

УДК 340
МРНТИ 10.77.51

ПОНЯТИЕ ПРЕСТУПЛЕНИЙ В СОЦИАЛЬНЫХ СЕТЯХ

Шут О.А.¹, Могунова М.М.¹

¹ОМГУ им. Ф.М. Достоевского, Омск, Россия

Аннотация

В данной статье рассматривается преступления в социальных сетях. Преступления в социальных сетях является общественно опасным деянием, часто совершаемым в Интернет ресурсах. Во многом данную категорию представляют мошенничество, но помимо этого существуют кражи, грабежи, обман, умышленное повреждение чужого имущества. Данный вид преступлений совершается путем обнаружения жертвы в социальных сетях, установление контакта результатом которого становится организация личной встречи, во время которой преступник обкрадывает свою жертву, похищая деньги и ценные вещи. Говоря о социальных сетях, следует понимать именно такую часть Интернет пространства, в которой существует возможность социального взаимодействия. Такое понимание дает возможность определить объекты исследования, которыми выступают не только привычные сети как «ВКонтакте», «Facebook», «Instagram» и другие, но и такие сервисы как «WhatsApp», «Skype», «Telegram» и т.д.

Ключевые слова: Интернет, преступление, преступник, аккаунт, социальные сети.

ӘЛЕУМЕТТІК ЖЕЛІЛЕРДЕГІ ҚЫЛМЫСТАР ҰҒЫМЫ

О.А. Шут¹, М.М. Могунова¹

¹Ф.М. Достоевский атындағы ОМГУ, Омбы, Ресей

Аңдатпа

Бұл мақалада әлеуметтік желілердегі қылмыстар ұғымы қарастырылады. ХХІ ғасыр ғылыми және техникалық прогрестің ең жоғары гүлдену дәуіріне айналды, олардың жетістіктері миллиондаған адамдардың өмірін едәуір жеңілдетеді. Алайда, мұндай гаджеттердің жаппай пайдалануында болуы осы саладағы қылмыс сияқты проблеманы тудырады. Ең қауіптілердің бірі ақпараттық-телекоммуникациялық ортаға, сондай-ақ Интернет желісіне ену қаупі болып табылады. Бұл мәселенің даму қаупін ХХ ғасырдың басындағы әдебиет өкілдері сипаттады. Интернет ғаламдық желісінде көптеген түрлер бар, бірақ оларды тек екі топқа бөлуге болады: адамның техникамен өзара әрекеттесуіне байланысты және адамның адаммен өзара әрекеттесуіне байланысты. Олардың арасында екінші топқа ерекше назар аудару керек, өйткені ол тек жеке тұлғаның ғана емес, сонымен қатар қоғам, мемлекет үшін де, әлеуметтік желілердегі қылмыстылық деп аталады. Әлеуметтік желілер туралы айтқанда, әлеуметтік өзара іс-қимыл мүмкіндігі бар Интернет кеңістіктің дәл осындай бөлігін түсіну керек. Facebook, Instagram және т.б. сияқты үйреншікті желілер ғана емес, сонымен қатар «WhatsApp», «Skype», «Telegram» және т.б. сияқты қызметтер көрсететін Зерттеу нысандарын анықтауға мүмкіндік береді.

Түйінді сөздер: Интернет, қылмыс, қылмыс, қылмыскер, аккаунт, әлеуметтік желілер.

