УДК 343.9.01

Ж. А. БОРИСОВА

ПРИЗНАКИ И СВОЙСТВА ПРЕСТУПНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

В статье рассматривается преступность в социальных сетях как комплексное явление, анализируются подходы отечественных и зарубежных исследователей к ее идентификации как составной части компьютерной и интернет-преступности. Предлагается определение понятия «преступность в социальных сетях в Республике Беларусь» на базе общепризнанного в криминологии понимания преступности. Выявляются общие признаки и закономерности развития преступности в социальных сетях, а также ее отличительные свойства, характерные для всех видов преступлений, которые она охватывает. Особое внимание уделяется специфическому комплексу способов и средств совершения указанных преступлений, основанному на использовании функциональных возможностей социальных сетей, парсинге персональных страниц пользователей, массовом вовлечении потенциальных жертв в сообщества преступной направленности, использовании методов социальной инженерии, организации активной поддерживающей преступность деятельности и быстром информационном обмене.

ZH. A. BORISOV

CHARACTERISTIC FEATURES AND PROPERTIES OF CRIME RATE IN SOCIAL NETWORKS

The article considers crime in social networks as a complex phenomenon, analyzes approaches of domestic and foreign researchers to its identification as a composite part of computer and Internet-crime. The definition of "criminality in social networks in the Republic of Belarus" is proposed on the basis of the generally recognized in criminology understanding of crime. Common signs and patterns of the development of crime in social networks, as well as its distinctive properties, characteristic of all types of crimes that it covers are identified. Particular attention is paid to a specific set of ways and facilities of committing these crimes, based on the use of the functional capabilities of social networks, parsing personal pages of users, mass involvement of potential victims in criminal groups, using social engineering techniques, organizing crime-supporting activities and rapid information exchange.

БОРИСОВА
Жанна Андреевна,
старший следователь
Партизанского районного
(г. Минска) отдела
Следственного комитета

Введение

За последнее десятилетие социальные сети стали глобальным и всеобъемлющим средством коммуникации. К ним относятся структурно децентрализованные, интерактивные многопользовательские веб-сайты (платформы или онлайн-сервисы), базовыми элементами которых являются персональные страницы пользователей и их сообщества, а также различные средства коммуникации и функциональные возможности, предназначенные для установления, поддержания и развития социальных связей, обмена текстовыми сообщениями и аудиовизуальной информацией.

Общедоступность и широкий охват аудитории, размещение на страницах пользователей их личных данных, разветвленная структура сообществ, всевозможные средства и функциональные возможности для поддержания коммуникации и распространения информации – все эти черты являются неотъемлемыми для социальных сетей. Оценивая их положительно, следует отметить, что они создают условия для парсинга (от англ. *parsing* – разбор, анализ) личных страниц пользователей и сообществ, использования различных приемов социальной инженерии и инструментов социального медиамаркетинга, информационной пропаганды и вовлечения в преступную субкультуру. К криминогенным свойствам социальных сетей относится также несовершенство механизма идентификации пользователей, размещение веб-сайтов и платформ социальных сетей за пределами национального сегмента сети Интернет, отсутствие должного контроля со стороны администрации социальных сетей за соблюдением пользователями установленных внутренних правил и т. д.

Так, социальные сети в современных условиях представляют собой особую сферу распространения преступности, предоставляя новые возможности для развития не только общеизвестных ее видов, но и для возникновения новых. Все это требует выделения и изучения преступности в социальных сетях как отдельного самостоятельного вида преступности. При этом выявление ее специфических признаков, свойств и детерминантов в конечном итоге позволит разработать эффективные меры борьбы с этим негативным явлением и усовершенствовать действующее законодательство, исходя из современных реалий научно-технического прогресса.

В статье мы рассмотрим преступность в социальных сетях как комплексное явление, а также определим ее отличительные признаки и свойства, характерные для всех видов преступлений, которые она охватывает.

