СОЦИАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОЙ РОССИИ

НАУЧНАЯ СТАТЬЯ

DOI: 10.21684/2587-8484-2018-2-4-42-58 **УДК** 316.334.4

Социологический анализ проблемы мошенничества на сайтах социальных сетей

Александра Игоревна Кухто[1], Анна Васильевна Мальцева[2]

[1] студентка кафедры социального анализа и математических методов в социологии, Санкт-Петербургский государственный университет (г. Санкт-Петербург, РФ)
a-kuh@bk.ru

[2] доктор социологических наук, доцент кафедры социального анализа и математических методов в социологии, Санкт-Петербургский государственный университет (г. Санкт-Петербург, РФ)
annamaltseva@rambler.ru

Аннотация. В статье рассматривается использование социальных сетей в качестве виртуального продолжения социального пространства, в рамках которого актуальна проблема реализации различных видов мошеннических действий. Целью исследования является социологический анализ компьютерной преступности, необходимый для выработки качественных мер по повышению уровня безопасности взаимодействий при использовании сайтов социальных сетей и профилактики интернет-преступности. В статье освещены общие принципы, негативная и позитивная специфика взаимодействий пользователей при использовании сайтов социальных сетей с учетом закономерностей реальных общественных отношений и некоторые аспекты нормативно-правовых актов государственного уровня в сфере компьютерных преступлений и интернет-безопасности. Данная статья содержит выявленные в ходе исследования характерные условия для реализации, роста и развития компьютерной преступности в пространстве социальных сетей, описание ее специфики, основных целей и технологических составляющих. На основе полученных в ходе социологического анализа данных возможна разработка мер личной защиты сведений пользователей, профилактики компьютерной преступности на сайтах социальных сетей.

Ключевые слова: сайты социальных сетей, Интернет, информация, интернет-мошенничество, киберпреступность, информационные угрозы, безопасность информации.

Цитирование: Кухто А. И. Социологический анализ проблемы мошенничества на сайтах социальных сетей / А. И. Кухто, А. В. Мальцева // Siberian Socium. 2018. Том 2. № 4. С. 42-58.
DOI: 10.21684/2587-8484-2018-2-4-42-58

ВВЕДЕНИЕ

Еще в конце XX в. цифровые технологии начали внедряться во все сферы человеческой жизни, стремительно изменяя ее и способствуя возникновению качественно новых видов общественных отношений. Интернет дал человеку почти безграничные возможности по передаче и обработке информации и совершению операций, которые раньше были осуществимы только в физическом мире, в том числе и банковских.

Однако не всю активность в Интернете можно рассматривать как положительную, и определенные виды деятельности внутри Сети способны привести к негативным последствиям и отрицательному влиянию на те или иные сферы жизнедеятельности.

Относительная новизна общественных отношений, реализуемых посредством социальных сетей интернет-пространства, и лишь частичное существование правового поля, которое способно регулировать действия внутри Сети, приводят к возникновению проблем и опасностей, связанных с угрозами преступлений, производимых с помощью интернет-технологий. Популярность и постоянное развитие социальных сетей в интернет-пространстве делает возможным возникновение новых видов общественно опасных действий, а также трансформации традиционных правонарушений.

Среди подобных преступлений мошенничество относится к числу наиболее часто встречающихся и проявляется в Сети в различных видах. Несмотря на то, что компьютерное мошенничество возникло уже на ранних стадиях внедрения Интернета в общее пользование, с каждым годом появляется все больше новых способов его реализации. Однако меры предупреждения и воздействия в этом случае в основном носят противоречивый и фрагментарный характер, редко поспевая за их изменчивостью.

Для создания качественного правового регулирования деятельности в социальных сетях интернет-среды крайне необходимо междисциплинарное исследование всех угроз, способных возникнуть на их платформе. Мошенничество является одной из самых часто возникающих и, возможно, опасных угроз, социологический анализ которой, являющийся основной целью данной работы, необходим для выработки качественных мер защиты и профилактики.