THE CONCEPT OF CRIMES IN SOCIAL NETWORKS

O. Shut¹, M. Mogunova¹

¹Omsk state University named after F.M. Dostoevsky, Omsk, Russia

Annotation

This article discusses the concept of crimes in social networks. The XXI century has become the era of the highest flowering of scientific and technological progress, achievements that significantly simplify the lives of millions of people. However, the presence of such gadgets in mass use, creates a problem such as crime in this area. One of the most dangerous is the threat of penetration into the information and telecommunications environment, as well as the Internet. The threat of such a problem was described by representatives of the literature in the early twentieth century. In the global Internet, there are many varieties, but they can be divided

into only two groups: those that are related to the interaction of man with technology, and those that are related to the interaction of man with man. Among them, special attention should be paid to the second group, since it is the one that poses the greatest threat to the security of not only the individual, but also to society and the state. It is called crime in social networks. Speaking of social networks, it is necessary to understand exactly the part of the Internet space in which there is a possibility of social interaction. This understanding gives you the ability to define objects, which are not only the usual networks as «Vkontakte», «Facebook», «Instagram» and others, but also services such as «WhatsApp», «Skype», «Telegram», etc.

Key words: Internet, crime, criminal, account, social networks.

Введение

XXI век стал эпохой наивысшего расцвета научного и технического прогресса, достижения которых существенно упрощают жизнь миллионов людей. Однако наличие таких гаджетов в массовом пользовании, и порождает такую проблему как преступность в данной сфере. Одной из наиболее опасных выступает угроза проникновения в информационно-телекоммуникационную среду, а также в сети Интернета. В глобальной сети Интернет существует много разновидностей, их можно разделить всего на две группы: на те, что связаны с взаимодействием человека с техникой (хищения при помощи программных и аппаратных средств), и на те, что связаны с взаимодействием человека с человеком (обязательное участие и действия двух живых людей). Особое внимание следует уделить второй группе, поскольку именно она представляет наибольшую угрозу для безопасности не только личности, но и для общества, государства и называется она, преступностью в социальных сетях [1].

В тенденции развития преступности в социальных сетях исследователи отмечают следующее:

- Образуются новые виды преступлений, такие как, нарушение конфиденциальности личных электронных данных, где объектом выступают новые охраняемые законом интересы, возникшие в связи с развитием преступности.

- Информационные сети в глобальной сети используются для совершения таких деяний, за которые предусмотрена ответственность уголовным законодательством многих стран (хищения имущества, распространение запрещенных товаров и т.д.).

Для того, чтобы стать преступником в социальных сетях не нужно иметь специальное, дорогостоящее оборудование и профессиональное образование. Начинающему киберпреступнику достаточно иметь компьютер, оснащенный соответствующим оборудованием и выход в Интернет. Причем дальнейшие знания он может приобрести на специальных форумах, где уже опытные хакеры пошагово научат молодого специалиста всем тонкостям преступного ремесла. Также, на все тех же форумах можно приобрести программное обеспечение для взлома какой-либо системы, или собрать команду для совместной атаки на интересующий объект [2].

Задачи. Для эффективного решения данной проблемы сформулированы основные задачи:

- социальных сетях, следует понимать именно такую часть Интернет пространства, в которой существует возможность социального взаимодействия. Такое понимание дает возможность определить объекты исследования, которыми выступают не только привычные сети как «ВКонтакте», «Facebook», «Instagram» и другие, но и такие сервисы как «WhatsApp», «Skype», «Telegram» и т.д. У данного подхода имеется немало последователей среди исследователей и криминалистов как отечественных, так и у зарубежных. Однако существует сложность в оценке масштабов криминальных

проявлений в социальных сетях. - для объективного анализа совершенных преступлений мешают такие факторы как низкий уровень статистической отчетности правоохранительных органов, а также трудности с выявлением, расследованием и раскрытием преступлений, совершенных с использованием информационно коммуникационных технологий. Большинство исследователей указывают на то, что сбор статистических показателей испытывает сложность в получении достоверной информации [3].

– основную часть преступлений в социальных сетях составляют общественно опасные деяния, непосредственно связанные с незаконным оборотом наркотических средств и психотропных веществ. Как правило, это незаконное приобретение и незаконный сбыт запрещенных средств. Помимо этого, встречаются случаи контрабанды и пересылки наркотических средств.