Основная часть

За многовековую историю изучения преступности были сформированы разнообразные зарубежные и отечественные криминологические теории и школы, разработана методология науки и четкий категориально-понятийный аппарат, а также определены отдельные концептуальные положения, признанные научным сообществом. Все перечисленные достижения криминологической науки положены в основу настоящей статьи.

Так, под преступностью в криминологии принято понимать «социальное, исторически изменчивое, массовое, уголовно-правовое, системное явление общества, проявляющееся в совокупности общественно опасных уголовно наказуемых деяний и лиц, их совершивших, на определенной территории за определенный период времени» [1, с. 32].

Исходя из данного определения, под преступностью в социальных сетях в Республике Беларусь мы понимаем исторически изменчивое, массовое, общественно опасное, социальное и уголовно-правовое явление, характеризующееся совокупностью преступлений (запрещенных Уголовным кодексом Республики Беларусь деяний) и лиц, их совершивших, в сфере социальных сетей с территории Республики Беларусь либо с территории других государств, но направленных против интересов Республики Беларусь и ее граждан (включая иностранных граждан и лиц без гражданства, проживающих на территории Республики Беларусь), за определенный промежуток времени. Данное определение содержит основные признаки и свойства преступности в социальных сетях, на рассмотрении которых мы предлагаем остановиться далее.

Зачастую криминологи отождествляют такое понятие, как «свойства преступности», либо с ее признаками, либо с ее закономерностями. Для объяснения нашей позиции по данному вопросу рассмотрим указанные термины как философские категории. Так, «под признаком какого-либо предмета (явления и т. п.) подразумевается его характерная черта…» [2, с. 1007–1108], «свойство – это философская категория, выражающая отношение данной вещи к другим вещам, с которыми она вступает во взаимодействие; свойство нередко рассматривается как внешнее выражение качества» [3, с. 1182], а «закономерность – это объективно существующая повторяющаяся существенная связь явлений общественной жизни или этапов исторического процесса» [3, с. 446]. Очевидно, что данные категории существенно отличаются по своему содержанию и не могут отождествляться.

В связи с этим для описания характерных и неотъемлемых черт преступности будем использовать именно термин «признак», поскольку данная позиция является общепризнанной в отечественной криминологии. Так, в приведенном выше определении преступности находят отражение такие ее основные признаки, как социальная обусловленность, историческая изменчивость, массовость, общественная опасность, уголовно-правовой, социальный и системный характер. Перечисленные признаки являются устойчивыми и неизменными с течением времени, в отличие от свойств, которые, как было отмечено выше, будучи внешним выражением качеств описываемого объекта, проявляют себя во взаимодействии с внешними обстоятельствами (историческими, общественно-политическими, экономическими и иными социальными явлениями).

Авторский коллектив учебника криминологии под общей редакцией профессора В. Д. Дмитриева описывает такие особенности преступности, как объективный, непреходящий характер; ее зависимость от состояния общественного развития, степени стабильности общества, существующих в нем противоречий; усложнение в связи с развитием научно-технического прогресса, экономики, средств связи, компьютеризации; рост преступности в обществе, ослабленном реформированием социально-экономических и политических отношений; ее качественные и количественные изменения в связи с потребностями общества в защите вновь возникших общественных отношений от преступных посягательств; ее самовоспроизводство и т. п. [1, с. 34]. При этом все перечисленные характеристики обозначаются общим термином «закономерности», что, на наш взгляд, не вполне верно.

Отметим, что ключевой отличительный признак любой закономерности состоит в ее повторяющемся характере, который проявляется в связи с определенными явлениями общественной жизни. Так, из вышеперечисленных характеристик преступности к закономерностям, безусловно, относится ее рост в обществе, ослабленном реформированием, а также качественные и количественные изменения, связанные с возникновением новых общественных отношений. В приведенных примерах закономерности роста и изменения показателей преступности приводятся в действие такими явлениями общественной жизни, как реформирование и изменение общественных отношений. При стабилизации общественной жизни прекращается и действие данных закономерностей (например, снижается рост преступности). Таким образом, закономерности носят повторяющийся, циклический характер, проявляя себя лишь при определенных обстоятельствах, способствующих запуску их механизма.

