защите конфиденциальности пользователя, находящегося в онлайне, за счёт чего и пользуется огромной популярностью у хакеров, которые желают скрыть свою видимость в Сети. При этом для его использования понадобится специальный браузер, который позволяет оставаться анонимом, и не выдавать свой настоящий IP-адрес.

Вплоть до 2000-х годов о скрытой стороне Интернета почти ничего не сообщалось. С 2004 года работает система анонимизации серверов, которая позволяет скрыть истинное их местонахождение с помощью специального программного обеспечения (далее – ПО). К этим серверам доступ возможен только через клиент Tor-сети (синонимы – TOR, Tor Browser (браузер), Tor-службы, «луковый маршрутизатор»). Tor (от англ. The Onion Router, отсюда и расширение в адресах DarkNet – «.onion») – «луковичная маршрутизация»[13], под ним подразумевается ПО с открытым кодом, которое позволяет создавать анонимные сетевые соединения, защищённые шифрованием. [2] Tor пользуется сетевыми уровнями onion-маршрутизаторов, позволяя обеспечивать анонимные исходящие соединения, а также работу анонимных скрытых служб.

Tor-службы являются частью Теневого онлайн-рынка. Соединения в DarkNet устанавливаются только между доверенными пирами[14] с использованием нестандартных протоколов и портов. Файлообмен происходит анонимно в одноранговых сетях, что позволяет передавать информацию без опасений её перехвата или подмены.

Основной целью «Тёмной Паутины» считается возможность предоставить пользователю полную анонимность, при этом гарантируя ему защищенность от ограничений со стороны закона. Количество пользовательских форумов, нелегальных рынков, блогов запрещенных законом лиц и организаций, а также документации конспиративного характера увеличивается на просторах этого ресурса ежедневно.

Если рассматривать все «за» и «против» Теневого интернета, безусловный перевес придётся на отрицательное действие. Несмотря на немалое количество положительных аспектов, DarkNet всё же обладает устоявшейся криминальной репутацией.

Из светлых сторон стоит отметить, что в Теневом интернете встречаются увлекательные проекты, посредством которых в Сети можно обнаружить настоящих интеллектуалов. Яркий примером служит завоевавшая известность в не только в скрытом интернете, но и в «видимом» головоломка

[13] Луковая маршрутизация – технология анонимного обмена информацией через компьютерную сеть. Сообщения неоднократно шифруются и отсылаются через несколько сетевых узлов, которые и называют луковыми маршрутизаторами. [https://ru.wikipedia.org/wiki/Луковая_маршрутизация]

[14] ***Пир*** *(англ. «peer») – равноправный участник (пользователь) сети, предоставляющий сервисы другим участникам одноранговой сети и сам пользующийся их сервисами. Часто так называется клиент, участвующий в раздаче в файлообменных сетях. [https://ru.wikipedia.org/wiki/Peer]*

«Цикада 3301»[15], которая в 2012 году дала много пищи для рассуждений на тему возможностей DarkNet и способов раскрыть их, опираясь на принцип анонимности. Кроме всего прочего здесь существуют свои доски объявлений (например, 8chan, nntpchan), для покупки разных товаров есть онлайн-рынки (Alphabay, Hansa), блоги (OnionNews, Deep Web Radio), даже своя энциклопедия – Hidden Wiki, где можно найти статьи на самые разные темы, а также ссылки на другие сайты ресурса. Dark Web предоставляет людям полную свободу слова и информации, становясь, таким образом, надёжной защитой демократии. Каждый пользователь может посредствам данной сети сообщить о чем-то неправомерном прессе без опасения быть рассекреченным, если не желает этого сам.

Но свою известность DarkNet получил вследствие противоправной деятельности. Выступает он в роли так называемого «чёрного рынка», где можно купить или продать что угодно, любую контрабанду, украденную вещь или незаконно добытую информацию.