Среди данных веществ, являющиеся предметом незаконных действия, можно выделить несколько распространённых веществ, такие как «спайс», который составляет 1/3 часть, амфетамин, марихуана, гашиш, героин и другие вещества, за хранение, распространение и оборот, которых предусмотрена уголовная ответственность. Основной способ незаконного приобретения незаконных веществ является «закладка». Система данной операции заключается в следующем, покупатель осуществляет покупку наркотика через электронный платеж, после чего продавец дает координаты тайника, где лежит заветный товар. Следующий способ приобретения наркотика заключается в заранее запланированной личной встречи продавца с покупателем, где передача товара и денежной платы за него производится на месте. Менее популярные способы посредством почты, через курьерские доставки, путем передачи через водителей общественного транспорта не подозревающие о содержимом посылки. Сотрудники спецслужб указывают на трудности в связи с электронными денежными переводами, где не имеется возможность установить преступный факт и проследить связь, между продавцом и покупателем. Также сложность заключается в определении местоположения. Поскольку продавец и покупатель могут быть не только в разных городах, но и странах, где действуют разные законодательства [4].

Цель. Преступления в социальных сетях является общественно опасным деянием, часто совершаемым в Интернет ресурсах. Во многом данную категорию представляют мошенничество, но помимо этого существуют кражи, грабежи, обман умышленное повреждение чужого имущества. Данный вид преступлений совершается путем обнаружения жертвы в социальных сетях, установление контакта результатом которого становится организация личной встречи, во время которой преступник обкрадывает свою жертву, похищая деньги и ценные вещи.

Преступление бывают разных категорий:

– Мошенничество. Выделяют два вида мошенничества: финансовое и нефинансовое. Однако при всем при этом, почти половина случаев мошенничества приходится на несанкционированное списание денежных единиц с банковской карты получившее название «фродинг». Для его осуществления нет необходимости социального взаимодействия преступника с жертвой [5].

Немало преступлений в сфере мошенничества совершаются при виртуальном товарообмене, то есть, жертва обращается по объявлению о продаже какой-либо вещи или оказание услуг. Далее, встреча назначается в удобном для нарушителя месте, где он может благополучно совершить кражу денег и ценных вещей. Также существуют такие схемы, где путем обмана, преступник предлагает жертве заработать деньги, но

для начала нужно перечислить Nсумму. Также, популярным стало преступление через социальные сети, цель которой заключается в получение доступа к персональным данным лица. Схема заключается в следующем. Преступник отправляет сообщение потенциальной жертве с весьма интересным содержанием, с ссылкой на фейковый сайт где необходимо ввести свои личные данные. Или, достаточно просто перейти по липовой ссылке, а преступник за счет этого получает доступ к данным жертвы [6].

– Вымогательство имеет за собой большую историю и с развитием человечества, преобразованию подвергалась и данная преступная ниша. В настоящее время, через социальные сети, вымогательство вышло на совершенно новый уровень. Главное суть не претерпела серьезных изменений, ведь получение легких денег в крупном размере всегда двигало преступников на рискованный шаг. Для потерпевшего стоит угроза в распространении позорящих сведений, информации, аудио-видео материалов в отношении его. Но как вымогатели получают такие материалы на конкретную личность? Добывают их не в течении десятилетней слежке. Преступник, обладающий знаниями в сфере Иттехнологий не сложным для себя путем получает доступ к личным данным интересующего объекта. Получить такой доступ можно используя, следующие инструменты - специальные программы, в основе которых лежит вирусный код, написанный преступником лично, либо приобретенный на соответствующих форумах или Интернет - площадках, задача которых проникнуть в систему жертвы и вывести все данные на адрес преступника - непосредственно личная, быстрая атака преступника на социальные сети жертвы с целью получения доступа к персональным данным.