Из изложенного можно сделать вывод о том, что такие особенности преступности, как ее самовоспроизводство, объективный, непреходящий характер, усложнение в процессе исторического развития и другие, являются не повторяющимися, а постоянными характеристиками преступности, ввиду чего их вряд ли можно назвать закономерностями. На наш взгляд, именно они требуют для своего обозначения категории «свойства».

Предложенный нами подход к разграничению таких понятий, как признаки, свойства и закономерности преступности, не является бесспорным, однако именно на него мы предлагаем ориентироваться в данной статье.

Так, преступность в социальных сетях – составная и неотъемлемая часть общего массива преступности. Ввиду этого ей в равной степени присущи все перечисленные выше основные признаки, свойства и закономерности. Полагаем, что в рамках настоящей статьи нет необходимости останавливаться на их содержании, поскольку обозначенные вопросы хорошо проработаны в теории криминологической науки. Нас же интересуют специфические, отличительные признаки и свойства преступности в социальных сетях, выделяющие ее в самостоятельный негативный феномен общественной жизни.

Факт возникновения преступности в социальных сетях – наглядное проявление такого общего признака преступности, как историческая изменчивость, и ее свойства усложняться в процессе компьютеризации общества и развития интернет-технологий. Безусловно, массовым явлением она стала лишь после того, как социальные сети приобрели статус современного и всеобъемлющего средства коммуникации.

На пути изучения преступности в социальных сетях, ее идентификации, а также совершенствования законодательства в данном направлении особое значение имеет разработка четкого категориально-понятийного аппарата. Ввиду тесной связи обозначенных вопросов с развитием компьютерных технологий и сети Интернет данный процесс невозможен без заимствования определенной терминологии из технических дисциплин. При этом следует учитывать, что «специальные термины должны не только отражать понятие, но и быть в той или иной степени признанными как в технической, так и в юридической науках» [4, с. 36].

Отметим, что до настоящего времени преступность в социальных сетях не была самостоятельным объектом исследования, а отдельные связанные с ней вопросы лишь поверхностно затрагивались в контексте рассмотрения глобальных проблем компьютерной и интернет-преступности.

Так, для идентификации того или иного преступления как «компьютерного» целесообразно, на наш взгляд, использовать два критерия: 1) средством (либо орудием) совершения такого преступления является компьютерная техника (компьютеры, их системы, сети и программное обеспечение) или иные технические устройства (смартфоны, мобильные телефоны и т. д.); 2) наличие непосредственной связи совершенного деяния с автоматизированной обработкой данных (изготовлением, модификацией, передачей компьютерной информации, незаконным доступом к ней и т. д.). Именно второй критерий позволит исключить из категории «компьютерных» преступлений деяния, не имеющие отношения к сфере информационных технологий (например, умышленное повреждение автомобиля путем сбрасывания на него персонального компьютера). Указанные критерии можно также назвать отличительными признаками компьютерной преступности.

Составной частью компьютерной преступности является преступность в сети Интернет. Именно к ней относится изучаемая нами преступность в социальных сетях. При этом в отличие от последней интернет-преступность ранее неоднократно выделялась как отдельный вид преступности и становилась объектом научных исследований. К данному виду преступлений относятся «любые запрещенные уголовным законом общественно опасные деяния, совершенные посредством или с помощью Интернет» [4, с. 44]. Существенных отличий в понимании интернет-преступлений в научном сообществе нет. Все определения сводятся к указанию основного критерия их идентификации – использование при их совершении сети Интернет.

В связи с тем что интернет-преступность является неотъемлемой частью компьютерной преступности, она обладает всеми присущими ей признаками, равно как и признаками преступности в общем понимании. Однако, будучи самостоятельным видом преступности, она обладает и собственным отличительным признаком – обязательным использованием сети Интернет при совершении каждого из преступлений, которые она охватывает.

