ISSN 2500-4255

УДК 343.9
DOI 10.17150/2500-4255.2016.10(4).649-655

НОВЫЕ ГРАНИЦЫ КИБЕРПРЕСТУПНОСТИ

Р.М. Узденов
Северо-Кавказский федеральный университет, г. Ставрополь, Российская Федерация

Информация о статье

Дата поступления
23 ноября 2015 г.

Дата принятия в печать
18 ноября 2016 г.

Дата онлайн-размещения
29 декабря 2016 г.

Ключевые слова
Интернет; глубокий; глубинный; невидимый; анонимный; киберпреступность; криминология; сеть TOR

Аннотация. Несмотря на относительно недавнее возникновение киберпреступности, криминологи накопили значительное количество информации, касающейся ее состояния, детерминации, виктимологических аспектов, личностных особенностей правонарушителей, и продолжают постоянный поиск (зачастую более чем успешный) новых направлений борьбы с указанным явлением. Однако подавляющее число соответствующих научных изысканий, так или иначе затрагивающих сеть Интернет, приходится лишь на малую ее часть — «видимый» Интернет, известный большинству пользователей.

В этой связи в статье ставится проблема необходимости проведения криминологического анализа киберпреступности с учетом особенностей глубинного сегмента Всемирной паутины — «темного» Интернета, значительную часть которого составляет сеть TOR (от англ. The Onion Router — «луковый маршрутизатор»), не индексируемая обычными поисковыми системами типа «Гугл», «Яндекс» и т.п.

Проведенное автором в период с 2012 по 2015 г. посредством наблюдения исследование «невидимого» Интернета позволило предпринять попытку выделения основных составляющих структуры преступности TOR-сети, которые обладают ярко выраженной спецификой. Учитывая тот факт, что TOR представляет собой свободное и открытое программное обеспечение для реализации «луковой маршрутизации» второго поколения, позволяющее сформировать анонимную сеть виртуальных туннелей, открывающую возможность передачи данных в зашифрованном виде, а точнее, систему прокси-серверов для анонимного сетевого соединения, защищенного от прослушивания, автор предлагает рассматривать преступность TOR-сети в качестве относительно новой, самостоятельной разновидности киберпреступности, обособленной по причине специфики криминологических характеристик образующих ее преступлений, и указывает на необходимость переоценки существующих результатов криминологических исследований обычной киберпреступности.

NEW FRONTIERS OF CYBERCRIME

Rasul M. Uzdenov
North-Caucasus Federal University, Stavropol, the Russian Federation

Article info

Received
2015 November 23

Accepted
2016 November 18

Available online
2016 December 29

Keywords
Internet; deep; profound; hidden; anonymous; computer crimes; criminology; TOR network

Abstract. Although cybercrime is a relatively recent phenomenon, criminologists have accumulated a considerable amount of information regarding its condition, determining factors, victimological aspects, personal characteristics of offenders; they continue their constant (and, often, more than successful) search for new ways to counteract it. However, the overwhelming majority of research examining the Internet in one way or another describes but a small part of it — the «visible» net, known to most of the users.

The paper discusses the necessity of conducting a criminological analysis of cybercrime that would take into consideration the deep segment of the world wide web — the dark web, a significant part of which is the TOR network (TOR standing for The Onion Router) whose contents are not indexed by standard search engines like Google or Yandex.

The author did a monitoring of the «invisible» web in 2012–2015, which allowed him to single out key components of the TOR network crime structure, which have their own prominent characteristics. TOR is a free and open software for second-generation «onion routing» that makes it possible to establish an anonymous network of virtual relays for transferring encrypted data, or, to be more exact, a system of proxy servers for anonymous network connection protected against surveillance; the author suggests viewing TOR network crime as a relatively new, independent type of cybercrime, distinguished from other types by the criminological characteristics of its offences. The author also points out that it is necessary to reconsider the existing results of criminological research of regular cybercrimes.

ISSN 2500-4255

Сеть Интернет и другие компьютерные технологии уже давно и прочно вошли в нашу повседневную жизнь, создав, по сути, качественно новый вид социума — виртуальное общество. Став отражением офлайновой реальности, глобальная сеть получила от нее в наследство как позитивные, так и негативные явления. К числу последних в первую очередь можно отнести преступность, которая в кратчайшие сроки взяла на вооружение новейшие информационные технологии. В результате возникли неизвестные до этого хакерство, кибертерроризм [1; 2], киберэкстремизм [3, с. 87; 4, с. 464; 5], кибервойны [6], компьютерное мошенничество [7; 8] и другие виды киберпреступности [9; 10].