Можно выделить несколько видов преступности [3]:

1) связанная с оборотом наркотиков, оружия, поддельных документов (от любого удостоверения личности до визы почти во все государства мира) компьютерной информации (например, похищение хакерами секретных документов);

2) связанная с незаконным контентом сексуального характера;

3) в сфере экономики (оборот поддельных банковских карт и их данных);

4) экстремистской направленности;

5) насильственная преступность (возможность найти киллера, исполнителя эвтаназии, суицида и др., а также работорговля и организация подпольных боев «на смерть»);

6) связанная с нарушением прав интеллектуальной собственности (библиотеки, фонотеки и пр., зачастую с незаконным контентом). Данный вид преступности не столь распространён в «Тёмной паутине» по причине его процветания на просторах обычного интернет-пространства.

В статье Р.М. Узденова «Новые границы киберпреступности» [3] автор сообщает о необходимости особой правовой регламентации этой технологии, потому как повышенный уровень анонимности и возможность свободного доступа к запрещённым ресурсам представляют Tor-технологии как идеальное подспорье для совершения ряда тяжких и даже особо тяжких преступлений.

В случае с киберпреступлениями (взлом, вирусописательство, атака на IT-ресурсы) дело обстоит проще. Написать программу, снимающую защи-

[15] «Цикада 3301» – название таинственной организации, которая публикует в DarkNet увлекательные головоломки, требующие не только сообразительности, но и глубоких знаний и активных путешествий. [https://habrahabr.ru/post/211182/]

ту с конфиденциальных данных, или создать ботнет[16] для DDoS-атак[17] (англ. Distributed Denial of Service) – преступление, борьба с которым может целиком идти в сфере технологий. А чтобы очистить от преступников пространство DarkNet, технологического противодействия преступникам совершенно недостаточно.

Нужно понимать, что преступное сообщество имеет в своем распоряжении гораздо большее количество ресурсов и методов манипулирования ими в отличии от правоохранительных органов, обязанных проводить какие-либо обыски и/или аресты только посредствам исков, доказательных аргументов и постановлений. Поэтому, самым эффективным из возможных методов для оперативников остается, так называемая, контрольная закупка, а также внимательный поиск открытой информации, выставленной преступником в сеть.

С 2013 года правоохранительные органы РФ призывали запретить Tor. Об этом говорили и глава ФСБ Александр Бортников, и общественный совет ФСБ вместе с адвокатом Эдварда Сноудена Анатолием Кучереной, и руководитель думского комитета по информационной политике, информационным технологиям и связи Леонид Левин. В июле 2014 года МВД России от лица научно-производственного объединения «Специальная техника и связь» (НПО «СТиС») объявило тендер на исследование возможности получения доступа к данным пользователей анонимной сети Tor. Стоимость работ оценивали в 3,9 миллиона рублей, однако Центральный научно-исследовательский институт экономики, информатики и систем управления (ЦНИИ ЭИСУ) не уложился в сроки, в виду чего МВД прибегло к суду. [4, 5]

В августе 2015 года корпорация IBM призвала компании всего мира отказаться от использования сети Tor и заблокировать её во всех корпоративных системах в связи с тем, что она подвергает их риску хакерских атак. [6]

В июле 2016 года Александр Бортников, директор ФСБ, снова поднял вопрос о необходимости решения проблемы анонимности в интернете. А с 1 ноября 2017 года в России VPN-сервисы и анонимайзеры обязаны блокировать доступ к запрещённому в РФ контенту. [7] Под действие этого закона попадает и браузер Tor, так как даёт возможность обойти блокировки. Но за пользование им ответственности пока не предусмотрено.

Спецслужбы по всем миру активно работают над установлением личностей преступников, которые пользуются «подпольным интернетом». На-

[16] Ботнет (англ. «botnet») – это сеть компьютеров, заражённых вредоносной программой поведения Backdoor, позволяющей киберпреступникам удалённо управлять заражёнными машинами (каждой в отдельности, частью компьютеров, входящих в сеть, или всей сетью целиком) без ведома пользователя. Такие программы называются ботами. [https://it-sektor.ru/botnety-/-botnets.html]

[17] DoS-атака (от англ. Denial of Service – «отказ в обслуживании») и DDoS-атака (Distributed Denial of Service – «распределённый отказ обслуживания») – разновидности атак злоумышленника на компьютерные системы, целью которых является создание таких условий, при которых легитимные пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён. [https://it-sektor.ru/dos-ataka.html]