Многие свойства интернет-преступности непосредственно связаны с технологией Интернет. К ним относятся глобальность и трансграничность, неперсонифицированность и условная анонимность. К перечисленным свойствам Р. И. Дремлюга добавляет удаленность, доступность, автоматизированность, крайне высокую латентность, интеллектуальность и быстрый рост указанного вида преступности [4, с. 45]. Мы полностью согласны с его выводами.

Так, говоря об удаленности как свойстве интернет-преступности, следует отметить, что сеть связывает множество компьютеров и иных технических устройств по всему миру. Любых пользователей, вступающих в контакт посредством Интернет, равно как преступника и его жертву, в физическом мире могут разделять сотни или тысячи километров. При этом использование различных анонимайзеров и прокси-серверов (средств сокрытия информации о компьютере или пользователе сети от удаленного сервера) позволяет виртуально присутствовать в нескольких местах (и даже государствах) одновременно. Таким образом, реальное местонахождение технического устройства, с использованием которого было совершено общественно опасное деяние, и место, где наступили его общественно опасные последствия, могут быть значительно удалены друг от друга. Все это порождает ряд сложностей при расследовании интернет-преступлений, начиная от установления места их совершения и заканчивая установлением субъекта преступления и его местонахождения.

Доступность заключается в массовом распространении интернет-технологий, внедрении их во многие сферы жизнедеятельности общества и одновременном удешевлении как самого подключения, так и технических устройств, обладающих минимальными характеристиками для такого подключения. В настоящее время возможность использования сети Интернет (зачастую с нескольких устройств) имеется даже у лиц младшего школьного возраста.

Такое свойство, как автоматизированность интернет-преступности, тесно связано с ее неперсонифицированностью, однако имеет несколько иное содержание. Современное программное обеспечение позволяет настроить выполнение многих действий в автоматическом режиме, без участия человека (подбор паролей, копирование данных и т. д.). Помимо этого, как отмечает Р. И. Дремлюга, «существуют вредоносные программы, которые самостоятельно распространяются уже в течение многих лет» [4, с. 47], т. е. участие человека требуется лишь на этапе создания такой программы и ее запуска. Среди примеров можно назвать троянские программы, которые попадают на компьютер пользователя под видом легального программного обеспечения и осуществляют различные несанкционированные пользователем действия: сбор и передачу информации, ее модификацию, уничтожение и тому подобные действия, а также различные вирусные программы, например, компьютерный вирус *I love you*, который распространяется по электронной почте и содер-

жит вложенный файл под названием «LOVE-LETTER-FOR-YOU.txt.vbs» (любовное послание для тебя). [5]. Его опасность состоит в том, что он скрывает видео и аудиофайлы, записывает в файлы различных форматов свои копии, а также скачивает из сети Интернет дополнительные вирусные модули и устанавливает их в систему.

Еще одним свойством интернет-преступности является ее крайне высокая латентность. Так, И. М. Рассолов по итогам проведенного исследования утверждает, что «лишь 10–12 % этих преступлений становятся достоянием гласности» [6, с. 133]. А по отдельным видам преступлений в сфере компьютерной информации М. В. Старичков (по выведенным им на основе теории социальной дезорганизации формулам) вычисляет уровень латентности около 99,7–99,8 % [7, с. 19]. Мы же согласимся с мнением Р. И. Дремлюги о том, что реальный уровень латентности преступности в Интернет «оценить сложно в силу неоднородности данного вида деяний» [4, с. 49]. Причинами латентности рассматриваемого вида преступности С. М. Храмов называет нежелание потерпевших сообщать в правоохранительные органы о совершенных компьютерных преступлениях, попытки самостоятельно решить проблему, боязнь затягивания процесса расследования уголовного дела. Сюда также относят «нежелание отдельных пользователей и компаний предоставлять правоохранительным органам доступ к своим конфиденциальным данным, вариабельность конфигураций возможностей, доступных преступнику в Интернет, быстрое развитие модификаций способов совершения преступлений» и т. д. [8, с. 50–51].