В последние годы благодаря усилиям правоохранительных органов было раскрыто немало таких преступлений и множество виновных понесли заслуженное наказание[1]. Как следствие, на просторах Всемирной паутины заметно уменьшился объем противоправного контента. Однако позитивные сдвиги в рассматриваемой сфере затронули лишь верхушку криминального айсберга в сети. Значительная часть существовавших и существующих на виртуальной поверхности Интернета девиаций не исчезла, а спустилась в не индексируемые обычными поисковыми машинами недра всемирной компьютерной сети, образовав так называемый глубинный Интернет (синонимы: «глубокий» Интернет, глубокий веб, «глубокая» Паутина, «невидимый» Интернет, «невидимая» Паутина, анонимный Интернет, invisible web, Deep web, Hidden web): «Невидимый интернет — это ресурсы, которые не обнаруживаются поисковыми машинами, а также порталы, сайты и т.д., доступ к которым предполагает либо платный характер, либо наличие специального разрешения на использование ресурсов. По имеющимся данным, в невидимом интернете находится порядка 90 % всего ценного научно-технического, технологического, финансово-экономического и государственного открытого контента. Объемы невидимого интернета постоянно растут» [11, с. 5–6].

Существенную часть «невидимого» Интернета в настоящее время составляет TOR-сеть. TOR (от англ. The Onion Router) — свободное и открытое программное обеспечение для реализации так называемой луковой маршрутизации второго поколения [12], представляющее собой систему прокси-серверов, которая позволяет устанавливать анонимное сетевое соединение с защитой от прослушивания. TOR можно рассматривать как анонимную сеть виртуальных туннелей [13, p. 361], осуществляющую передачу данных в зашифрованном виде.

Посредством TOR пользователи Интернета могут анонимно посещать сайты, вести блоги, отправлять почтовые сообщения, а также работать с другими приложениями, использующими протокол TCP. Сохранение анонимности трафика происходит за счет использования распределенной сети серверов. Помимо этого, технология TOR обеспечивает защиту от инструментов анализа трафика [14], которые не только угрожают деанонимизации в Интернете [15], но и компрометируют конфиденциальность деловых контактов, коммерческую тайну и тайну связи в целом.

О высокой степени анонимности, обеспечиваемой TOR-сетью, свидетельствует тот факт, что небезызвестный Эдвард Сноуден использовал ее для передачи газетам The Washington Post и The Guardian информации о совершенно секретном комплексе мероприятий, осуществляемых американским Агентством национальной безопасности с целью негласного массового сбора информации, передаваемой по сетям электросвязи[2].

Наше исследование TOR-сети, промежуточные результаты которого были опубликованы ранее [16; 17], осуществлялось в период с 2012 по 2015 г. Приведенные далее эмпирические данные получены главным образом в результате комплексного применения научных методов скрытого, эпизодического, нестандартизированного, включенного и исключенного наблюдения за процессами и явлениями в TOR-сети, а также опроса посетителей TOR-сети в виде полустандартизированного интервью при строгом соблюдении принципа законности. Использование указанной методики позволило в общих чертах сформировать субъективное представление о структуре преступности «невидимой» Паутины, которая, как мы полагаем, имеет весьма существенные как качественные, так и количественные особенности в сравнении с традиционной киберпреступностью.

Здесь сразу следует отметить чрезвычайную сложность любых попыток оценки крими-

[1] Управление «К» ликвидировало более 100 сайтов // Geektimes. 2007. 7 февр. URL : http://geektimes.ru/post/3054.

[2] Snowden und das Tor-Netzwerk // Daserste.de. URL : http://www.daserste.de/information/wissen-kultur/ttt/sendung/br/20130630-ttt-darknet-102.html.