ОСНОВНАЯ ЧАСТЬ

Понятие социальной сети начало разрабатываться в социологии еще в середине XX в., однако за шестьдесят с лишним лет оно претерпело большую трансформацию значений. Первые сайты, появившиеся в Интернете, не предполагали связи ни между пользователем и администратором сети, ни между пользователями. Пользователи оставались анонимными потребителями предложенного администраторами контента. Различные инструменты обратной связи появлялись постепенно, с развитием технологий. Первоначально возникли функции голосования, комментирования, потом службы общения развивались в виде конференций, чатов [1, с. 111]. Тем самым веб-сайты стали постепенно превращаться в разновидности виртуальных социальных сетей.

В целом виртуальные социальные сети — одна из форм виртуального социального пространства, которую можно определить как виртуальную социальную структуру, в которой различаются виртуальные социальные группы, виртуальные личности, виртуальные индивидуумы. Поэтому в качестве социальной сети можно рассматривать любое интернет-сообщество, где пользователи каким-либо образом могут общаться и обмениваться информацией между собой. Данные сообщества чаще всего формируются на основе общих интересов людей, их взглядов на жизнь, ценностей.

Для понимания онлайн-взаимодействий во второй половине XX в. ученые, в первую очередь западные, обратились к активным исследованиям социальных сетей, структуры отношений в них и действий пользователей, создающих и изменяющих данные структуры. Еще большее развитие подобные исследования получили в начале XXI в. (см., напр., работы Б. Хогана (B. Hogan) [15], Д. М. Бойд (D. M. Boyd) [14] и мн. др.). Так, 10 лет назад под редакцией Н. Г. Филдинга и Р. М. Ли (N. G. Fielding and R. M. Lee) был опу-

бликован фундаментальный «Справочник по методам онлайн-исследований» [16]. Поэтому трудно не согласиться с мнением А. А. Морозовой о том, что сформировались представления, в соответствии с которыми сайты социальных сетей, являясь одним из атрибутов информационного общества, формируют особое коммуникативное пространство, общение в котором имеет свои особенности и отличия от общения в реальном, физическом мире [7, с. 201-202].

Взаимодействие на сайтах социальных сетей представляет собой серию связей между профилями пользователей, реализуемых как «дружба» в социальной сети. Эти связи, как справедливо указывает Е. Г. Ефимов, «позволяют пользователям сети создавать общественные или полуобщественные профили в пределах ограничений, наложенных системой, определять группу других пользователей, с которыми они могут общаться и делиться информацией, просматривать и связывать их контакты, сообщения, лайки и пр.» [4, с. 27].

Несмотря на всю специфику виртуальных отношений, они все еще остаются отношениями между человеком и человеком, человеком и группой или группой и группой, в которых по-прежнему действуют человеческие законы и правила [10, с. 128-129], реализуются поведенческие установки и потребности [13]. Кроме того, несмотря на достоинства социальных сетей, основным их недостатком является анонимность и обезличенность, которые могут повлечь за собой опасности и угрозы различного рода, в числе которых и различные мошеннические действия.

Довольно большой объем добровольно размещаемой в сети личной информации выводит на первый план проблему информационной безопасности и защиты от неправомерных посягательств на хранящиеся в социальных сетях данные, а также на интеллектуальную, финансовую и физическую собственность.

Важность угроз информационного характера подчеркивается Доктриной информационной безопасности Российской Федерации, которая обозначает «основные их виды:

— угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
— угрозы информационному обеспечению государственной политики Российской Федерации;
— угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
— угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России» [2].

Одним из основных видов компьютерной преступной деятельности, наиболее часто реализуемой посредством социальных сетей в Интернете и имеющей непосредственную связь с безопасностью информации и личных данных, является компьютерное мошенничество. С развитием информационных технологий и становлением сайтов социальных сетей в качестве основных платформ для взаимодействия в Интернете мошеннические действия стали приобретать особую специфику, выражающуюся в создании новых форм преступной деятельности, опирающихся на определенные свойства и функции виртуальной среды.

Сайты социальных сетей привлекают разного рода мошенников тем, что их аудитория постоянно и быстро растет и обновляется, она свободна в распространении информации, может сохранять анонимность и практически не контролируется администрацией сайта, что порождает отсутствие регулирования любой деятельности, связанной с общением на сайте.