Такое свойство, как интеллектуальный характер, подразумевает, что совершение любого преступления в сети Интернет требует определенного набора знаний (умение пользоваться компьютером, знание физических и логических принципов функционирования сети Интернет и т. д.). Безусловно, в последние годы требования к уровню образования субъекта преступления в сфере информационных технологий становятся все менее высокими, поскольку преступники зачастую используют программные средства и скрипты (от англ. *script* – сценарий, краткое описание действий, выполняемых системой), созданные другими людьми. Однако, как показывает мировая практика, многие компьютерные преступники обладают высоким уровнем интеллекта и стремятся к постоянному развитию своих умений и навыков. Как отмечает Р. И. Дремлюга, «интеллектуальность пропагандируется также посредством субкультуры хакеров, что дает стимул интернет-преступнику для умственного саморазвития» [4, с. 48].

Еще одним важным свойством интернет-преступности является ее быстрый рост. В исследовании Т. Л. Тропина указывает, что «количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей, и, по оценкам Интерпола, темпы роста преступности в глобальной сети Интернет являются самыми быстрыми на планете» [9, с. 3]. Эта общемировая тенденция проявляется и в нашем государстве, о чем свидетельствуют статистические данные. Так, в первом полугодии 2017 года в сфере информационной безопасности возбуждено на 8,8 % уголовных дел больше, чем за аналогичный период 2016 года [10]. Все это свидетельствует о широкой распространенности такого негативного явления, как интернет-преступность, и недостаточной эффективности мер по борьбе с нею.

Составной частью интернет-преступности является преступность в социальных сетях. Как уже отмечалось, никогда ранее она не рассматривалась в качестве самостоятельного вида преступности. Однако в последние годы социальные сети выделились в особую коммуникационно-информационную сферу в рамках Интернета, находятся на лидирующих позициях по посещаемости в сравнении с другими ресурсами Глобальной сети и обладают специфическими криминогенными свойствами. Ввиду этого социальные сети создают особые условия как для развития традиционных преступлений (мошенничество, оскорбление и т. д.), так и для появления их новых разновидностей (например, несанкционированный доступ к чужому аккаунту в социальной сети; вовлечение несовершеннолетних в деятельность, ставящую под угрозу их жизнь и здоровье, – так называемые игры со смертью и др.). В связи с этим современная реальность требует разработки новых криминологических подходов к рассмотрению преступности в социальных сетях как отдельного вида интернет-преступности и соответствующей системы мер ее предупреждения.

Являясь составной частью интернет-преступности, а также компьютерной преступности и преступности в общем ее понимании, преступность в социальных сетях обладает всеми признаками и свойствами, присущими указанным видам преступности и рассмотренными выше. При этом сами социальные сети занимают отдельный сегмент сети Интернет и представляют собой особую специфическую сферу распространения преступности. Ввиду изложенного преступность в социальных сетях является самостоятельным видом преступности и обладает особыми, присущими только ей и непосредственно связанными с социальными сетями свойствами и закономерностями развития, на которых мы предлагаем остановиться далее.

Так, к отличительным свойствам преступности в социальных сетях можно отнести широкую выборку потенциальных жертв преступления, исходя из размещенных пользователями на персональных страницах личных данных. Как уже отмечалось, социальные сети обладают огромной популярностью в сравнении со многими другими ресурсами сети Интернет, особенно в молодежной и подростковой среде. Они образуют особую информационно-коммуникационную сферу, основанную в первую очередь на поиске и установлении контактов с определенным кругом лиц. Исходя из этого, большинство пользователей социальных сетей указывают на страницах свои персональные данные: фамилию, имя, дату рождения, место учебы, работы и т. д. Это позволяет другим пользователям легче найти в социальных сетях своих родственников, друзей и знакомых. Но в то же время предоставляет преступникам широкие возможности для парсинга личных данных пользователей при осуществлении выборки потенциальных жертв преступления по полу, возрасту, уровню образования, кругу интересов и т. п.

