

УДК 336.025.2

Deep Web / Dark Net: баланс между конфиденциальностью (individual privacy) и информационной безопасностью (cybersecurity)

Виктор Владимирович Буряк

кандидат философских наук

доцент кафедры ФЕНП философского факультета

Таврической академии Крымского федерального университета имени В. И. Вернадского
(ФГАОУ ВО «КФУ имени В.И. Вернадского»)

Аннотация. Анализируется проблематика, относящаяся к теме обеспечения кибербезопасности в условиях современного информационного общества и существования так называемого альтернативного киберпространства *Deep Web / Dark Net*. Исследование сфокусировано на междисциплинарной рефлексии относительно необходимых и достаточных мер по поддержанию баланса между информационной открытостью высокотехнологичной экономики и её защищённостью от несанкционированных вторжений. Эффективная экономическая активность граждан и организаций в условиях современного социума во многом определяется государственными стратегиями и целями. Значительный экономический рост во многом зависит не только от финансовых инвестиций в наукоёмкие проекты, но также от степени информационной безопасности для граждан и организаций. Тотальная цифровизация деятельности в постиндустриальных социумах влечёт за собой многочисленные опасности и риски, включая несанкционированное вмешательство в экономическую деятельность корпораций, организаций и личную жизнь граждан. Несмотря на предпринимаемые меры кибербезопасности, количество, материальный и моральный ущерб нанесённый хакерами, увеличивается. Задачи стоящие перед специалистами в сфере защиты государственных и частных данных усложняются ввиду существования *Deep Web / Dark Net*. Условия повышения безопасности хранения и передачи информации в сети интернет должны стать объектом междисциплинарного исследования.

Ключевые слова: информационное общество, киберпреступления, кибербезопасность, *Deep Web / Dark Net*, цифровая экономика

Введение

Актуальность исследования. Идентификация инженерно-технических и программных границ киберпространства не позволяет выделить достаточно точно такой проблематичный в плане легитимности сегмент интернет, который чаще всего называется *Deep Web / Dark Net*, что в переводе с английского может означать: «глубинная сеть», «скрытая сеть», «тёмная часть

интернет», «тёмный интернет», «теневого интернет». Это такая интернетизированная сеть, в которой соединения между информационными ресурсами устанавливаются только между доверенными (и многократно проверенными) IP адресами, с использованием специфицированных протоколов и портов. В киберпространстве *Dark Net* через сеть не связанных между собой виртуальных информационных потоков, предоставляется возможность передачи данных в зашифрованном виде. Обмен файлами в *Dark Net* анонимен, поскольку IP-адреса юзеров скрыты от внешнего контроля. Поэтому пользователи могут надеяться, что их конфиденциальное общение происходит без государственного вмешательства. Независимо от точного перевода, намерений создателей этого параллельного киберпространства и социокультурных коннотаций *Deep Web / Dark Net*, понятно, со «стеклянной ясностью», что меры безопасности при нахождении в интернет-пространстве, каким бы оно ни было, «белым», «серым» или «чёрным» - должны соблюдаться. Ведь на ночных улицах для автомобилистов действуют точно такие же правила дорожного движения, что и в дневное время. Тем не менее, из-за исторически сложившейся иллюзии феномена «абсолютной свободы», в силу живучести либертарианских и крипто анархистских идей в киберпространстве, существования так называемого международного «хактивизма», миф об автономной «территории смыслов для избранных» в глобальной сети интернет в форме *Deep Web / Dark Net* устойчив. Принципом анонимности пользуются киберпреступники для несанкционированного вторжения в базы данных граждан и организаций. Идеология хактивизма основывается на идее относительно анонимного использования компьютеров и глобализированных информационных сетей (интернет) для продвижения либертарианских идей, принципов «свободы слова» и «защиты прав человека». К сожалению, пока что нет универсальных эффективных программных инструментов для «опрозрачивания» *Deep Web / Dark Net* и, тем более контроля информационных потоков в этом сегменте интернетизированного киберпространства. Тем не менее, оптимальное осуществление государственной политики по защите национальной безопасности (*cybersecurity*), рассматривается как приоритетная задача усиления мер безопасности работы граждан в киберпространстве. Укрепление ресурсной базы кибербезопасности обеспечивает оборонительную и наступательную функции защиты национальных интересов. Реальное противостояние конкурирующих за обладание стратегическими информационными ресурсами стран, иногда доходит до ситуации кибервойны (*cyberwarfare*), как составной части перманентной информационной войны. Экспоненциальная цифровизация экономической деятельности в современном обществе неизбежно влечёт многочисленные риски, в том числе несанкционированный доступ преступников к базам данных, находящихся в труднодоступной части киберпространства - *Dark Net*.