Кроме того, существует ряд характеристик данных сайтов, образующих совокупность условий для роста и развития преступлений этого вида. Такими характеристиками являются:

1. Во-первых, анонимность, которую можно создать при наличии определенных навыков и знаний, причем зачастую достаточно простых и базовых. Возможности анонимного доступа к социальным сетям не только порождают большое количество опасной информации, спама и рекламы, но и ощущение свободы и безнаказанности, благоприятствующее развитию мошеннических схем внутри сети.
2. Во-вторых, предоставляемая функционалом социальных сетей оперативность действий и передачи информации, которая позволяет в максимально короткие сроки получать сообщения, совершать электронные платежи и коммерческие операции. Быстрота таких операций и легкий доступ к ним охватывает практически все интернет-пространство и создает задержку от момента совершения преступного деяния до момента осознания пользователем того, что он стал его жертвой, что, в свою очередь, способно обеспечить отсутствие последствий для мошенника.
3. В-третьих, отсутствие эффективного правового регулирования интернет-платежей и интернет-банкинга, а также обеспечения мер по осуществлению безопасного пользования услугами киберплатежей и переводов.
4. В-четвертых, трансграничный характер социальных сетей, а значит, и совершаемых на их платформе преступлений, вследствие которого мошенник и его жертва могут находиться в разных городах, регионах и странах земного шара. Посредством разницы в законодательствах и территориях данное явление способно усложнить поимку преступника, а также предоставить ему возможность совершения преступлений в нескольких местах одновременно.

Таким образом, социальные сети создают благоприятную среду для развития мошенничества, использующего все более изощренные способы совершения преступных деяний. В настоящее время наказание за компьютерное мошенничество предусмотрено ст. 159 УК РФ. Но, тем не менее, оно широко распространено и очень динамично развивается.

В современной научной литературе существуют различные его дефиниции: «завладение чужим имуществом путем обмана, злоупотребления доверием, присвоения, растраты, а также причинение имущественного ущерба путем обмана или злоупотребления доверием, совершенные с использованием средств компьютерной техники» [12, с. 445]; «противоправное умышленное искажение, изменение или раскрытие данных с целью получения выгоды (обычно в денежной форме) с помощью компьютерной системы, которая используется для совершения или прикрытия одиночного, или серийного преступления» [6, с. 62] и др. Все они раскрывают те или иные стороны подобного вида преступлений в сфере компьютерной информации.

Данный вид преступлений в социальных сетях представляет собой результат взаимодействия внутри наиболее незащищенной сферы общественных отношений. В отличие от любого другого вида компьютерных преступлений, мошеннические действия наиболее примечательны тем, что в сути своей направлены не на компьютер и иные средства передачи информации, а непосредственно на человека. В основном мошенники нацелены на получение денежных средств обманным путем или путем злоупотребления доверием человека. Чаще всего преступники совершают такие действия, которые практически невозможно отличить от предлагаемых в сети легальными предпринимателями и фирмами товаров и услуг, не только нанося ущерб пользователям, но и подрывая репутацию и доверие к законной коммерческой деятельности в сети.

Мошенничество на сайтах социальных сетей имеет, согласно характеристике И. А. Никитиной, две составляющие — технологическую и коммуникативную. Первая подразумевает под собой создание схемы действий и использование интернет-среды для сокрытия следов преступления (например, создания анонимности) и получения денежных средств от пользователя без непосредственного контакта с ним. Вторая же

включает психологическое воздействие на потенциальную жертву, мотивирующее ее действовать в интересах мошенников [9, с. 122].

Важным аспектом информационной безопасности является предупреждение и противодействие использованию сайтов социальных сетей в мошеннических целях, однако в условиях современного динамически развивающегося мира это становится непростой задачей. Исследователи считают, что на сегодняшний день не выработано мер эффективного предотвращения мошенничества в Сети, и потому высокая ответственность лежит на пользователях, к которым предъявляются требования разумной осторожности и стремления сделать свои действия в Сети максимально безопасными [3] и др.

Из возможных мер, направленных на защиту пользователей социальных сетей, можно выделить три категории: меры, предпринимаемые администрацией социальных сетей; меры, предпринимаемые коммерческими организациями, которые могут нести риски в случае мошеннических действий; и меры, которые способны предпринять рядовые пользователи [8, с. 71].