Отличительным свойством преступности в социальных сетях также является специфический комплекс способов и средств совершения подобных преступлений, основан-

ный на использовании функциональных возможностей социальных сетей (массовая рассылка сообщений, репосты, приглашения, реклама и т. д.) и активном применении методов социальной инженерии. Среди наиболее ярких примеров здесь следует привести мошенничество при проведении розыгрышей призов. Подобные розыгрыши являются одним из наиболее действенных способов расширения аудитории определенного сообщества или группы в социальных сетях. Так, объявляя розыгрыш какого-либо приза (зачастую в качестве такового выступают довольно дорогостоящие вещи – смартфоны, планшеты, гироскутеры и т. д.), администрация сообщества выдвигает два условия участия в нем: вступление в данное сообщество и репост записи конкретного розыгрыша, т. е. размещение информационной заметки о его проведении на своей странице в социальной сети без изменения ее содержания и со ссылкой на источник. В случае реального проведения такого розыгрыша победитель определяется рандомным путем (от англ. *random* – случайный, произвольный, выбранный наугад) с использованием специальных приложений из числа лиц, выполнивших оба условия. Мошенники же каждому человеку, сделавшему репост, пишут сообщение о том, что он выиграл приз, однако для его пересылки в адрес победителя требуется внести определенную денежную сумму на счет организатора розыгрыша. Как правило, запрашиваемая сумма значительно меньше ценности самого приза, что заставляет множество людей, теряя бдительность, выполнять указания мошенников. И даже в случае обнаружения обмана потерпевшие, как правило, не сообщают об этом в правоохранительные органы по причине незначительного материального ущерба. Обычно подобная деятельность мошенников заканчивается всего лишь блокированием созданного ими сообщества администрацией социальной сети, что никоим образом не мешает им вновь создавать аналогичные группы. Разумеется, что описанная деятельность неразрывно связана с методами социальной инженерии, которую также называют «хакерством с использованием человеческого фактора, неискушенности жертв в вопросах мошенничества и методах скрытого управления человеком» [11, с. 2–3], изучению которых посвящены соответствующие разделы социологии и психологии.

Еще одной особенностью преступности в социальных сетях является организация активной поддерживающей преступность деятельности (создание сообществ, групп, организация виртуальных мероприятий и т. д.). Она имеет тесную связь с описанными выше свойствами и вытекает из сущности самих социальных сетей. Как для привлечения целевой аудитории, интересующейся определенной проблематикой, создается соответствующее тематическое сообщество, так и преступники создают различные группы в социальных сетях, где аккумулируются персональные страницы их потенциальных жертв (например, как в описанной выше ситуации – желающих выиграть определенный приз) либо закрытые группы единомышленников, где преступники делятся своим опытом, идеями и т. д. Например, по запросу «хакер» по состоянию на 01.10.2017 в социальной сети «ВКонтакте» обнаружилось 1477 различных сообществ, численность наиболее популярных из которых превышала 30–60 тыс. человек.

Помимо изложенного к специфическим свойствам преступности в социальных сетях относится использование при совершении преступлений, как правило, фейковых (от англ. *fake* – подделка) аккаунтов либо «взломанных» персональных страниц других пользователей. Очевидно, что ни один человек (за исключением лишь малообразованных дилетантов) не решится совершить преступление со страницы, на которой указаны его реальные анкетные данные и место жительства. Для этих целей создаются фиктивные страницы с указанием вымышленных сведений либо персональных данных другого лица. Более подготовленные преступники, обладающие навыками несанкционированного доступа к компьютерной информации, используют чужие страницы. В такой ситуации они получают дополнительные преимущества, в частности доступ к страницам других пользователей из круга общения лица, чей аккаунт был взломан, и возможность манипулировать доверительными отношениями, которые наладило это лицо в социальной сети, общаясь с потенциальными жертвами от его имени.

