Павлова Марина Владимировна
канд. пед. наук, доцент
Чебоксарский институт (филиал) ФГБОУ ВО «Московский политехнический институт»
г. Чебоксары, Чувашская Республика

ПРОБЛЕМА РАСПРОСТРАНЕНИЯ ЗАПРЕЩЕННОГО КОНТЕНТА ЧЕРЕЗ СЕТЬ DARKNET

Аннотация: *в данной работе рассматривается механизм распространения запрещенного контента через сеть DarkNet и методы борьбы с ним. Автор отмечает, что данная проблема возникла с вхождением интернета в человеческую жизнь и сегодняшние методы, используемые для борьбы с распространением запрещенного контента, не справляются со своей задачей, а его количество продолжает расти, особенно на ресурсах сети Darknet.*

Ключевые слова*: киберпреступность, запрещенные ресурсы, DarkNet, интернет.*

Сегодня трудно представить себе жизнь без компьютера. Интернет стал неотъемлемой частью жизни современного человека. К сожалению, данная платформа стала не только источником ценной информации, но и площадкой для распространения запрещенного контента, которая имеет название DarkNet (далее DarkWeb, темный интернет). К термину «запрещенный контент» на территории РФ принято относить информацию, содержащий детскую порнографию, пропаганду наркотических веществ, информацию о способах совершения самоубийства и прочее [1]. Значит, действия, которые встречаются в DarkNete содержат самые разнообразные составы преступлений, предусмотренные УК РФ.

DarkNet привлекает злоумышленников анонимностью, следовательно, безнаказанностью в Интернете. Чтобы обеспечить полную анонимность в темном интернете, правонарушители используют сеть Tor (TheOnionRouter) – которая строится на принципе многослойной или луковой маршрутизации, при которой пользователя нельзя идентифицировать. Его трафик отправляется через

несколько сетевых узлов, где каждый маршрутизатор удаляет слой шифрования, чтобы открыть инструкцию, куда слать трафик дальше. После этого данные пересылаются следующему маршрутизатору [3, с. 116]. В итоге промежуточные узлы не знают ни источника, ни назначение трафика, что является главной причиной, препятствующей работе правоохранительных органов.

Также отметим, что на сайты darkweb возможно зайти только через специальные браузеры как Tor. Адреса порталов имеют домены .onion. Кроме этого, злоумышленники используют зашифрованную структуру имен, создающую ссылки, которые часто невозможно запомнить.

Сегодня перед государством стоит важная задача – изучить данную проблему и понять причины, предложить меры для устранения (минимизации) этого пагубного явления. Рассмотрим некоторые важные методы борьбы с распространением запрещенного контента в интернете:

1. Для ограничения доступа к запрещенным сайтам на государственном уровне в России был создан «Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено [4]. Необходимо отметить, если домен сайта находится в данном списке, то Интернет-провайдеры обязаны заблокировать к нему доступ. Но блокировка работает в пределах РФ, поэтому пользователи могут воспользоваться помощью VPN для получения доступа к информации.

2. Выявление временной уязвимости. Несмотря на то, что одна из целей Tor – предоставлять приватность и анонимность пользователям, время от времени встречаются уязвимости – так в 2017 случилась утечка реальных IP-адресов пользователей, в следствии чего, был арестован Александр Винник (Владелец криптобиржи BTC – главная платформа транзакций между покупателями наркотиков и darkweb площадками).

3. Получение необходимой информации с открытых сайтов. Злоумышленники могут искать своих клиентов в общедоступных сетях. В связи с этим они могут оставить свои данные на открытых веб-сайтах.

Существуют различные схемы противоправных деяний в сети Интернет. Для одних, возможно, это способ развлечься, для других – обогатиться. Однако важно помнить, что за совершение таких правонарушений может последовать уголовная ответственность. Особенности квалификации преступлений, совершенных в сети Интернет в том, что эти правонарушения сложно разграничить как между собой, так и с другими видами преступлений, предметом которых является информация, находящаяся на компьютерном носителе, системе ПК или компьютерных сетях.

Таким образом, можно сделать вывод, что рынки DarkNeta, существующие во всемирной паутине, помогают контрабандистам продавать оружие, наркотики и в тоже время оставаться вне поля зрения правоохранительных органов. Нельзя не отметить и то, что общественная опасность данного явления возрастает с каждым годом, современные методы борьбы с распространением запрещенного контента в DarkNet еще недостаточно эффективны. Это доказывает статистика с официального сайта Tor, на которой заметно увеличение количества пользователей и контента в сети DarkNet [5]. Именно поэтому, для борьбы с угрозой киберпреступности, которая, безусловно, будет расти, необходимо постоянное международное сотрудничество, постоянные профилактические работы с населением, создание профессиональных узконаправленных киберотрядов.

Список литературы

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2016 г. №149-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798 (дата обращения: 22.10.2020).

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

3. Стручков Ю. Установка и настройка Tor / Ю. Стручков // Сетевая литература. – 2011. – С. 115–120.

4. Tor Metrics: Официальный сайт [Электронный ресурс]. – Режим доступа: https://metrics.torproject.org/userstats-relay-table.html

5. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: официальный сайт [Электронный ресурс]. – Режим доступа: https://rkn.gov.ru/mass-communications/p753/p826/ (дата обращения: 22.10.2020).