нологических характеристик преступности не только «глубинного» Интернета, но и его «видимой» части и высокую степень относительности ее результатов. Это объясняется и их значительной латентностью, и относительной приспособленностью традиционных криминологических методик исследования киберпреступности, а также рядом иных факторов, которые требуют отдельного анализа. А потому, не претендуя на исключительность, позволим себе вынести на суд общественности собственную, субъективно воспринимаемую теоретическую конструкцию преступности в пределах TOR-сети, которую образуют следующие сегменты:

1. *Преступность, связанная с незаконным контентом сексуального характера.* Точное количество ресурсов с детским порно в TOR-сети определить практически невозможно, однако их масштабы поистине грандиозны. Объем материалов некоторых сайтов исчисляется сотнями гигабайт. Лица, задействованные при совершении этого вида преступлений, как правило, самоорганизуются в «клубы по интересам» посредством тематических сайтов и форумов, где обмениваются фотографиями и делятся опытом. Некоторые из этих ресурсов открыты для всех желающих, другая часть доступна при условии определенного «взноса» в существующую коллекцию порноматериалов: добавление видео- и фотоматериалов, как вариант — описание собственного сексуального контакта с малолетними. Зачастую преступники бравируют своими «достижениями», создавая сайты, посвященные их собственным деяниям и жертвам. К их услугам — служба знакомств соответствующей направленности, каталоги, теги, возможности комментирования материалов. Содержание контента представлено полным спектром шкалы COPINE (Combating Online Paedophile Information Networks in Europe) [18] — десять градаций от indicative (намекающий) до sadistic / bestiality (садизм / сношения в животными) и шкалы SAP (Sentencing Advisory Panel)[3] — пять градаций от Nudity or erotic posing with no sexual activity (нагота или эротические позы без сексуальной активности) до Sadism or bestiality (садизм или сношения с животными), а также шкалы SODG (Sexual Offences Definitive Guideline, с 1 апреля 2014 г. заменившей шкалу SAP)[4] в трех категориях: A — изображение проникающей половой активности, зоофилии или садизма; B — изображение непроникающей сексуальной активности; C — другие неприличные изображения, не относящиеся к категории A или B.

Возраст жертв, как правило, каталогизирован ячейками: 0–3 года, 4–7 лет, 8–12 лет, 13–15 лет и 16–17 лет. Причем порнографические материалы с изображением жертв в возрасте 1–2 месяцев (!) мало уступают по объему аналогичному контенту с жертвами, находящимися в пубертатном периоде.

2. *Преступность, связанная с оборотом наркотиков.* На соответствующих тематических страницах содержится информация о возможности приобретения, изготовления, переработки и прочих действий, связанных практически с любыми видами наркотиков и сопутствующих им веществ, а также о возможности приобретения и изготовления разнообразных технических средств и оборудования для создания соответствующих лабораторий. Нам неизвестен ни один из видов наркотических средств, который не мог бы быть предложен к реализации в «глубокой» Паутине. Здесь же можно поделиться опытом, обсудить продавцов, покупателей и качество «товара».

3. *Преступность, связанная с оборотом компьютерной информации,* включает в себя многочисленные действия, касающиеся неправомерного доступа к информации. В частности, в TOR-сеть выложены секретные документы, похищенные хакерами из самых разнообразных источников: почтовые, электронные адреса и иные персональные данные должностных лиц милитаризированных органов Европы и т.п. В соответствующих разделах предоставляется возможность заказать DDoS-атаки, взлом конкретной электронной почты, сайта, программного обеспечения или даже компьютерной игры. Обращает на себя внимание уровень профессионализма хакеров, предлагающих услуги по взлому того или иного объекта: время от получения информации о заказе до обнаружения уязвимости в объекте и принятия решения о готовности принять заказ составляет шесть минут.

4. *Преступность в сфере экономики.* Этот вид преступности включает в основном дей-

[3] Regina v Oliver case summary. COURT OF APPEAL Criminal Division. URL : http://www.inquisition21.com/pca_1978/reference/oliver2002.html.

[4] Sentencing Council — Sexual Offences Definitive Guideline. URL : https://www.iwf.org.uk/assets/media/hotline/Sentencing%20Councils%20Sexual%20Offences%20Definitive%20Guideline%20April%202014.pdf.

ствия, связанные с оборотом поддельных банковских карт и их данных. Данные банковских карт, как известно, позволяют без соответствующего ПИН-кода совершать покупки в интернет-магазинах. Цены на эту продукцию отличаются демократичностью — в 2015 г. около 4 тыс. р. за данные одной карты. При оптовой покупке предлагаются существенные скидки. Более высокие цены предусмотрены за двусторонние изображения банковских карт и их ПИН-коды, с помощью которых можно изготовить реальную карту для оплаты покупок в обычных магазинах. Данные банковских карт злоумышленники традиционно получают посредством скиммеров (приборов, устанавливаемых на банкоматах), которые также можно приобрести в «невидимой» Паутине. Кроме того, соответствующие ресурсы позволяют найти компетентных сообщников для получения инсайдерской информации — работников различных структур, имеющих доступ к сведениям, составляющим коммерческую или иные виды тайн. Помимо этого, свои услуги предлагают фальшивомонетчики и торговцы имуществом, полученным преступным путем.