Самым эффективным остается первый способ. Его суть заключается в создании вирусного кода, который проникает в незащищенную или слабо защищенную систему, после необдуманных и случайных действий пользователя. Такие действия как регистрация на сомнительном сайте, использование одного пароля для всех аккуантов, переход по ссылке из сообщения от неизвестного пользователя, скачивание каких-либо материалов из Интернета и многие другие виды уловок, на которые попадают обычные пользователи Интернета. В последнее время распространенным становится проникновение и изъятие данных из мобильных телефонов, так как они очень плотно вошли в жизнь большинства жителей земли. По своей неосторожности, мы доверяем слишком много информации для наших мобильных гаджетов, что в конечном счете может сыграть с нами в злую шутку. Помимо того, что преступники получают доступ к конфиденциальным данным в распространении, которых пользователь совершенно не заинтересован, количество хакерских атак на сотовые телефоны увеличились в связи с внедрением банковских приложений «мобильный банкинг» [7].

Целью вымогателей является получить выгоду, финансовое вознаграждение за нераспространение информации, играя на внутренних чувствах жертвы. Никто не хочет, чтобы о нем распространяли информацию, которая как-то очернит или опозорит лицо, именно на этих тонких нотах играют преступники. Для перевода денежных средств, преступники обычно используют подставные банковские карты, одноразовые Интернет кошельки и как сейчас стало модно, через криптовалюту. На данный момент, это самая безопасная система для скрытых денежных транзакций, несмотря на то, что все транзакции в открытом доступе. Однако, выследить личность, которой принадлежит криптовалютный кошелек практически невозможно.

Результаты исследования

Решить эту проблему возможно проведением многокритериальных исследований оптимальных параметров эффективности алгоритма, охватывающих вопросы состава и структуры преступлений. Структурные блоки алгоритма должны учитывать связи между элементами состава преступлений, определять функции и задачи, решаемые при помощи методов управления и контроля средств современной вычислительной техники и банков данных.

В преступлениях, связанных с нарушением неприкосновенности частной жизни, характерно распространение информации, добытая законным путем в отношении конкретного лица. Такие поступки совершаются не профессиональными преступниками, а скорее знакомыми из общего круга общения, который затаил обиду и решил отомстить. Однако, бывают случаи, когда данное преступление совершается профессионалом своего дела и в большинстве случаев, такое преступление проходит по совокупности с «создание, использование и распространение вредоносных компьютерных программ». Связано это, конечно же, с тем, что профессиональный преступник использует незаконные способы добычи информации на жертву, во многом это осуществляется при помощи специальных программ, в основе которых заложен вирусный код.

Таким же образом, производится добыча личной переписки жертвы. Фрагменты переписки могут использоваться для вымогательства, очернение репутации, обмана и прочее. Нарушение тайны переписки влечет уголовную ответственность в соответствии со статьей 145 УК РК от 3 июля 2014 года [9].

Совершение преступлений, связанных с незаконным оборотом специальных технических средств, назначением которых является негласное получение информации связано с тем, что преступники используют социальную сеть для заказов или для сбыта незаконного товара, информации, материалов и т.д.

Нарушение авторских прав в современном мире получило широкое распространение и здесь не обошлось без социальных сетей. Пользователи, находясь в Интернете, регулярно пользуются услугами компьютерных мастеров, для улучшения состояния своего компьютера. Этим и пользуются преступники, размещая на своих страницах рекламу, с соответствующим перечнем услуг и переходили в состояние покоя, ожидая, когда жертва сама придет к ним. Когда же наступал день «Х», то преступник устанавливал на компьютер жертвы программы, где вирный код обезвреживал всю систему защиты, после чего, преступник получал доступ ко всей информации находящейся на компьютере жертвы удаленно.

При помощи социальных сетей совершаются такие противоправные деяния как преступления в сфере компьютерной информации. Основная составляющая такого вида преступности составляет – неправомерный доступ к компьютерной информации, а также, встречаются случаи создания, использования и распространения вредоносных компьютерных программ. Огромное количество преступлений были совершены в результате взлома аккаунта пользователя в социальных сетях, после чего они его блокировали, меняли логин и пароль, вносили некоторые изменения на странице, распространяли сообщения подписчикам и друзьям с просьбой об оказании материальной помощи.