Исходя из вышесказанного, мошенничество на сайтах социальных сетей можно считать одним из самых распространенных и опасных противоправных действия в интернет-среде. Оно имеет различные формы и особенности и трансформируется с развитием технологий, создавая угрозы как для рядовых пользователей, так и для коммерческих организаций, становясь проблемой государственного и даже межгосударственного уровня. Кроме того, оно имеет опасное социально-психологическое влияние на пользователей, имевших опыт столкновения с данным явлением.

Социологический опрос пользователей сети Интернет был проведен нами с целью изучения осведомленности и отношения пользователей к действиям мошенников на сайтах социальных сетей. В выборку по данному опросу были включены те пользователи сети Интернет, которые также зарегистрированны на сайтах следующих социальных сетей: «ВКонтакте», «Одноклассники», Instagram, YouTube, Facebook, Twitter; так называемые мессенджеры — системы мгновенного обмена текстовыми, аудио- и видео-сообщениями (например, Telegram, WhatsApp) — в исследовании не учитывались.

Объемом генеральной совокупности было решено считать количество пользователей социальной сети «ВКонтакте» (488 810 000) в соответствии с «Каталогом пользователей ВКонтакте» [5], так как практически все российские пользователи социальных сетей зарегистрированы в данной сети. В таком случае при доверительном интервале, равном 5, и доверительной вероятности, равной 95%, минимальный размер выборки респондентов для того, чтобы она считалась репрезентативной, будет равняться 385 респондентам. При расчете выборки учитывалось возрастное распределение пользователей социальной сети. Кроме того, в анкету вошли вопросы, призванные выявить причину регистрации и пользования сайтами социальных сетей, уровень доверия пользователей к собеседникам и администрации сайтов и актуальность проблемы мошенничества.

В ходе эмпирического исследования было опрошено 428 человек. Для информационного обеспечения исследования были использованы следующие программные средства. Социологический опрос был запущен на платформе Google Forms (Google Формы), которая является онлайн-сервисом для создания форм обратных связей, включающих в себя анкетирование, опросы, онлайн-тестирования и формы регистрации.

Использование в эмпирическом исследовании данного технического инструмента обусловлено удобством его применения и рядом достоинств:

- простота и понятность интерфейса для респондентов;
- бесплатность и круглосуточная доступность к данным с различных устройств;
- возможность публикации ссылки на различных платформах, в том числе на сайтах социальных сетей;
- предоставление возможности скачивания полученных данных в различных форматах, подходящих для Microsoft Excel и статистического пакета для обработки данных — SPSS.

Всего опрошено 1 093 пользователя сети. Время проведения опроса — май 2018 г.

Результаты социологического опроса можно разделить на четыре части: основная информация, область личных данных, область угроз мошенничества и область влияния направления обучения.

Большинство опрошенных находится в возрасте от 14 до 28 лет, что соответствует официальной статистике пользовательской аудитории представленных в опросе социальных сетей, позволяя считать выборку репрезентативной [11] (рис. 1).