Цель исследования заключается в том, чтобы определить социокультурный статус *Dark Net* как такого сегмента киберпространства, который прямо или косвенно угрожает безопасности экономическим интересам государств. Для этого необходимо решить ряд задач: 1) определить место и значение *Dark Net* в планетарном киберпространстве; 2) выделить границы информационной открытости / анонимности *Dark Net*; 3) указать риски для граждан, коммерческих предприятий и государственных учреждений от несанкционированной деятельности киберпреступников, находящихся на территории *Dark Net*. Основная проблема данного исследования состоит в междисциплинарном анализе инструментов, обеспечивающих безопасное использование интернетизированных информационных ресурсов. В легитимном сегменте киберпространства (персональных и корпоративных сайтах, социальных сетях) хранится открытая и конфиденциальная информация. В сегменте «теневого интернет» (*Dark Net*), система гарантированной компьютерной безопасности не работает, поскольку защита компьютерных систем в *Dark Net* дело добровольное, эксклюзивное и потому ситуативное. Проблема обеспечения гарантированной кибербезопасности приобретает все большую значимость из-за экспоненциально растущей значимости социальных сетей [19]. Такие комплексные информационные технологии на которых работают интернетизированные сервисы *Bluetooth* и *Wi-Fi*, *Internet of Things*, *blockchain* и другие, создают существенные программные и технологические проблемы для анонимных киберпреступников / хакеров.

Тема *Dark Web* является междисциплинарной и находится в эпистемологическом фокусе информационных наук, а также антропологии киберантропологии, *media studies*, социологии и других дисциплин, в которых содержатся актуальные размышления о предстоящих социально-политических переменах в эпоху ускоренного продвижения цифровых технологий.

Исследование сфокусировано на анализе возрастающей контркультурной угрозы со стороны альтернативной киберреальности продуцируемой *Deep Web*, структурированной и функционирующей как совокупность сетей анонимного обмена конфиденциальной информацией. Потенциальным обитателям *Deep Web*, со своими информационными ресурсами, закрытыми от пользователей легитимного киберпространства, предлагают эксклюзивные рыночные площадки, альтернативные интернет-поисковики и закрытые социальные сети. Выражение *Deep Web* / *Dark Web* ассоциируется с нелегальным рынком продажи наркотиков (*drug markets*), нелегитимной продажей оружия (*unregulated gun sales*), сбытом украденных кредитных карт (*stolen credit cards*). Проблема криминогенности *Deep Web* носит дискуссионный характер, считает Роберт Гел. Веб-сайты размещённые в *Dark Web* доступны только с помощью специального программного обеспечения для маршрутизации поиска нужной информации. Основные информационные ресурсы *Dark Web* - *Freenet*, *Tor* и *I2P*. Исследование функционирования этих ресурсов, показывает, что использование шифрования

своих сообщений политическими диссидентами в киберпространстве *Dark Web* находится хоть и вне легитимного киберпространства (например, *Google*, *Twitter* или *Facebook*), но в то же время не является криминальной деятельностью. Роберт Гел настойчиво артикулирует ценность анонимного политического дискурса на территории *Dark Web*, что является альтернативной интеллектуальной деятельностью в эпоху тотальной электронной поднадзорности (*ubiquitous surveillance*). Полностью перекрыть информационные потоки на *Dark Web*, считает Роберт Гел, означает элиминировать важный канал для проявления инакомыслия [4].