5. *Преступность экстремистской направленности.* TOR-сеть используют экстремисты самого широкого спектра — от ультраправых до ультралевых. Доступ к ценной информации той или иной группировки открывается проверенным в реальных акциях лицам. В частности, экстремистами из Дании охотно распространяется персональная информация о неугодных компетентных лицах, как правило, силовых органов — телефоны, почтовые адреса, имена родственников и т.п.

6. *Преступность, связанная с оборотом поддельных документов.* Потенциальным покупателям предлагается широкий их ассортимент — от любого удостоверения личности до визы почти во все государства мира. Как правило, поддельные документы пересылаются покупателям обычной почтой в тайниках.

7. *Преступность, связанная с оборотом оружия.* Наибольшей популярностью у покупателей оружия пользуются модели пистолетов Desert Eagle и Glok. Доставка — почтой составными частями по всему миру.

8. *Насильственная преступность.* В «невидимом» Интернете есть возможность найти киллера, исполнителя или заказчика эвтаназии, суицида и др. К этой же категории преступности мы относим и существующие в сети TOR работорговлю и организацию подпольных боев «на смерть».

9. *Преступность, связанная с нарушением прав интеллектуальной собственности.* В TOR-сети имеются различные библиотеки, фонотеки и пр., зачастую с незаконным контентом. Данный вид преступности не столь распространен в «глубинной» Паутине по причине его процветания на просторах обычного интернет-пространства.

Российский сегмент преступности TOR-сети в целом отражает ее мировую структуру, но отличается более высокими ценами на соответствующие услуги. Как правило, все операции в сети TOR оформляются через взимающих со сделки определенный процент посредников. Чаще всего валютой в торговом обороте TOR-сети выступает биткоин.

Обеспокоенность российских правоохранителей преступностью «невидимого» Интернета обусловила появление на сайте госзакупок МВД РФ в июле 2014 г. заказа на «Исследование возможности получения технической информации о пользователях (пользовательском оборудовании) анонимной сети TOR», шифр «TOP (Флот)». Конкурс среди потенциальных исполнителей был закрытый, стоимость контракта составила 3 900 тыс. р.[5] В августе того же года стало известно о заключении соответствующего договора с неназванной российской компанией[6]. Ранее мы отмечали, что, несмотря на безусловно позитивный характер заявляемых правоохранителями целей, указанный тендер следует воспринимать с определенной долей скептицизма, кроме того, необходимо объективно оценивать соответствующие коррупционные риски при его реализации [17]. Позже сомнения в результативности подобных исследований высказали эксперты из компаний «Лаборатория Касперского», Symantec и The Tor Project, Inc. [19; 20].

Между тем и ранее правоохранителями различных стран неоднократно предпринимались попытки взять под контроль TOR-сеть [21–26]. Однако, несмотря на все усилия и значительные затраты, было признано невозможным созда-

[5] Портал закупок. Закупка № 0373100088714000008 // Единая информационная система в сфере закупок : офиц. сайт. URL : http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber=0373100088714000008.

[6] МВД подписало контракт на проведение исследований возможности взлома анонимной сети Tor // SecurityLab.ru. URL : http://www.securitylab.ru/news/456957.php.

ние действенного механизма по выявлению конечных пользователей TOR[7].

Автор не относится к числу сторонников полного запрета TOR-сети, поскольку признает за законопослушными гражданами право на анонимность в виртуальном пространстве. Дискуссионный характер данной проблемы не оспаривается, но явно выходит за границы предмета нашего исследования.

Вместе с тем вполне очевидна необходимость принятия самых решительных мер по противодействию преступности «глубинного» Интернета. И несмотря на то что соответствующий комплекс мер еще предстоит создать, его разработка должна проводиться с активным привлечением IT-специалистов на основе международного сотрудничества оперативно-технических подразделений компетентных органов.