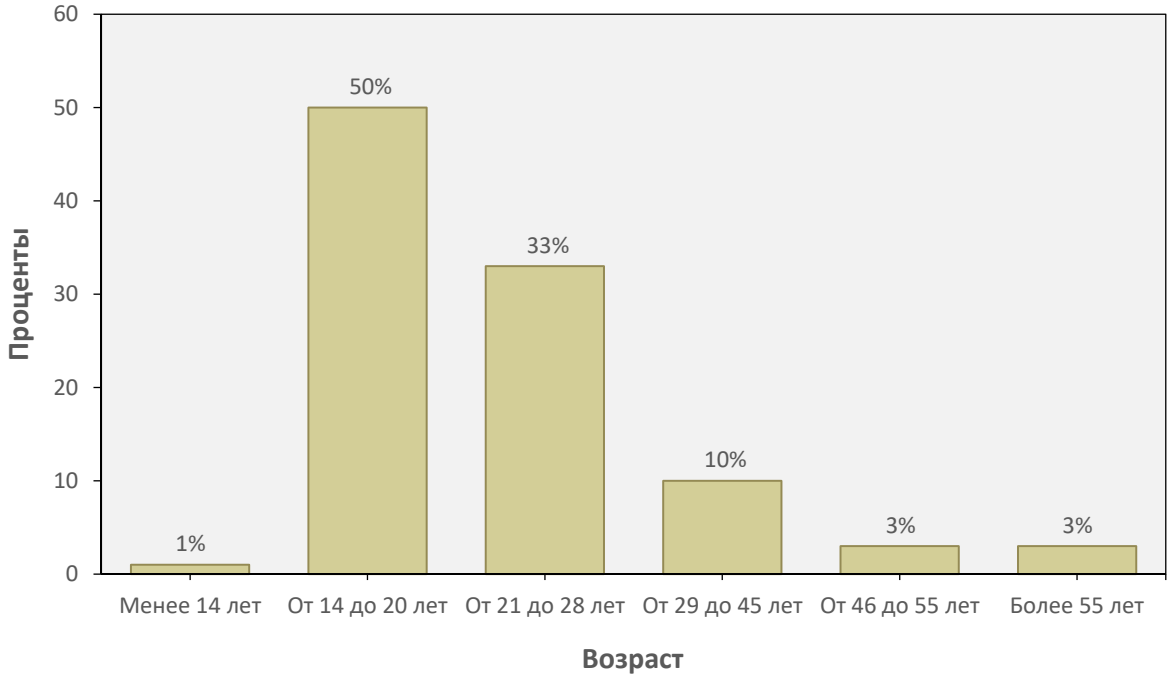
Практически все респонденты зарегистрированы на тех или иных сайтах социальных сетей. Из них подавляющее большинство сделало это самостоятельно, и лишь малая часть призналась в том, что доверила данный процесс родственникам и друзьям.

Однако даже наличие данной совокупности (меньше 5%) может говорить о том, что некоторая доля пользователей сайтов социальных сетей более подвержена опасностям и рискам взлома, так как регистрация сторонним лицом зачастую ведет к передаче паролей посредством Сети, а также к появлению у данного лица возможности социально-психологического воздействия на пользователя (рис. 2).

Наиболее популярным среди российских пользователей сайтом социальной сети безоговорочно является «ВКонтакте», однако второе место по популярности занимает YouTube — социальная медиаплатформа, построенная по принципу социальной сети, третьей же идет социальная сеть для обмена фотографиями и видеозаписями Instagram. Учитывая специфику социальных медиа и сетей, направленных на визуальные данные, можно предположить, что сохранить анонимность при регистрации на данных сайтах сложнее, чем на сайтах социальных сетей классического вида, таких как «ВКонтакте», Facebook или «Одноклассники» (таблица 1).

Информация, касающаяся личных данных, была представлена в опросе вопросами, направленными на выявление наиболее часто выкладываемых пользователями в сеть данных с учетом степени закрытости профиля пользователя от иных пользователей данной сети или Интернета.

Рис. 1. Возрастное распределение пользователей социальных сетей
Fig. 1. Age distribution of social networks' users



Наиболее актуальной информацией, чаще всего попадающей в Сеть посредством добровольной публикации, являются фотографии (что не удивительно, учитывая большое количество пользователей Instagram), однако велик процент и тех людей, которые не выкладывают в открытый доступ никаких данных. Это может объясняться как отсутствием необходимости, так и желанием сохранить полную анонимность в сети (таблицы 2-3).

Также в большинстве случаев пользователи оставляют свой профиль в социальной сети открытым. Однако при повышении возраста пользователей повышается и процент тех, кто разрешает доступ к своему профилю индивидуально (рис. 3), что может свидетельствовать о большей осторожности среди более взрослых людей и объясняться опытом столкновения с различными мошенническими действиями (рис. 4).

Область исследования, связанную с восприятием пользователями угроз мошенничества на сайтах социальных сетей, представляли вопросы об отношении к данному явлению и личном опыте (угрозы какого характера влияют на деятельность пользователей в сети, сталкивались ли пользователи с мошенничеством в социальных сетях, считают ли они себя защищенными).

У большинства пользователей вызывают волнение угрозы как человеческого, так и компьютерного характера (рис. 5), однако процент отметивших угрозы, связанные с деятельностью людей и направленные непосредственно на пользователей (например, мошенничество), почти в два раза превышает процент выбравших угрозы компьютерного характера, направленные на разрушение системы их технических средств (например, вирусы) (рис. 6).