Создание *Dark Web* некоторые конспирологически мотивированные авторы пытаются непосредственно связать с теорией заговора (*conspiracy theory*). Согласно их представлениям, интернет изначально находится под плотным концептуальным контролем и управлением мощных заговорщических сил (*conspiratorial undercurrents*) [17]. Разумеется, что, будучи централизованной системой маршрутизации информационных потоков, интернет не есть «Дикое поле» криптоанархистов, не хаотическое турбулентное киберпространство. Однако его абсолютная прозрачность и тотальный контроль с математической точки зрения попросту невозможны. Методологический хактивизм, независимо от мотивации и культурных ценностей хакеров («белых», «серых» и «чёрных») содержит в себе реальные и мнимые опасности, угрозы конфиденциальности, а также многочисленные риски для актуальной цифровизации [6]. Поскольку *online* - преступность (киберпреступность) имеет сходную природу с *offline* – преступностью, то покончить с ней «в одночасье» практически невозможно. Противодействие несанкционированному вмешательству в экономическую деятельность организаций и частную жизнь граждан, обеспечивается высокопрофессиональной системой кибербезопасности. Международные конгрессы по информационной безопасности позволяют специалистам в сфере IT-безопасности обмениваться полезным профессиональным опытом [15]; [1]. Эти и другие международные мероприятия, безусловно, способствуют оптимизации IT-безопасности. Однако, активность граждан в киберпространстве сталкивается не только с хакерами, но также с реальными угрозами увеличения цифрового неравенства. Как показывает Кэти О'Нил, используемые сегодня математические модели и алгоритмы в информационном пространстве, усиливают дискриминацию: мотивируют трудолюбивых, опосредованно наказывают аутсайдеров и в конечном счёте формируют наше будущее [11].

Проблема конфиденциальности и безопасности (*privacy and security*) в интернете с каждым годом становится всё более актуальной, показывает Брюс Шнейер. Операторы сотовой связи отслеживает местоположение каждого собственника мобильного телефона (*tracks your location*) и тех, кто находится на связи с ним. Все учетные записи в Интернете регистрируются. По электронным письмам (*your e-mails and texts*) легко установить круг ваших близких друзей. *Google* и *Facebook* знают, что вы думаете, потому что они автоматически сохраняют все ваши

личные запросы. Интернет-корпорации используют техническое наблюдение, чтобы манипулировать новостями и рекламными объявлениями, которые мы каждый видим, ценами на товары и услуги, которые мы выбираем. До поры они просто хранят эту конфиденциальную информацию. Но не только правительства используют информационный надзор за гражданами. Эту ценную информацию используют киберпреступники в своих корыстных целях. Отчасти граждане согласны на это добровольно. Сотрудничество с надзорными государственными органами удобно, потому что гарантирует нам защиту от киберпреступников (для них всегда уязвимы наш телефон, компьютер, кредитные карты и даже автомобиль). Эксперт по вопросам кибербезопасности Брюс Шнайер, учитывая комплексность проблемы «тотальной поднадзорности», предлагает искать разумный баланс между информационной безопасностью и конфиденциальностью (*individual privacy*) [16]. Ежедневно интернет-корпорации в автоматическом режиме связывают точки входа в киберпространство и паттерны нашего персонального поведения. Насколько бескорыстны глобальные мегакорпорации и насколько плотно они контролируют деньги и конфиденциальную информацию? Какова степень коммерческих злоупотреблений в условиях информационных монополий (*Google, Twitter и Facebook*)? Эти и другие экзистенциальные вопросы задаёт Фрэнк Паскуале [14].