Изложенное позволяет рассматривать преступность TOR-сети как относительно новую, самостоятельную разновидность киберпреступности, обособленную по причине специфики криминологических характеристик образующих ее преступлений и незаслуженно обделенную вниманием российской криминологической науки. Данное обстоятельство обусловливает необходимость переоценки известных на сегодняшний день результатов криминологических исследований киберпреступности.

[7] OpenNews: Опубликованы материалы о методах АНБ по получению контроля за пользователями TOR. URL : http://www.opennet.ru/opennews/art.shtml?num=38087.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Collin B. The Future of Cyberterrorism / B. Collin // Crime & Justice International Journal. — 1997. — Vol. 13, iss. 2. — P. 51–71.

2. Lewis J. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats [Electronic resource] / J. Lewis // Center for Strategic and International Studies. — 2002. — Dec. — Mode of access : http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

3. Пудовочкин Ю.Е. Теоретические конструкции определения экстремизма: проблемы и перспективы / Ю.Е. Пудовочкин, Р.М. Узденов // Криминологический журнал. — 2005. — № 2. — С. 84–87.

4. Узденов Р.М. К вопросу об определении объекта преступных проявлений экстремизма / Р.М. Узденов // «Черные дыры» в российском законодательстве. — 2007. — № 2. — С. 464–465.

5. Узденов Р.М. Профилактический эффект общесоциального воздействия на истоки экстремизма / Р.М. Узденов // Бизнес в законе. — 2009. — № 3. — С. 93–95.

6. Gable K.A. Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent / Kelly A. Gable // Vanderbilt Journal of Transnational Law. — 2010. — Vol. 43, № 1. — P. 57–118.

7. Титарева Е.Г. Мошенничество, совершаемое с использованием информационно-телекоммуникационных технологий / Е.Г. Титарева // Научный альманах. — 2015. — № 7 (9). — С. 1158–1161.

8. Лопатина Т.М. Проблемы уголовно-правовой защиты сферы компьютерной информации: современный взгляд на мошенничество / Т.М. Лопатина // Право и безопасность. — 2013. — № 3–4 (45). — С. 89–95.

9. Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления / И.М. Рассолов // Юридический мир. — 2008. — № 2. — С. 44–46.

10. Номоконов В.А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. — 2012. — № 24. — С. 45–55.

11. Ларина Е.С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден / Е.С. Ларина, В.С. Овчинский. — М. : Кн. мир, 2014. — 352 с.

12. Dingledine R. Tor: The Second-Generation Onion Router [Electronic resource] / Roger Dingledine, Nick Mathewson, Paul Syverson // Onion Routing. — Mode of access : http://www.onion-router.net/Publications/tor-design.pdf.

13. Tanenbaum A.S. Computer networks / Andrew S. Tanenbaum, David J. Wetherall. — 5th ed. — N.Y. : Prentice Hall, 2011. — 960 p.

14. Syverson P. Onion routing for resistance to traffic analysis / P. Syverson // Proceedings of the DARPA Information Survivability Conference and Exposition. — Washington, DC, USA, 2003. — Vol. 2. — P. 108–110.

15. David E.E. Some Thoughts About the Social Implications of Accessible Computing / E.E. David, R.M. Fano // Proceedings of the Fall Joint Computer Conference, Las Vegas, NV, November 30 — December 1, 1965. — N.Y., 1965. — P. 243–247.

16. Узденов Р.М. Структура преступности «глубинного интернета» / Р.М. Узденов // Актуальные проблемы современного уголовного права и криминологии : материалы ежегод. межвуз. круглого стола, посвящ. Дню рос. науки, Ставрополь, 8 февр. 2013 г. — Ставрополь : Изд-во Ставроп. гос. аграр. ун-та, 2013. — С. 239–243.

17. Узденов Р.М. Преступность «невидимого» Интернета / Р.М. Узденов // Российский криминологический взгляд. — 2014. — № 3. — С. 218–221.

18. Taylor M. Typology of Paedophile Picture Collections / Max. Taylor, Gemma Holland, Ethel Quayle // Police Journal. — 2001. — Vol. 74. — P. 97–107.

19. Зыков В. Российским правоохранительным органам не понравилась анонимность шифрованного интернета [Электронный ресурс] / В. Зыков, А. Криворучек // Izvestia.Ru. — 2014. — 25 июля. — Режим доступа : http://izvestia.ru/news/574345.

20. Лун А. Россия: 3,9 млн рублей за взлом сети TOR [Электронный ресурс] / Алек Лун // inosmi.ru. — 2014. — 25 июля. — Режим доступа : http://inosmi.ru/world/20140726/221937035.html.