Таблица 1. Таблица популярности социальных сетей среди пользователей
Table 1. Popularity of social networks among users

Какой социальной сетью вы пользуетесь?	Процент наблюдений
Facebook	10
ВКонтакте	96
Twitter	21
Tumblr	8
Одноклассники	4
LiveJournal	0
Ask.fm	7
Instagram	47
YouTube	62
Не пользуюсь никакой	0

Таблица 2. Публикуемые данные в среднем по выборке
Table 2. Published average data by sample

Публикуемые пользователями данные	Процент наблюдений
Фото	65
Номер телефона	12
Адрес	3
Местоположение	10
Информация о семье	6
Информация о работе	12
Не выкладываю ничего	31

Таблица 3. Публикуемые данные в разных возрастных группах
Table 3. Published data by different age groups

Публикуемые данные	До 14	14-20	21-28	29-45	46-55	56 и старше
Фото	1	33	24	5	2	1
Телефон	0	5	5	1	1	0
Адрес	0	1	1	1	0	0
Местоположение	0	4	4	1	1	1
Информация о семье	0	2	1	1	0	0
Информация о работе	0	4	6	2	1	0
Не выкладываю ничего	0	16	9	4	1	1

Рис. 2. Распределение доли зарегистрированных в социальных сетях пользователей по результатам опроса
Fig. 2. Distribution of users registered in social networks according to the survey results

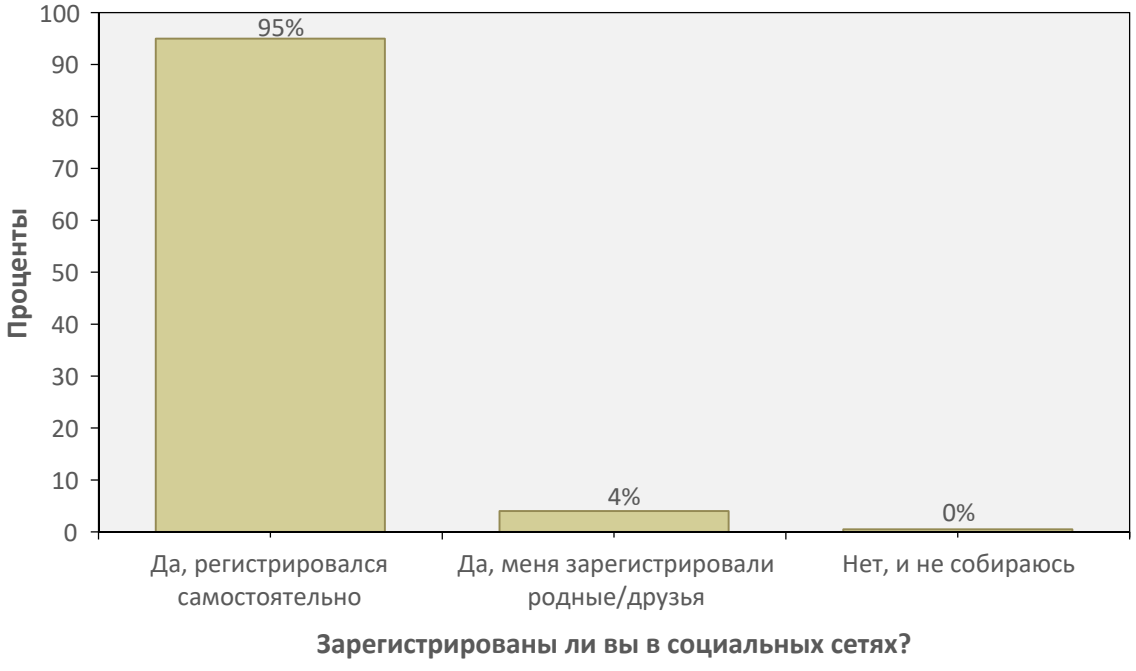
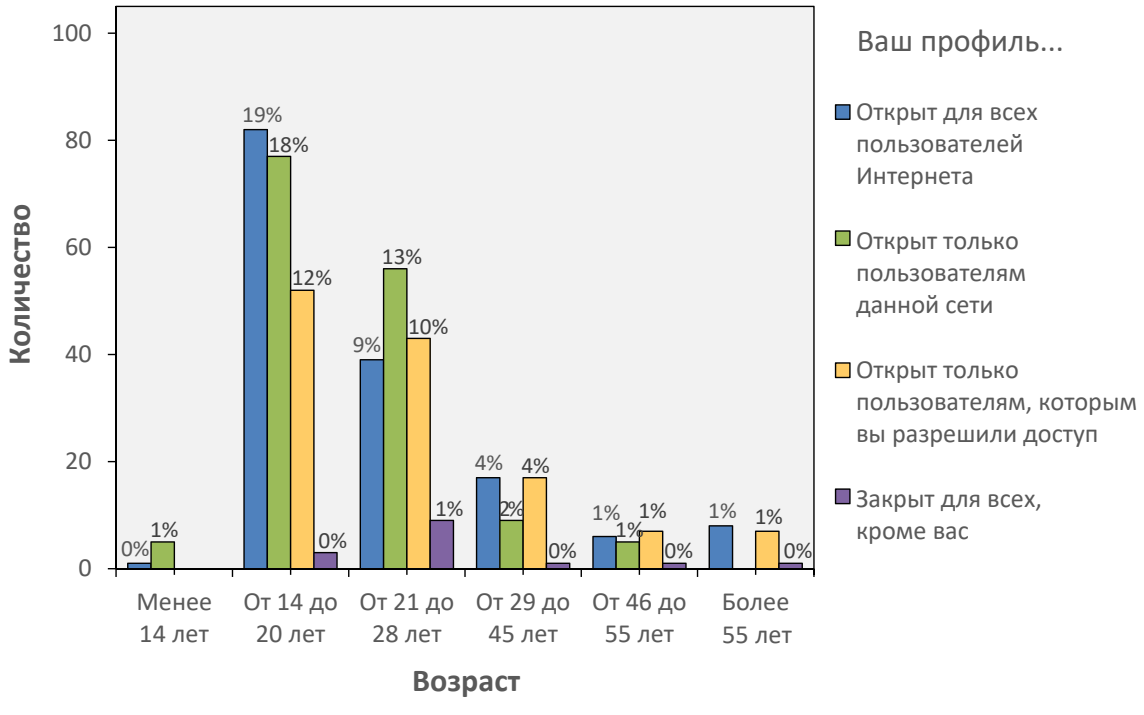