Информационное общество является результатом научно-технологического прогресса. Однако, технологические достижения (*new and emerging technologies*) имеют и свою оборотную сторону. Марк Гудман, эксперт в области глобальной безопасности (*leading authority on global security*) убеждён, что параллельное прозрачному цифровому миру, «цифровое подполье» (*Digital Underground, Dark Net*) помогает киберпреступникам, коммерчески заинтересованным информационным корпорациям и правительственным организациям, используя новейшие технологии, делать всех граждан более уязвимыми, чем когда бы, то ни было в истории человеческой цивилизации. Он убеждён, что даже самый сложный кибернетический гаджет, будь то имплантируемое медицинское устройство, беспилотный автомобиль или летательный аппарат, 3D принтер и т. д., могут быть взломаны преступниками с катастрофическими последствиями [5].

Deep Web и Silk Road: экзистенциальный конфликт императива конфиденциальности

Помимо знакомого всем яркого и глянцевого «дружелюбного» онлайн-мира (*Google, Facebook и Twitter*), существует тёмный («мутный») информационный материк *Dark Net*. Там находится обширная хорошо скрытая сеть сообществ, культур сайтов. Именно там люди могут быть, кем угодно и делать что угодно, утверждает Джейми Бартлетт [2]. Территория *Dark Net* - это кокаино-героиновый *Silk Road*, криптовалюты (*bitcoin* и т. д.), международный терроризм и детская порнография. Цифровое подполье (*digital underworld*) киберпространства, место для

тех, кто мечтает об анонимности в условиях всегда прозрачного для хакеров и спецслужб информационного общества. Высокий интеллект, специализированные компьютерные программы и дорогое «железо» позволяют эффективно сканировать *Dark Net*. По всей видимости, «свобода в интернет» это всего лишь ретролибертарианская иллюзия.

Dark Web (*Dark Net*, *Darknet*, *Deep Web*) это своего рода «параллельный интернет» со своими программными и финансовыми секретами. Криптоэкономика сформировалась под воздействием разнонаправленных драйверов. Одним из них был подпольный веб-сайт *Silk Road*, размещенный в *Dark Web*, где любой пользователь интернет мог торговать чем угодно. На *Silk Road* созданный Россом Ульбрихтом (*Ross William Ulbricht*, он же *Dread Pirate Roberts*) продавались наркотики, оружие, удостоверения личности и другие противозаконные вещи за криптовалюту [12]. Веб-сайт *Silk Road* представлял собой своего рода «теневого *eBay*», для продажи и покупки наркотиков», с объёмом более миллиарда долларов. Эйлин Ормсби изучила многие «закоулки» *Dark Web*. В качестве эксперимента она даже участвовала в форумах, покупала криптовалюту, общалась с наёмными убийцами, присутствовала на судебных процессах, встречалась с преступниками и правоохранителями [13]. Федеральное правительство США, начало эпическую двухлетнюю охоту за «Страшным Пиратом Робертсом» (*Dread Pirate Roberts*, Росс Ульбрихт) неуловимым владельцем сайта. Поскольку Росс Ульбрихт планировал исчезнуть, агенты ФБР работали круглосуточно, чтобы поймать его. Наконец он был арестован на территории Сан-Франциско второго октября 2013 года. Ему официально предъявили обвинения в наркоторговле, отмывании денег и многочисленных хакерских атаках. С 29 мая 2015 года Росс Ульбрихт отбывает пожизненное заключение [3].

У отдельных граждан есть множество причин (психологические комплексы, социопатия, социофобия, экзистенциальный аутизм, перманентные конфликты с законами данного государства) для того, чтобы сохранять анонимность в киберпространстве. Именно им «продают» экзотичный, интригующий брэнд *Dark Net* (*Darknet*, *Deep Web*, *Dark Web*) в качестве «сверхнадёжной банковской ячейки», «цифрового логова», куда никто никогда не проникнет. Параллельно привычному и дружелюбному онлайн-миру с интерфейсами *Google*, *Facebook* и *Twitter*, существует, якобы, подобно невидимой подводной части айсберга, скрытая сеть сайтов, онлайн-сообществ и субкультур, где свобода стремиться к своим мыслимым пределам и где юзеры могут представляться кем угодно. Это *Dark Net*. Джейми Бартлетт попытался проанализировать архитектуру и экзистенциальные риски глубинного погружения в это «цифровое подземелье» (*digital underworld*). Он продемонстрировал неординарное видение интернет [2].

