Секция «Уголовное право и криминология, уголовно-исполнительное право»

Влияние теневого веба на формирование личности преступника

Научный руководитель – Грибанов Евгений Викторович

Ильницкий Александр Сергеевич
Студент (специалист)
Краснодарский университет Министерства внутренних дел Российской Федерации,
Краснодарский край, Россия
E-mail: kursant.ilnickii@gmail.com

Изучение личности преступника не только представляется важным для развития криминологии, но и способствует улучшению системы предупреждения преступлений, так как значительная часть профилактических мер воздействуют непосредственно на личность. Эффективность такого воздействия будет намного выше тогда, когда имеются научно-обоснованные знания о личности преступника, а также способы и методики противодействия конкретным преступлениям. В такой связи возникают сомнения по поводу эффективности сегодняшней профилактики в силу динамичных изменений самой преступности.

Информационные технологии и массовая цифровизация затронули все сферы общественной жизни, в том числе и криминальную среду. Это требует новых подходов к предупреждению преступлений, формирования методов воздействия на личность преступника с учетом происходящих изменений.

Анализ научной литературы на данную тематику показал, что влияние «криминального интернета» на формирование личности преступника и вовсе не освящено.

Говоря о «криминальном интернете», следует понимать, что значительную её часть занимает скрытое Интернет-пространство. В данном случае речь идет не просто о привычном уровне сети (социальные сети, интернет-магазины, форумы и т.д.), а о её обратной стороне. Так называемый «Теневой веб» (теневой интернет; Dark Web; Dark Net), который представляет собой некое цифровое подполье, где царит полная анонимность, а содержимое сайтов открыто только «для своих»[2].

По мнению В.С. Овчинского «Темный веб» представляет собой одноранговую сеть, название которой обязано широкому использованию своих ресурсов различного рода преступными, незаконными группами и группировками[1].

Доступ к «Теневому вебу» открывает специальное программное обеспечение, наиболее популярным из которых является «Tor browser».

Браузер создаёт наиболее благоприятные условия для развития преступности в силу своих особенностей: а) шифрование данных и подключение к сети по схеме многократного присоединения к различным сетевым серверам; б) удаление cookies-файлов; в) использование криптовалюты при расчёте за приобретение товаров или оказание услуг, запрещенных законодательством; г) доступ к запрещенному законодательством, информационному контенту.

Анализ судебной практики показал, что уже сегодня «Tor browser» является весьма распространенным средством для совершения преступлений, в частности в сфере наркоторговли, оборота оружия, распространения детской порнографии и других видов преступной деятельности[5].

В связи, с чем актуальным видится изучение процессов влияния «Теневого Веба» на личность преступника, знание о которых восполнит пробел в криминологической теории преступности в эпоху «цифрового мира».

На **первом этапе**, формирование преступных свойств личности и вовсе не происходит, так как пользователь открывает доступ к теневому пространству сети Интернет с целью

«безобидной» анонимизации. Потребность в анонимности лица в сети на сегодняшний день становится все более популярным явлением и может быть обусловлена различными факторами[6].

Одним из основных факторов, популяризации анонимности в сети является цифровой авторитаризм, т.е. деятельность власти, направленная на манипулирование информацией, обеспечение себе популярности при использовании формально демократических институтов[4]. В данном случае лицо пытается уйти от государственного манипулирования информацией, забывая о подобных возможностях преступных структур.

Большую роль в популяризации анонимности играет законодательная политика в сфере регулирования интернет-пространства, а именно ограничение прав в сети Интернет. Следует обращать внимание на то, что, что во многом реальные ограничения и вовсе отсутствуют, а тема просто становится «хайпом», толкая людей на использование различного рода анонимайзеров.

Взяв во внимание зарубежный опыт, можно выделить такой фактор как распространение идеологии анонимности. Не смотря на то, что субкультура «шифропанков» массово не прижилась на территории России, на западе она является весьма популярной. Основные их цели $\frac{3}{4}$ противодействие правительству в части использования сети Интернет в целях ограничения свободы и конфиденциальности, а также подрыв основ государства с помощью инструментов диверсии, которые предлагает цифровой мир[2].

Второй этап влияния теневого веба характеризуется процессом непосредственного внедрения в среду «Dark Net» и формирования у лица преступной мотивации, которая, как правило, носит профессиональный или игровой характер.

Большие масштабы воздействующей криминальной информации и её плюрализм, способствуют возникновению интереса к преступной деятельности.

Особое влияние на формирование преступной мотивации оказывают такие факторы как: а) активное обсуждение в СМИ невозможности правоохранительных органов противостоять средствам анонимизации (Tor; 2iP и т.д.)[7]; б) преступная идеология; в) деструктивная реклама (легкий заработок, покупка наркотических средств, оружия и т.д.); г) наличие методических рекомендаций по тактическим основам совершения преступления и сокрытия следов.

На **третьем этапе**, информационное влияние на формирование личности преступника оканчивается, так как приобретаются все свойства личности потенциального преступника. К тому - же, формируется «эффект растормаживания в сети», т.е. лицо считает себя «скрытым» за монитором, чувствует избавление от необходимости следования социальным и правовым нормам, избавляясь от страха ответственности за совершение преступления.

Рассмотренное явление вбирает себя концептуальное положение, высказанное еще Ф.Ницше - «Кто сражается с чудовищами, тому следует остерегаться, чтобы самому при этом не стать чудовищем. И если ты долго смотришь в бездну, то бездна тоже смотрит в тебя»[3].

Масштабность и динамичность проблемы требует совершенствования механизмов противодействия влиянию криминального интернета, выработки научно-обоснованных методик и технологий.

Источники и литература

1) Овчинский В. С. Криминология цифрового мира: учебник для магистратуры / В. С. Овчинский. — М.: Норма: ИНФРАМ, 2018. — 352 с.

2) Джейми Б. Подпольный интернет: темная сторона мировой паутины/ Джейми Барлетт; [пер. с англ. М. Райтмана].— М.: Эксмо, 2017. — 352 с.

3) Ф. Ницше По ту сторону добра и зла [Текст] / Ф. Ницше [U+F02D] Санкт-Петербург: Азбука-классика, 2006. 99 С.

4) Guriev S., Treisman D. How modern dictators survive: an informational theory of the new authoritarianism // Cambridge: National bureau of economic research, 2015. – N 21136. – 46 p.

5) Судебные и нормативные акты РФ [Электронный ресурс] / URL: https://sudact.ru/ (дата обращения 12.02.2020 г.)

6) Россия стала мировым рекордсменом по числу пользователей «Tor» [Электронный ресурс] / URL: https://cnews.ru/news/top/2019-07-17_rossiya_ustanovila_mirovoj_rekord_po_chislu_polzovatelej (дата обращения 12.02.2020 г.)

7) В МВД признались, что оказались не готовы к наплыву IT-преступлений [Электронный ресурс] / URL: https://news.rambler.ru/other/43552138/ (дата обращения 04.02.2020 г.)