21. Мальцев А. TOR заблокирован в Китае, но есть выход [Электронный ресурс] / А. Мальцев // Magazeta.com. — 2009. — 11 окт. — Режим доступа : http://magazeta.com/2009/10/tor-blocked.

22. Poulsen K. FBI Admits It Controlled Tor Servers Behind Mass Malware Attack [Electronic resource] / Kevin Poulsen // Wired.com. — 2013. — Sept. 13. — Mode of access : http://www.wired.com/2013/09/freedom-hosting-fbi.

23. Gellman B. Secret NSA documents show campaign against Tor encrypted network [Electronic resource] / Barton Gellman, Craig Timberg, Steven Rich // The Washington Post. — 2013. — Oct. 4. — Mode of access : https://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story.html.

24. Ализар А. Оператор выходного узла TOR осужден в Австрии [Электронный ресурс] / А. Ализар // Xakep.ru. — 2014. — 3 июля. — Режим доступа : https://xakep.ru/2014/07/03/tor-austria.

25. Monroy M. Europol startet neue Cyber-Patrouille mit US-Behorden, auch das BKA macht mit [Electronic resource] / Matthias Monroy // Netzpolitik.Org. — 2014. — Sept. 1. — Mode of access : https://netzpolitik.org/2014/europol-startet-neue-cyber-patrouille-mit-us-behoerden-auch-das-bka-macht-mit.

26. Weiser B. International Raids Target Sites Selling Contraband on the Dark Web [Electronic resource] / Benjamin Weiser, Doreen Carvajal // The New York Times. — 2014. — Nov. 7. — Mode of access : http://www.nytimes.com/2014/11/08/world/europe/dark-market-websites-operation-onymous.html?_r=0.

REFERENCES

1. Collin B. The Future of Cyberterrorism. *Crime & Justice International Journal*, 1997, vol. 13, iss. 2, pp. 51–71.

2. Lewis J. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic and International Studies*, 2002, December. Available at: http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

3. Pudovochkin Yu.E., Uzdenov R.M. The theoretical constructs of defining extremism: issues and prospects. *Kriminologicheskii zhurnal = Journal of Criminology*, 2005, no. 2, pp. 84–87. (In Russian).

4. Uzdenov R.M. To the issue of defining the object of criminal extremist manifestations. *«Chernye dyry» v rossiiskom zakonodatel'stve = «Black Holes» of Russian Legislation*, 2007, no. 2, pp. 464–465. (In Russian).

5. Uzdenov R.M. The preventative effect of general social impact on the sources of extremism. *Biznes v zakone = Business in Law*, 2009, no. 3, pp. 93–95. (In Russian).

6. Gable Kelly A. Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent. *Vanderbilt Journal of Transnational Law*, 2010, vol. 43, no. 1, pp. 57–118.

7. Titareva E.G. Fraud committed using information and telecommunication technologies. *Nauchnyi al'manakh = Science Almanac*, 2015, no. 7 (9), pp. 1158–1161. (In Russian).

8. Lopatina T.M. Problems of criminal protection of computer information: a modern view on fraud. *Pravo i bezopasnost' = Law and Security*, 2013, no. 3–4 (45), pp. 89–95. (In Russian).

9. Rassolov I.M. Cybercrimes: concept, key characteristics, manifestations. *Yuridicheskiy mir = The Legal World*, 2008, no. 2, pp. 44–46. (In Russian).

10. Nomokonov V.A., Tropina T.L. Cybercrime as a new criminal threat. *Kriminologiya: vchera, segodnya, zavtra = Criminology: Yesterday, Today, Tomorrow*, 2012, no. 24, pp. 45–55. (In Russian).

11. Larina E.S., Ovchinskii V.S. *Kibervoiny XXI veka. O chem umolchal Edvard Snouden* [Cyberwars of the 21st century. What Edward Snowden withheld]. Moscow, Knizhnyi mir Publ., 2014. 352 p.

12 Dingledine Roger, Mathewson Nick, Syverson Paul. Tor: The Second-Generation Onion Router. *Onion Routing*. Available at: http://www.onion-router.net/Publications/tor-design.pdf.

