(cc) BY

Моторова Анна Владимировна
старший преподаватель
Мефодьева Кристина Витальевна
студентка
Плясунова Екатерина Сергеевна
студентка
ФГБОУ ВО «Чувашский государственный
университет им. И.Н. Ульянова»
г. Чебоксары, Чувашская Республика

ОСОБЕННОСТИ РАСКРЫТИЯ КИБЕРПРЕСТУПЛЕНИЙ: ПРОБЛЕМНЫЕ АСПЕКТЫ

Аннотация*: статья посвящена анализу становления современной методики раскрытия киберпреступлений с использованием зарубежного опыта. Рассмотрены основные направления использования ресурсов сети Интернет в ходе раскрытия и расследования интернет-преступлений. На основании анализа предложены пути решения возникающих проблем.*

Ключевые слова*: киберпреступления, даркнет, интернет-преступления, следователь.*

Сегодня преступления в сети Интернет приобрели неслыханную популярность. Преступники для сохранения своей анонимности перешли не просто на просторы информационной сети, а спустились в ее темные уголки. Темный интернет, по-другому darknet, стал популярной платформой для мошенников, террористов, торговцев нелегальной продукцией и распространителей детской порнографии. Большинство обывателей этих мест – умелые IT-специалисты или, как их называют в простонародье, хакеры. Особенностью даркнета является то, что любое соединение гораздо труднее отследить, что обеспечивается за счет сложной маршрутизации соединения и многократного шифрования информации.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Проведенный, в работе Осипенко, контент-анализ одного из популярных русскоязычных сайтов «теневого интернета» Russian Silk Road, который позаимствовал часть имении у наиболее известного рынка Darknet, показал, что на момент исследования на сайте было размещено 433 объявления, из них 208 посвящено психоактивным веществам, половину из которых составляют предложения каннабиодов (97), остальные – стимуляторов (71), эйфоретиков (18), психоделиков (19). Кроме того, есть раздел «Цифровые товары» (116 объявлений), где продают доступ к взломанным сайтам, базы данных госорганов, раздел «Документы, деньги» (44 объявления), где можно заказать удостоверения, автодокументы и сканированные изображения чужих документов, а также раздел «Карты, SIM, аккаунты» (42 объявления) с предложениями данных кредитных карт и платежных данных [4, с. 5]. На форуме данного сайта в разделах можно найти московские «магазины» наркотиков и оружия в открытом доступе. Таким образом, даркнет является плодотворной почвой для развития преступности, которая, на сегодняшний день, остается практически безнаказанной из-за критической невозможности отследить таких «торговцев».

Согласно информации, приведенной Министерством Внутренних Дел, за первый месяц 2022 года в России зарегистрировано 37,2 тыс. преступлений в области информационно-телекоммуникационных технологий. При этом злоумышленники на 39% чаще использовали мобильные сети для осуществления своих целей, а сеть интернет – на 51,3% чаще. Кроме того, как отмечает МВД, наибольшая доля прироста показателей подобных преступлений зафиксирована в Северной Осетии (87%), а также в Севастополе – 77% и Тульской области – 71%. Ранее в СК заявили о росте уровня киберпреступности в 20 раз за последних семь лет [3, с. 5].

Необходимо отметить, что сложная система отслеживания киберпреступников, а также использование этими лицами VPN-серверов делают практически невозможным установление места совершения преступлений, что ставит под вопрос территориальную подсудность содеянного не только между субъектами

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

Российской Федерации, но и всего мира в целом. Без специальных познаний в данной области раскрытие таких преступлений практически невозможно.

Высокая анонимность, децентрализация хранимой информации, шифрование исходных данных значительно усложняют работу правоохранительных органов. Появление большого количества новых терминов и понятий заводят в угол даже самых опытных следователей и замедляют ход расследования дела. Без специалистов в этой области не представляется возможным определение нужной экспертизы и постановка вопросов эксперту [5, с. 5].