Следующий вид преступлений связан с незаконным оборотом сильнодействующих веществ. Так, через социальные сети производится распространение анаболических стероидов, а также иные сильно действующие

вещества, целевой аудиторией которых являются спортсмены, которые хотят нарастить мышечную массу и улучшить свои спортивные показатели. К наиболее распространенным можно отнести такие вещества как метандиенон, дегидрохлорметилтестостерон, метилтестостерон, станозолол, тренболон, эфиры тестостерона и другие. Также, часто встречаются распространители средств для похудения, которые приносили большой вред здоровью. В составе таких веществ преобладал сибутрамин, которые предавал чувство насыщения, после приема которого, человек долгое время не нуждается в пище, что может привести к анорексии.

Виновные лица, занимались рекламой запрещенных препаратов путем таргетированной рекламы и рассылкой в личные сообщения. После чего реализовали незаконный оборот запрещенных веществ.

Дискуссия

Социальные сети способствуют развитию таких преступлений как насильственные общественно опасные деяния, направленные против жизни и здоровья личности. Данный вид преступлений и без социальных сетей был широко распространен, однако, в современном мире он перешел на новый уровень. В процессе общения в социальных сетях, между собеседниками возникает конфликт, который перерастает в откровенное оскорбление друг друга, последствием которого является совместная встреча и перепалка. Простым языком, конфликт в Интернете переходит в выяснение отношений на кулаках. Итог таких конфликтов всегда один, это причиненный вред здоровью.

Далее, будут описываться единичные виды преступлений, совершенных в социальных сетях или посредством их использования, несмотря на то, что по отдельности их мало и они кажутся незначительными, в совокупности они составляют 1/12 часть всех видов преступлений в социальных сетях. Среди которых замечены преступления связанные со сбытом холодного оружия, охотничьи ножи, кастеты, распространение нацистской атрибутики на холодном оружии. Преступники занимались рекламой и сбытом данных вещей, некоторые самостоятельно изготавливали кастеты и продавали, и размещали их в соц. сетях на своей странице с целью продажи [10, с. 192].

Сводничество также приобрело свое место в социальных сетях. Организовывая интим-салон, организатор создает страницу в социальных сетях скрывая основной род ее деятельности, используя термины и прочие слова, чтобы человек не знающий их, не имел понятия о данной странице. Некоторые смелые организаторы таких притонов в открытую говорят, о своем роде деятельности и публикуют все сведения, а также, фотографии своих сотрудниц для привлечения клиентов. Данные страницы не пользуются услугами рекламы.

С развитием социальных сетей, очень сильно выросли, преступления, квалифицируемые как клевета. Характерные черты данного рода деяния, основана на личной неприязни лиц между собой или в одну сторону. Эта неприязнь переходила в опубликование в социальных сетях ложной информации, порочащая, честь и достоинство оппонента. За все время не было зарегистрировано жалоб по этому поводу со стороны мужского пола, что наталкивает на вывод, что данные преступления свойственны в отношении лиц женского пола. Также, нарушители общественного порядка создавали страницы на имя потерпевшего, где публиковали заведомо ложную информацию, а также интимные предпочтения потерпевшего, в том числе оказание сексуальных услуг. Более изобретательные лица используют фотографии

порнографического характера с изображением девушки, которая была похожа на потерпевшую с указанием номера телефона для связи.

В таких случаях, помимо распространения ложной информации, порочащая, честь и достоинство потерпевших, распространению поддавалась и информация из личной тайной жизни граждан, в том числе фотографии с их изображением, сведения о фамилии, имени, дата и место рождения, сведения о семье, месте учебы, номера телефона, домашний адрес [11].