Рис. 3. Специфика конфиденциальности профилей (возрастной аспект)
Fig. 3. Profile privacy specifics by age



При распределении по возрастным категориям начинает понижаться значение переменной «компьютерные угрозы» и повышаться значение переменной, говорящей о том, что пользователей не волнует ни один из перечисленных видов угроз (рис. 5). Данная ситуация может быть связана с меньшей осведомленностью старшего поколения пользователей в сравнении с младшим, которое получает доступ к социальным сетям уже в раннем возрасте.

Также интересно распределение отношения пользователей к угрозам в зависимости от предпочитаемых сайтов социальных сетей (таблица 4). В данном случае количество людей, отметивших угрозы человеческого характера, тоже преобладает над компьютерным практически во всех социальных сетях. Исключение составляют лишь пользователи Tumblr и Ask.fm, что может объясняться большей открытостью сетей и меньшей защищенностью данных техническими средствами (например, чтобы зарегистрироваться в сети Ask.fm, подтверждение регистрации с помощью e-mail не обязательно).

При сравнении процента пользователей, сталкивавшихся за время своей деятельности в социальных сетях с мошенничеством (рис. 7), можно увидеть, что в данном случае прямой зависимости не ощущается. Примерно одинаковое количество людей, имевших личный опыт столкновения с мошенничеством в сети, как волнует проблема человеческих угроз, так и не волнует ни одна угроза.