Тематика, связанная с хакерскими субкультурами и цифровой экономикой раскрывается Мэтью Мэзером в художественной форме. События романа-техноутопии *Darknet* происходят в

турбулентном мире будущего, где биткойны и криптовалюта являются единственными способами оплаты за любые услуги. *Darknet* пугающе реалистичный техно-триллер (*noir/tech edge*) содержит конспирологический нарратив о том, как некая глобальная корпорация скрывает от граждан свои опасные тайны (*dark secrets*). Раскрыть темную тайну мега корпорации берутся маргиналы, хакеры Джейк О'Коннелл и Джин Хуан. [10]. Проблема защищённой анонимности пользователей в интернет беспокоит как обычных пользователей, так и государственные структуры. Здесь можно выделить технологический и юридический аспекты. Попытки сохранять анонимность в сети интернет тщетны. Такие службы как CIA (*Central Intelligence Agency*, Центральное разведывательное управление США, ЦРУ) и NSA (*National Security Agency*, Агентство национальной безопасности Соединённых Штатов, АНБ – одно из подразделений МО США, разведывательный орган, который занимается радиоэлектронной разведкой и защитой электронных коммуникационных сетей) отслеживают *cookies* любого пользователя, предотвращая кражу личных данных [7]. Некоторые пользователи, во что бы то ни стало, пытаются оставаться анонимными в киберпространстве. Но, манипуляции биткойнами, энергичный хактивизм, информационные ресурсы *Tor* и *Darknet* не являются гарантией свободы в киберпространстве [8].

Анонимность в интернете – норма или исключение? Что такое подлинная онлайн-свобода? Как обеспечить безопасность в *Deep Web*? Видимо с коммерческой целью некоторые авторы внушают наивным юзерам, что *Deep Web* один из последних «истинных бастионов свободы» в интернете. Джек Джонс обещает открыть топ-секрет, для гарантированной анонимности в интернете [9]. Это разумеется либертарианский миф. Интернет-поисковик *Google* в автоматическом режиме собирает информацию о вас с каждым запросом. *Google* знает о вас «всё»: географическое местоположение компьютера (стационарного или мобильного), день рождения, размер вашей обуви, рецепт любимой пиццы и другие ваши вкусы и предпочтения. В такой ситуации игры в сетевого «человека-невидимку» забавны. Попытки запугать обывателей комфортного для добропорядочных пользователей киберпространства хакерами, «чужими» из *Deep Web* продолжаются. Как нас убеждает Клинт Уоттс, манипуляторы массовым сознанием благодаря изощрённым схемам, используют интернет-форумы, социальные медиа (такие как *Facebook*, *Twitter*, *LinkedIn* и другие) для того, чтобы незаконно применять в своих коварных целях персонализированную конфиденциальную информацию, [18].

Заключение

Рассмотрена детально проблематика, связанная непосредственно с темой гарантированного обеспечения кибербезопасности в современной инфосфере. Экспонированы технологические и правовые параметры *Deep Web* / *Dark Net* (альтернативного