В социальных сетях не обошлось без преступлений, связанных с незаконным приобретением, нарушением порядка выдачи и оборота официальных документов. Пользуясь услугами рекламы в социальных сетях широко распространяются объявления, о свободном получении поддельных документов о высшем образовании, свидетельств, награждениях, сертификатов, лицензий, удостоверений (в том числе служебных), паспортов и водительских удостоверений [12].

Заключение

Таким образом, результаты аналитических исследований позволили сделать вывод, где нельзя утверждать, что проведенное исследование отражает истинное состояние и структуру преступности в социальных сетях Интернета. Фактически описаны результаты работы правоохранительных органов по выявлению, раскрытию и расследованию таких преступлений. Однако и эти результаты могут служить основой для оценки тенденций преступности, для организации профилактической деятельности, в том числе виктимологической профилактики. В ряде случаев они позволяют обнаружить проблемы, связанные с юридической оценкой деяний, требующие дополнительной разработки и решения.

Преступления в социальных сетях переживают свой рассвет в преступной среде. Сложность в определении лица совершившее уголовно наказуемое деяние оставляет без наказанными преступников, что порождает дальнейшее распространение незаконных действий привлекая все новые и новые лица в жизнь по ту сторону закона. На данный момент персональные данные граждан находятся под очень слабой защитой, будь это аккаунт в социальных сетях или банковский счет, для матерого преступника не составит труда получить доступ кэти данным. Даже при условии, что уровень безопасности данных будет на высочайшем уровне, человеческий фактор может сделать эту безопасность бесполезной. Наивная доверчивость людей, к незнакомцам, которые предлагают какую-либо заманчивую и выгодную помощь порождает очень много преступлений. А значит, необходимо проводить профилактические мероприятия по обеспечению безопасности своих личных данных, поведение в социальных сетях и давать рекомендации при выявлении признаков преступного деяния.

Литература:

1. Ефимов Е.Г. Социальные Интернет- сети (методология и практика исследования)/ Е.Г. Ефимов. - Волгоград: Волгоград. науч. изд-во, 2015. - 169 с.
2. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы / А.Л. Осипенко. - Омск: Омская академия МВД России, 2009. - 480 с.
3. Тропина Т.Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма? / Т.Л. Тропина // Международное правосудие. - 2012. - № 3. - С. 86-95.
4. Никулин И.В. О практике противодействия незаконному обороту и пропаганде наркотических средств и иных психотропных веществ в информационно-телекоммуникационной сети

- Интернет / И.В. Никулин // Вестник Сибирского юридического института ФСКН России. - 2013. - № 2 (13). - С. 46–50.
5. Сынгаевский Д.В. Мошенничество в глобальной сети Интернет как объект виктимологического исследования / Д.В. Сынгаевский // Современный юрист. - 2013. - № 4. - С. 136-144.
 6. Простосердов М.А. Вымогательство, совершенное в сети Интернет / М.А. Простосердов // Библиотека криминалиста. - 2013. - № 6 (11). - С. 150-162.
 7. Соловьев В.С. Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) / В.С. Соловьев // Криминологический журнал Байкальского государственного университета экономики и права. - 2016. - Т. 10, № 1. - С. 60-72.
 8. Pol'shikov A.V. Criminogenic Characteristics of Persons Involved in the Production and Trade of Child Pornography in the Internet. *Obshchestvoipravo = SocietyandLaw*, 2009, no. 3, pp. 190-194. (InRussian).
 9. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 11.01.2020 г.).
 10. Pol'shikov A.V. Criminogenic Characteristics of Persons Involved in the Production and Trade of Child Pornography in the Internet. *Obshchestvoipravo = Society and Law*, 2009, no. 3, pp. 190-194. (In Russian).
 11. Смагина А.В., Сопун Д.И. Причины распространения экстремизма в России // Российский следователь. – 2012 г. - № 8 – С. 35.
 12. Комаров А.А. Компьютерное мошенничество в России и США: Анализ количественных показателей за 2002-2012 г. // Юридическая правоохранительная практика. – 2016 г. - № 35 – С. 172-177.