пример, осенью 2016 года в рамках международной операции «Титан» полиция Швеции установила личности 3000 покупателей наркотиков в Tor. [8] Это не первая интервенция силовиков в DarkNet. Ранее, в феврале 2015-го ФБР провело другую примечательную операцию, целью которой был крупнейший сайт детской порнографии. ФБР смогло найти и арестовать модераторов и администраторов портала. [9]

Правоохранительные органы не раскрывают технические подробности операций и то, как именно они находили нарушителей. За последние годы американские спецслужбы провели несколько операций в DarkNet, хотя законность этих методов до сих пор не определена: например, в деле о сайте с детской порнографией суд отказался принимать улики, потому что «ордер на такую технологию обыска в сети был выдан без надлежащей юрисдикции».

На основании изученных данных можно сделать лишь о том, что вопрос о DarkNet, его существовании, предоставляемой им информации и его регулировании, на сегодняшний день остаётся открытым. Службы безопасности и технологические корпорации разных стран не оставляют попыток создания если не законодательно управляемой среды, то прекращения существование DarkNet как такового.

В связи с отсутствием удовлетворительного правового регулирования данной стороны Сети, правоохранительным органам доступны лишь незначительные методы влияния на последствия существования «тёмного» Интернета, что является несоизмеримой мелочью по сравнению с разрушительными возможностями его негативных сторон.

Список литературы

1. Википедия. Даркнет. [Электронный ресурс]. – URL: https://ru.wikipedia.org/ wiki/ Даркнет#cite_note-4. (дата обращения: 03.03.2018).

2. Новиков Игорь. «История Darknet и семь заблуждений о ней» // Интернет-журнал «ИТ Медиа». 2017. [Электронный ресурс]. – URL: http://www.it-world.ru/tech/ science/ 133437.html (дата обращения: 28.02.2018).

3. Узденов Расул Магометович. «Новые границы киберпреступности» // Всероссийский криминологический журнал. 2016. [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/novye-granitsy-kiberprestupnosti (дата обращения: 03.03.2018).

4. «МВД подписало контракт на проведение исследований возможности взлома анонимной сети Tor» // Информационный портал SecurityLab.ru. 2014. [Электронный ресурс]. – URL: https://www.securitylab.ru/news/456957.php. (дата обращения: 28.02.2018).

5. Коломыченко Мария. «TOR хозяйствующих субъектов» // Издательский дом Коммерсантъ. 2015. [Электронный ресурс]. – URL: https://www.kommersant.ru/ doc/ 2861002. (дата обращения: 28.02.2018).

6. «В IBM призвали отказаться от использования Tor» // Информационный портал NEWSru.com. 2015. [Электронный ресурс]. – URL: https://hitech.newsru.com/ article/ 31aug2015/ibmnotor. (дата обращения: 28.02.2018).

7. Тодоров Владимир. «Анонимы не плачут. Почему в России запретили VPN и Tor» // Электронное периодическое издание ООО «Лента.Ру». 2017. [Электронный ресурс]. – URL: https://lenta.ru/articles/2017/07/21/notorandvpn/. (дата обращения: 10.03.2018).

8. Нилов Степан. «Операция «ТИТАН»: как полиция деанонимизировала покупателей наркотиков в Даркнете по всему миру» // Интернет-журнал FURFUR. 2016. [Электронный ресурс]. – URL: http://www.furfur.me/furfur/changes/changes/219311-hyperion. (дата обращения: 10.03.2018).

9. Нилов Степан. «Как агенты ФБР 13 дней управляли крупнейшим сайтом Даркнета с детской порнографией» // Интернет-журнал FURFUR. 2016. [Электронный ресурс]. – URL: http://www.furfur.me/furfur/changes/changes/216879-playpen. (дата обращения: 10.03.2018).

10. Бурцев С.Е. «Причины роста числа российских пользователей анонимной сети Tor и влияние PR-кампаний на интерес к скрытым интернет-сервисам» // ИТпортал. 2017. [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/prichiny-rosta-chisla-rossiyskih-polzovateley-anonimnoy-seti-tor-i-vliyanie-pr-kampaniy-na-interes-k-skrytym-internet-servisam (дата обращения: 03.03.2018).