В заключение следует выделить такое свойство преступности в социальных сетях, как быстрый информационный обмен и расширение целевой аудитории в геометрической прогрессии. Данное свойство также тесно связано с функциональными возможностями социальных сетей. Например, суть репоста заключается в том, что определенное информационное сообщение попадает не только на страницу того человека, который его сделал, но и в новостные ленты всех лиц, с которыми у него установлен контакт.

Возвратимся к описанному примеру с розыгрышем призов. Любой пользователь, решивший в нем поучаствовать, неосознанно вовлекает в участие десятки и даже сотни своих друзей и знакомых, а те в свою очередь распространяют эту информацию далее с «эффектом снежного кома». У данного свойства имеется и другая сторона. В равной степени быстро распространяется информация и о возможных способах совершения преступлений. Получив подобную информацию, определенные неустойчивые личности (зачастую несовершеннолетние) решают самостоятельно ее апробировать. В результате с нарастающим эффектом создаются копии определенных сообществ преступной направленности, до тех пор пока определенная идея не станет общеизвестной и не исчерпает себя. Наиболее ярким примером здесь можно назвать популяризацию и широкое распространение в 2016–2017 гг. так называемых групп смерти с названиями «Синий кит», «Море китов», «Тихий дом» и т. д. При этом, как отмечают официальные средства массовой информации, лишь в одной социальной сети «ВКонтакте» с начала 2017 года заблокированы «более 3 миллионов сообществ и пользователей откровенно “китовой” направленности». Большинство кураторов таких сообществ – те же подростки, которые просто раньше своих сверстников узнали о проведении «смертельных игр» в социальных сетях и которыми «движет возможность потренироваться в манипулировании своими сверстниками… Добавьте сюда полное отсутствие познаний в сфере уголовной ответственности – и, как результат, игра продолжается» [12, с. 15].

Заключение

На основании изложенного остановимся на следующих положениях и выводах.

1. Под преступностью в социальных сетях в Республике Беларусь предлагается понимать исторически изменчивое, массовое, общественно опасное социальное и уголовно-правовое явление, характеризующееся совокупностью преступлений (запрещенных Уголовным кодексом Республики Беларусь деяний) и лиц, их совершивших, в сфере социальных сетей с территории Республики Беларусь либо с территории других государств, но направленных против интересов Республики Беларусь и ее граждан (включая иностранных граждан и лиц без гражданства, проживающих на территории Республики Беларусь), за определенный промежуток времени.

2. Преступность в социальных сетях является составной частью преступности в общем ее понимании, ввиду чего обладает присущими ей основными признаками, такими как социальная обусловленность, историческая изменчивость, массовость, общественная опасность, уголовно-правовой, социальный и системный характер; свойствами – объективный, непреходящий характер; зависимость от состояния общественного развития, степени стабильности общества, существующих в нем противоречий; самовоспроизводство и тому подобное, а также закономерностями – усложнением в связи с развитием научно-технического прогресса, экономики, средств связи, компьютеризации; качественными и количественными изменениями в связи с потребностями общества в защите вновь возникших общественных отношений от преступных посягательств и др.

3. Будучи составной частью компьютерной преступности, преступность в социальных сетях обладает присущими ей признаками: средством (либо орудием) совершения преступления является компьютерная техника (компьютеры, их системы, сети и программное обеспечение) или иные технические устройства (смартфоны, мобильные телефоны и т. д.); наличие непосредственной связи совершенного преступления с автоматизированной обработкой данных (изготовлением, модификацией, передачей компьютерной информации, незаконным доступом к ней и т. д.).

