

DARKNET – СОВЕРШЕННО НОВОЕ ПРОСТРАНСТВО ДЛЯ РАЗВИТИЯ ПРЕСТУПНОСТИ, СКРЫТОЕ ОТ ГЛАЗ КОНТРОЛЬНО-НАДЗОРНЫХ ОРГАНОВ

Шеллер Игорь Анатольевич

студент 1 курса

Научный руководитель: **Выжитович А.М.**

к.э.н., доцент кафедры налогообложения, учета и экономической безопасности,
Сибирский институт управления — филиал Российской академии народного хозяйства и
государственной службы при Президенте Российской Федерации, г. Новосибирск

Аннотация. В данной статье рассматривается анонимная сеть – Darknet. Приводятся основные цели использования данной сети и её влияние на экономическую и социальные сферы. А также, изучаются её характерные особенности, которые служат полем для совершения преступлений. Рассматриваются пути решения данной проблемы.

Ключевые слова: даркнет, темная сторона интернета, преступления, теневая экономика, контроль.

Интернет - всемирная сеть для хранения и обмена информацией. Абсолютно каждый человек в наши дни может получить доступ к этой сети. Внедрение такого рода технологий как интернет в различные области человеческой жизнедеятельности сделало её гораздо более комфортной, но также открыла и новые пути для развития преступности, поскольку есть еще одна, черная сторона глобальной сети, под названием «Darknet».

Darknet - это термин, относящийся к определенной группе конкретных веб-сайтов, которые существуют в зашифрованном сетевом пространстве.[4] Они не могут быть обнаружены традиционными поисковыми системами, используя обычные браузеры. Фактически, темная сеть – это сеть поверх другого привычного нам Интернета, которая использует специальные домены. Почти все сайты Darknet скрывают личные данные с использованием инструментов шифрования Tor.[2] Данная сеть пользуется популярностью благодаря своей способности полностью скрывать идентификацию пользователя и его сетевую активность. Соответственно, для того чтобы получить доступ к сайтам, которые запрещены, человеку необходимо всего лишь подключиться к сети Tor, что способен сделать почти каждый обыватель Интернета.

Факт того, что пользователь не может быть отслежен и способствовал развитию преступности в данной сети. Количество пользователей этой сети увеличивается примерно на 100 миллионов пользователей в год. [3] Это означает, что мы можем говорить о развитии преступности, которая скрыта от правительственных структур и соответственно не подлежит

какому-либо контролю и надзору со стороны государства. Контрольно-надзорные органы на данный момент бессильны перед темной стороной интернета.

Преступления, совершённые в темной сети, редко разоблачаются, в силу своей анонимности. Но помимо этого у правоохранительных органов имеется ещё ряд проблем. Это связано с тем, что преступные деяния, которые субъекты преступной деятельности осуществляют с помощью сети Darknet требуют соответствующей юридической оценки. В силу этих обстоятельств возникают вопросы по какой статье и части Уголовного Кодекса РФ квалифицировать то или иное преступление. Контроль за преступными деяниями лиц в Darknet является актуальным направлением правоприменительной и правозащитной деятельности государства. Так же у правоохранительных органов возникают проблемы, связанные с оперативно-розыскной деятельностью и процессом доказывания по преступлениям, которые были совершены в сети Darknet. Отсутствие решения указанных проблем, а также методик противодействия преступным деяниям в Darknet представляет собой большую опасность правовой безопасности личности, общества и государства.

Так же, немалый удар темная сторона интернета наносит и по экономике страны. Предоставление неправомερных услуг и незаконная торговля основной сегмент Darknet. Объем доходов на таких анонимных интернет рынках очень высок и может достигать порядка 30 миллионов рублей в день. Динамика торговли оценивается до 600% годового роста (данные на 2 февраля 2017 года). На сегодняшний день суммы увеличились и продолжают расти, рынок остается стабильным. Darknet напрямую способствует развитию теневого сектора экономики в стране и ухудшению ее положения на мировой арене.

При выявлении банками среди своих клиентов лиц, занятых в этой сфере, необходимо пересматривать уровень рисков вовлеченности в сомнительные операции [1].

Так выглядит ряд некоторых типовых преступных деяний, осуществляемых людьми в сети Даркнет ежедневно и мера наказания за них:

- 1) За торговлю наркотическими веществами с помощью сети Даркнет. Преступники наказываются по статье 228 УК РФ на срок до 15-и лет в зависимости от тяжести;
- 2) За незаконное приобретение или передачу оружия с помощью Даркнет. Преступники наказываются по статье 222 УК РФ на срок до 8-и лет;
- 3) За продажу поддельных документов в сети Даркнет. Преступники наказываются по статье 327 УК РФ на срок до 4-х лет;
- 4) За педофилию, к которой может подтолкнуть человека информация на имеющихся в Даркнет тематических форумах. Преступники наказываются по статье 134 УК РФ на срок вплоть до пожизненного заключения;
- 5) За хакерство. Преступники наказываются по статье 272 УК РФ на срок до 7-и лет

- 6) За мошенничество, сообщников для которого набирают посредством специализированных форумов в Даркнет. Преступников наказывают по статье 159 УК РФ на срок до 10-и лет.

Также в Тог можно найти объявления о услугах, связанных с убийствами. Например, о слежке, поджогах, грабежах, избиениях или же о заказном убийстве.

Преступность в Darknet продолжает развиваться. В связи с этим необходимо подойти к этой проблеме более детально и тщательно. Жесткий контроль данной сети может способствовать пресечению огромного количества преступлений. Для того чтобы реально повлиять на динамику и структуру преступности в полностью анонимной сети, необходимы абсолютно новые подходы, новый персонал и понимание масштабов этой проблемы. Одним из путей решения данной проблемы может стать создание государством органов, специализация которых будет заключаться именно в борьбе с данным вида преступлениями и где сотрудники будут обладать всеми необходимыми компетенциями для решения данных задач. Так же необходимо объединение стран, в которых Darknet процветает для совместной борьбы, поскольку это может стать отправной точкой к созданию абсолютно нового, открытого и полностью законного интернет-пространства.

Список литературы:

1. Кругликов В.П., Выжитович А.М. Развитие системы управления рисками при принятии клиентов на обслуживание как инструмент обеспечения экономической безопасности банка // Развитие территорий. СИУ - филиал РАНХиГС. - 2018. №1. С.28-34.
2. Новиков И.С. 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: 28.03.2019)
3. Узденов Р. М. Новые границы киберпреступности // Всероссийский криминологический журнал. 2016. [Электронный ресурс]. – URL: <https://cyberleninka.ru/article/n/novye-granitsy-kiberprestupnosti> (дата обращения: 28.03.2019)
4. Munksgaard R., Demant J. Mixing politics and crime — The prevalence and decline of political discourse on the cryptomarket // International Journal of Drug Policy. 2016. No. 35. Pp. 77–83