11. Богатырева О.Н., Шмулевич Т.В. «К вопросу о существовании управления денежными потоками на предприятиях» // Сборник «Институты и механизмы инновационного развития: мировой опыт и российская практика». Сборник научных статей 7-й международной научно-практической конференции. В 3-х томах. Ответственный редактор А.А. Горохов. 2017. С. 140-144.

12. Мельчаков Ю.А., Чуркина В.В., Макаревич М.Л. «Роль краудфандинга в предпринимательской деятельности и вопросы его правового регулирования» // Сборник «Исследование инновационного потенциала общества и формирование направлений его стратегического развития». Сборник научных статей 7-й Всероссийской научно-практической конференции с международным участием. Ответственный редактор А.А. Горохов. 2017. С. 265-267.

13. Структура и особенности мирового рынка золота/ Горохов А.А., Пайкович П.Р.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 1 (19). С. 87-93.

14. Экономическое содержание и назначение государственных внебюджетных фондов/ Пайкович П.Р., Горохов А.А.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 1 (19). С. 266-271.

15. Особенности производства и реализации золота на международных рынках/ Горохов А.А., Пайкович П.Р.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 2 (20). С. 49-53.

16. Анализ бюджета федерального фонда обязательного медицинского страхования РФ/ Пайкович П.Р.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 2 (20). С. 137-142.

17. Экономическое содержание и назначение государственных внебюджетных фондов/ Пайкович П.Р., Горохов А.А.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 1 (19). С. 266-271.

18. Структура и особенности мирового рынка золота/ Горохов А.А., Пайкович П.Р.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 1 (19). С. 87-93.

19. Правовые основы бизнеса. наука и практика/ Мохоров Д.А., Демидов В.П., Мохорова А.Ю., Макаревич М.Л., Доровская Ю.В.// Монография / Санкт-Петербург, 2015.

20. Вопросы правового регулирования деятельности транснациональных корпораций/ Антонова П.А., Макаревич М.Л.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 1 (19). С. 12-18.

21. Проблемы повышения ответственности транснациональных корпораций в области соблюдения прав работников/ Макаревич М.Л., Антонова П.А.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 1 (19). С. 199-204.

22. Правовой статус офшорных компаний/ Макаревич М.Л., Саранчина С.А.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 1 (19). С. 194-198.

23. Правовые аспекты процедуры медиации в современной России/ Макаревич М.Л., Овчинникова А.С.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 1 (19). С. 211-219.

24. Правовое положение иностранцев в россии и правовое положение российских граждан за границей/ Краева З.В., Макаревич М.Л.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 1 (19). С. 220-224.

25. Международное сотрудничество россии в сфере регулирования трудовых отношений: проблемы и перспективы/ Голубенко Я.А., Макаревич М.Л.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 2 (20). С. 43-48.

26. Проблемы трудоустройства инвалидов на предприятиях торговли/ Макаревич М.Л., Митрофанова М.И., Митрофанов А.А.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 3 (21). С. 68-72.

27. Правовое положение отечественных и иностранных юридических лиц - участников внешнеэкономической деятельности согласно российскому законодательству/ Макаревич М.Л., Абдулазизова Р.Д.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 1 (19). С. 188-194.

28. Особенности правого статуса государства, как субъекта внешней экономической деятельности/ Макаревич М.Л., Малышева Н.Н.// Инновационная экономика: перспективы развития и совершенствования. 2017. № 1 (19). С. 205-210.

***Dzhumadil Ekaterina Evgenevna**, student*
(e-mail: kit_96@list.ru)
***Makarevich Marina Leonidovna,** Cand.Hist.Sci., associate professor*
(e-mail: makarevichm@mail.ru)
Peter the Great St. Petersburg Polytechnic University, Saint Petersburg, Russia

THE WAYS OF ILLEGAL USE OF INTERNET OPPORTUNITIES AND ISSUES OF LEGAL REGULATION

***Abstract.** This article describes the main types of illegal use of the Internet space, and also the legal aspects of the regulation of this crime type.*

***Keywords:** Internet, Dark web, DarkNet, cybercrime, computer fraud, Tor-networks, hacking, banned Internet content, legal regulation.*