От 500 тысяч до миллиона человек – такая нехватка кадров наблюдается сегодня в российской IT-индустрии [2, с. 5]. Во многих субъектах Российской Федерации ощущается острый дефицит государственных экспертов в области информационных технологий, что подталкивает правоохранительные органы обращаться в негосударственные экспертные учреждения. Несмотря на такую нехватку, хакеры не очень охотно идут на сотрудничество с правоохранительными структурами. С другой стороны, возникают проблемы с доверием к добросовестности выполненных консультаций и экспертных заключений.

Помимо нехватки специалистов, в России отсутствует единая методика раскрытия киберпреступлений и поиска криминалистически значимой информации, способы ее получения и фиксации. Также статус информации, полученной из теневого интернета законодательно нигде не закреплен.

Исследовательский институт RAND Europe выделил основные методы борьбы с даркнет-преступностью [1, с. 5]: во-первых, это сопоставление реальных действий с онлайн-активностью. Однако, не все преступники настолько легкомысленно относятся к своей конфиденциальности, и на вычисление таких личностей уходит много времени и ресурсов, которые не всегда оправдываются. Во-вторых, это получение информации с открытых сайтов. Несмотря на то, что большая часть активных действий преступников разворачивается на просторах теневого интернета, рекламировать свои услуги им приходится на открытых веб-сайтах. В-третьих, это перехват почтовых отправлений. Однако многие преступники ухитряются перевозить наркотические вещества под видом лекарственных

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

препаратов и маскировать их в плотных вакуумных упаковках для предотвращения распространения запаха. Отследить обратный адрес отправителя тоже не всегда получается, поэтому удается вычислить только «потребителя», а не продавца нелегальной услуги. В-четвертых, это использование искусственного интеллекта для отслеживания IP-адресов и размещенной информации. Такие технологии еще не получили широкого распространения и на данный момент проходят только стадию апробации, поэтому говорить об их эффективности пока не приходится. В-пятых, отслеживание платежных транзакций. Несмотря на оплату услуг криптовалютой и биткоином, можно отследить перевод электронных платежных средств в наличную форму. Но и этот способ не зарекомендовал себя своей эффективностью. С учетом стоимости криптовалюты сегодня, многие хакеры предпочитают оставлять свои средства в электронном формате, либо же придумывают более легальные способы их вывода. К примеру, покупка и продажа NFT-изображений.

На основании всего вышесказанного, в первую очередь, необходимо расширить штат государственных экспертов в области информационных технологий, а также тщательно проработать методику проведения программно-технической и других компьютерных экспертиз, для упорядочения проводимых в этих областях исследований. Также, мы видим острую необходимость повышения квалификации правоохранительных органов в области информационных технологий, чтобы они элементарно понимали базовые термины и процессы, которые происходят в IT-сфере. Как вариант, для преодоления дефицита специалистов в данной области, возможно сотрудничество с преступниками, которые ранее были задержаны за аналогичные киберпреступления. Если такие лица при отбывании наказания зарекомендовали себя с положительной стороны и охотно идут на контакт с правоохранительными органами, вполне возможно использовать их в качестве консультантов для формирования линии расследования в особо трудных случаях. Такая практика получила широкое распространение в США и доказала свою результативность.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

Список литературы

1. Мазур А.А. Актуальные проблемы предупреждения преступности в социальной сети даркнет / А.А. Мазур [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/aktualnye-problemy-preduprezhdeniya-prestupnosti-v-sotsialnoi-seti-darknet/viewer (дата обращения: 25.01.2023).

2. Алексей Глинкин Кадровый голод в России // Lenta.ru [Электронный ресурс]. – Режим доступа: https://lenta.ru/articles/2021/07/27/golod/ (дата обращения: 25.01.2023).

3. Краткая характеристика состояния преступности в Российской Федерации за январь 2022 года [Электронный ресурс]. – Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/28021552/ (дата обращения: 25.01.2023).

4. Осипенко А.Л. Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения / А.Л. Осипенко // Вестник Воронежского института МВД России. – 2015. – №2. – С. 13–19.

5. Мухин С.М. Преступления в сети Darknet: краткая характеристика, проблемы противодействия / С.М. Мухин // Альманах молодого исследователя. – 2018. – №5. – С. 110–114.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)