4. Преступность в социальных сетях входит в состав интернет-преступности, ввиду чего обладает присущим ей отличительным признаком – обязательным использованием сети Интернет при совершении любого из преступлений, которые она охватывает, а также рядом свойств, среди которых выделяют глобальность, трансграничность, неперсонифицированность, условную анонимность, удаленность, доступность, автоматизированность, крайне высокую латентность, интеллектуальность и быстрые темпы роста.

5. Преступность в социальных сетях является самостоятельным видом преступности, ввиду чего она обладает и особыми, присущими только ей и непосредственно связанными с социальными сетями свойствами и закономерностями развития. К ним можно отнести широкую выборку потенциальных жертв преступления, исходя из размещенных пользователями на персональных страницах личных данных; специфический комплекс способов и средств совершения преступлений, основанный на использовании функциональных возможностей социальных сетей (массовая рассылка сообщений, репосты, приглашения, реклама и т. д.); применение методов социальной инженерии; организация активной поддерживающей преступность деятельности (создание сообществ, групп, виртуальных мероприятий и т. д.); использование при совершении преступлений фиктивных аккаунтов либо персональных страниц других пользователей, к которым получен несанкционированный доступ; массовое вовлечение потенциальных жертв в сообщества преступной направленности, а также быстрый информационный обмен о способах и средствах совершения преступлений.

Список использованных источников

1. Криминология : учебник для вузов / А. Ф. Агапов [и др.] ; под ред. В. Д. Малкова. – 2-е изд., перераб. и доп. – М. : ЗАО «Юстицинформ», 2006. – 528 с.
2. Толковый словарь русского языка / под ред. В. Д. Дмитриева. – М. : ООО «Издательство Астрель»: ООО «Издательство АСТ», 2003. – 1582 с.
3. Большой энциклопедический словарь / Л. И. Абалкин [и др.]; гл. ред. А. М. Прохоров. – М. : Сов. энцикл.1993. - 1632 с.
4. Дремлюга, Р. И. Интернет-преступность : моногр. / Р. И. Дремлюга. – Владивосток : Изд-во Дальневост. ун-та, 2008. – 240 с.
5. 10 самых опасных компьютерных вирусов всех времен [Электронный ресурс] // Ба!Топ: Все рейтинги мира. – Режим доступа: http://batop.ru/10-samyh-opasnyh-kompyuternyh-virusov-vseh-vremen/. – Дата доступа: 30.08.2017.
6. Рассолов, И. М. Право и Интернет : 2-е изд., доп. / И. М. Рассолов – М. : Изд-во НОРМА, 2003. – 210 с.
7. Старичков, М. В. Умышленные преступления в сфере компьютерной информации. Уголовно-правовая и криминологическая характеристика : автореф. дис. … канд. юрид. наук: 12.00.08 / М. В. Старичков; Байкал. гос. ун-т экономики и права. – Иркутск,2006. – 26 с.
8. Храмов, С. М. Латентная преступность: методология познания и основные направления противодействия : моногр. / С. М. Храмов; Брест. гос. ун-т имени А. С. Пушкина. – Брест : БрГУ, 2010. – 169 с.
9. Тропина, Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дис. … канд. юрид. наук : 12.00.08 / Т. Л. Тропина ; Юрид. инст. Дальневосточного гос. университета. – Владивосток, 2005. – 27 с.
10. Следственный комитет предупреждает: сообщая личную информацию в социальных сетях, вы рискуете стать жертвой злоумышленников! [Электронный ресурс] // Следственный комитет Республики Беларусь. – Режим доступа: http://sk.gov.by/ru/news-usk-gminsk-ru/view/sledstvennyj-komitet-preduprezhdaet-soobschaja-lichnuju-informatsiju-v-sotsialnyx-setjax-vy-riskuete-stat-5100/. – Дата доступа: 01.09.2017.
11. Кузнецов, М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. – СПб.: БХВ-Петербург, 2007. – 368 с.
12. Ластовский, А. Куда плывут «синие киты»? / А. Ластовский // На страже. – 2017. – 24 марта. – С. 15.

28.11.2017