киберпространства). В контексте междисциплинарной рефлексии подвергнут анализу парадокс баланса информационной открытости современной высокотехнологичной экономики и обеспечение её защищённости от несанкционированных (хакерских) вторжений. Показано, что эффективная экономическая активность граждан во многом определяется государственными программами инвестиций, прозрачными стратегиями и рационально обоснованными целями. Значительный экономический рост во многом зависит не только от финансовых инвестиций в экономически целесообразные проекты, но также от инвестиций в наукоёмкие аналитические исследования. Осуществление цифровизации в постиндустриальных обществах детерминирует возникновение многовекторных процессов, сопровождающихся опасностями и рисками, часть из которых возникает из *Deep Web / Dark Net*. Предпринимаемые меры кибербезопасности, хотя и минимизируют материальный и моральный ущерб нанесённый хакерами, к сожалению, не могут полностью устранить негативные эффекты хактивизма и существования *Dark Net*. Безопасность хранения и передача конфиденциальной информации в сети интернет при наличии «теневого интернет» должны стать объектом междисциплинарного исследования.

Список литературы:

1. Международный конгресс по кибербезопасности *International Cybersecurity Congress* (2018). 05.07.2018. Москва, Центр международной торговли, Конгресс-центр. Режим доступа: <https://ict2go.ru/events/5617/>
2. Bartlett, Jamie (2016) *The Dark Net: Inside the Digital Underworld*. New York, Brooklyn: Melville House; 320 p.
3. Bilton, Nick (2017) *American Kingpin: Catching the Billion-Dollar Baron of the Dark Web*. N.Y.: Portfolio; 352 p.
4. Gehl, Robert W. (2018) *Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P (Information Society)*. Massachusetts, Cambridge: The MIT Press; 288 p.
5. Goodman, Marc (2016) *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*. N.Y.: Anchor; 608 p.
6. Harper, Allen & Regalado, Daniel & Linn, Ryan (2018) *Gray Hat Hacking: The Ethical Hacker's Handbook*. N.Y.: McGraw-Hill Education; 640 p.
7. Henderson, Lance (2013) *Darknet: A Beginner's Guide to Staying Anonymous (Penetration testing, Kali Linux)*. South Carolina, North Charleston: CreateSpace Independent Publishing Platform; 88 p.
8. Henderson, Lance (2017) *Tor and the Deep Web: Bitcoin, DarkNet & Cryptocurrency*. WA, Seattle: Amazon Digital Services LLC; 174 p.

9. Jones, Jack (2017) *Tor: Accessing The Deep Web & Dark Web With Tor: How To Set Up Tor, Stay Anonymous Online, Avoid NSA Spying & Access The Deep Web & Dark Web (Tor, Tor ... Invisible, NSA Spying, Python Programming)*. South Carolina, North Charleston: CreateSpace Independent Publishing Platform; 136 p.
10. Mather, Matthew (2015) *Darknet*. QC, Montreal: Matthew Mather ULC; 346 p.
11. O'Neil, Cathy (2017) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. N.Y.: Broadway Books; 288 p.
12. Ormsby, Eileen (2014) *Silk Road*. NSW, Sydney: Macmillan Australia; 352 p.
13. Ormsby, Eileen (2018) *Darkest Web: Drugs, death and destroyed lives ... the inside story of the internet's evil twin*. New South Wales, Crows Nest: Allen & Unwin; 320 p.
14. Pasquale, Frank (2016) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Massachusetts, Cambridge: Harvard University Press; 320 p.
15. RSA Conference 2018 Opens Today In San Francisco (April 16, 2018) RSA Conference, the world's leading information security conferences and expositions. Режим доступа: <https://www.rsaconference.com/.../rsa-conference-2018-open>
16. Schneier, Bruce (2016) *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. N.Y.: W. W. Norton & Company; 448 p.
17. Thomas, Kenn (Ed.) (1999) *Cyberculture Counterconspiracy: A Steamshovel Web Reader*. CA, San Diego: Book Tree; 180 p.
18. Watts, Clint (2018) *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News*. New York: Harper; 304 p.
19. Webber, Zach (2018) *Cybersecurity: The Ultimate Beginners Guide To Learn And Understand Cybersecurity Measures Effectively*. South Carolina, North Charleston: Amazon Digital Services LLC; 42 p.