13. Tanenbaum Andrew S., Wetherall David J. *Computer networks.* 5th ed. New York, Prentice Hall, 2011. 960 p.

14. Syverson P. Onion routing for resistance to traffic analysis. *Proceedings of the DARPA Information Survivability Conference and Exposition.* Washington, DC, USA, 2003, vol. 2, pp. 108–110.

15. David E.E., Fano R.M. Some Thoughts about the Social Implications of Accessible Computing. *Proceedings of the Fall Joint Computer Conference, Las Vegas, NV, November 30 — December 1, 1965*. New York, 1965, pp. 243–247.

16. Uzdenov R.M. The structure of «deep web» crime. *Aktual'nye problemy sovremennogo ugolovnogo prava i kriminologii. Materialy ezhegodnogo mezhvuzovskogo kruglogo stola, posvyashchennogo Dnyu rossiiskoi nauki, Stavropol', 8 fevralya 2013 g.* [Topical Issues of Contemporary Criminal Law and Criminology. The Materials of Annual Inter-University Round Table Dedicated to the Day of Russian Science. Stavropol, February 8, 2013]. Stavropol State Agrarian University Publ., 2013, pp. 239–243. (In Russian).

17. Uzdenov R.M. Crimes of the «invisible» web. *Rossiiskii kriminologicheskii vzglyad = Russian Criminological Outlook*, 2014, no. 3, pp. 218–221. (In Russian).

18. Taylor Max., Gemma Holland, Ethel Quayle. Typology of Paedophile Picture Collections. *Police Journal*, 2001, vol. 7, pp. 97–107.

19. Zykov V., Krivoruchek A. Russian law enforcement did not like the anonymity of the encrypted Internet. *Izvestia.Ru*, 2014, July 25. Available at: http://izvestia.ru/news/574345. (In Russian).

20. Lun Alek. Russia: 3.9 mln rubles for hacking the TOR network. *Inosmi.Ru*, 2014, July 25. Available at: http://inosmi.ru/world/20140726/221937035.html. (In Russian).

21. Mal'tsev A. TOR is blocked in China, but there is a way out. *Magazeta.com,* 2009, October 11. Available at: http://magazeta.com/2009/10/tor-blocked/.(In Russian).

22. Poulsen Kevin. FBI Admits It Controlled Tor Servers Behind Mass Malware Attack. *Wired.com,* 2013, September 13. Available at: http://www.wired.com/2013/09/freedom-hosting-fbi.

23. Gellman Barton, Timberg Craig, Rich Steven. Secret NSA documents show campaign against Tor encrypted network. *The Washington Post*, 2013, October 4. Available at: https://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story.html.

24. Alizar A. TOR exit node operator prosecuted in Austria. *Xakep.ru*, 2014, July 3. Available at: https://xakep.ru/2014/07/03/tor-austria. (In Russian).

25. Monroy Matthias. Europol startet neue Cyber-Patrouille mit US-Behorden, auch das BKA macht mit. *Netzpolitik.Org*, 2014, September 1. Available at: https://netzpolitik.org/2014/europol-startet-neue-cyber-patrouille-mit-us-behoerden-auch-das-bka-macht-mit.

26. Weiser Benjamin, Carvajal Doreen. International Raids Target Sites Selling Contraband on the Dark Web. *The New York Times*, 2014, November 7. Available at: http://www.nytimes.com/2014/11/08/world/europe/dark-market-websites-operation-onymous.html?_r=0.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Узденов Расул Магометович — доцент кафедры уголовного права и процесса Юридического института Северо-Кавказского федерального университета, кандидат юридических наук, доцент, г. Ставрополь, Российская Федерация; e-mail: rasul.uzdenov@yandex.ru.

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Узденов Р.М. Новые границы киберпреступности / Р.М. Узденов // Всероссийский криминологический журнал. — 2016. — Т. 10, № 4. — С. 649–655. — DOI : 10.17150/2500-4255.2016.10(4).649-655.

INFORMATION ABOUT THE AUTHOR

Uzdenov, Rasul M. — Ass. Professor, Chair of Criminal Law and Procedure, Law Institute, North-Caucasus Federal University, Ph.D. in Law, Ass. Professor, Stavropol, the Russian Federation; e-mail: rasul.uzdenov@yandex.ru.

BIBLIOGRAPHIC DESCRIPTION

Uzdenov R.M. New frontiers of cybercrime. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2016, vol. 10, no. 4, pp. 649–655. DOI: 10.17150/2500-4255.2016.10(4).649-655. (In Russian).