Рис. 4. Диаграмма представлений респондентов о влиянии угроз в контексте их возраста
Fig. 4. Respondents' perceptions of the impact of threats depending on the age

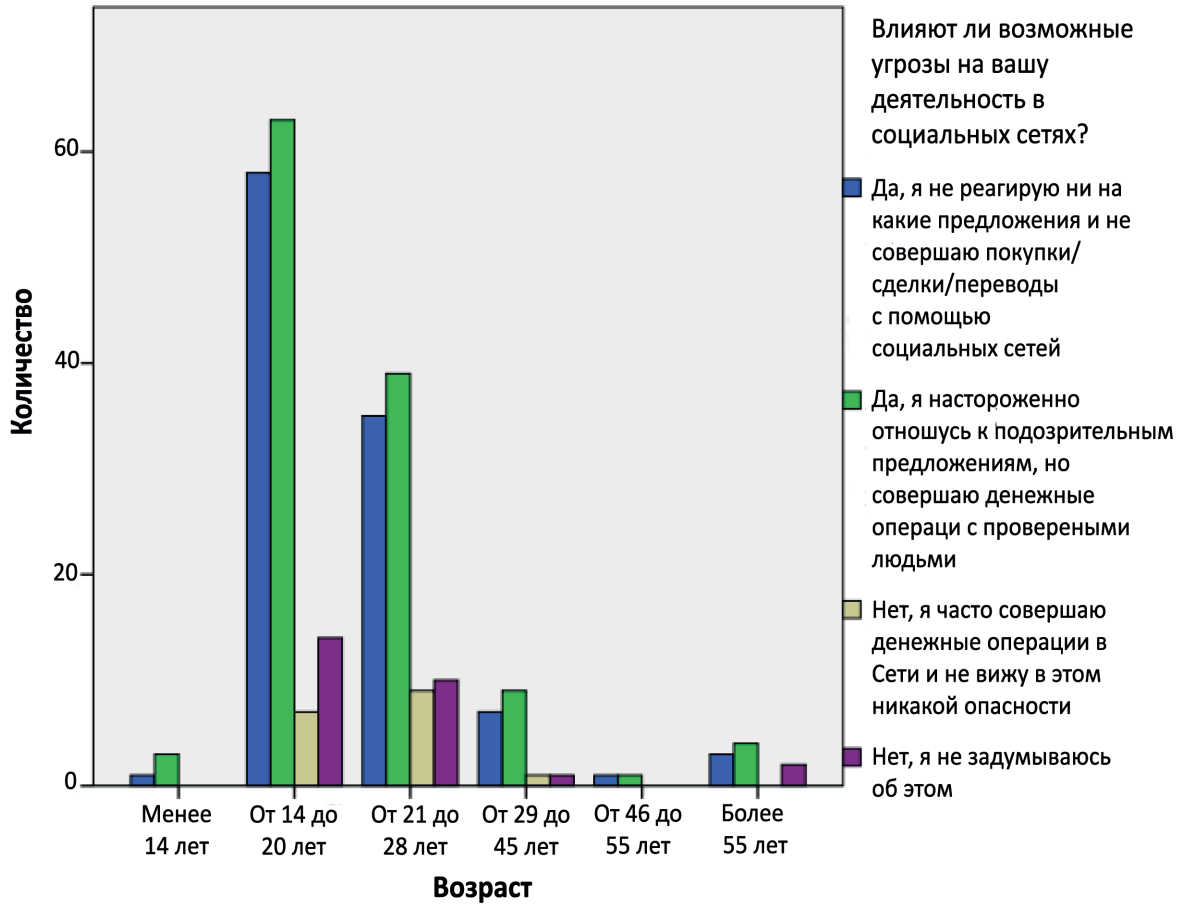


Таблица 4. Распределение характера угроз в зависимости от социальной сети, которую предпочитает респондент
Table 4. Distribution of threats depending on the social network, preferred by a respondent

Социальная сеть	Характер угроз				
	Волнуют человеческие угрозы	Волнуют компьютерные угрозы	Волнуют в равной мере	Не волнуют	Итого
Facebook	25	14	39	23	100
ВКонтакте	24	13	39	23	100
Twitter	21	12	49	17	100
Tumblr	17	20	46	17	100
Одноклассники	20	13	53	13	100
LiveJournal	0	0	0	100	100
Ask.fm	3	17	73	7	100
Instagram	26	13	44	17	100
YouTube	26	11	39	24	100
Не пользуюсь никакой	0	50	0	50	100

Рис. 5. Диаграмма представлений респондентов о влиянии мошеннических угроз на пользовательскую деятельность экономического характера в социальных сетях
Fig. 5. Respondents' perceptions about the fraudulent threats' economic impact on user activity on social networks

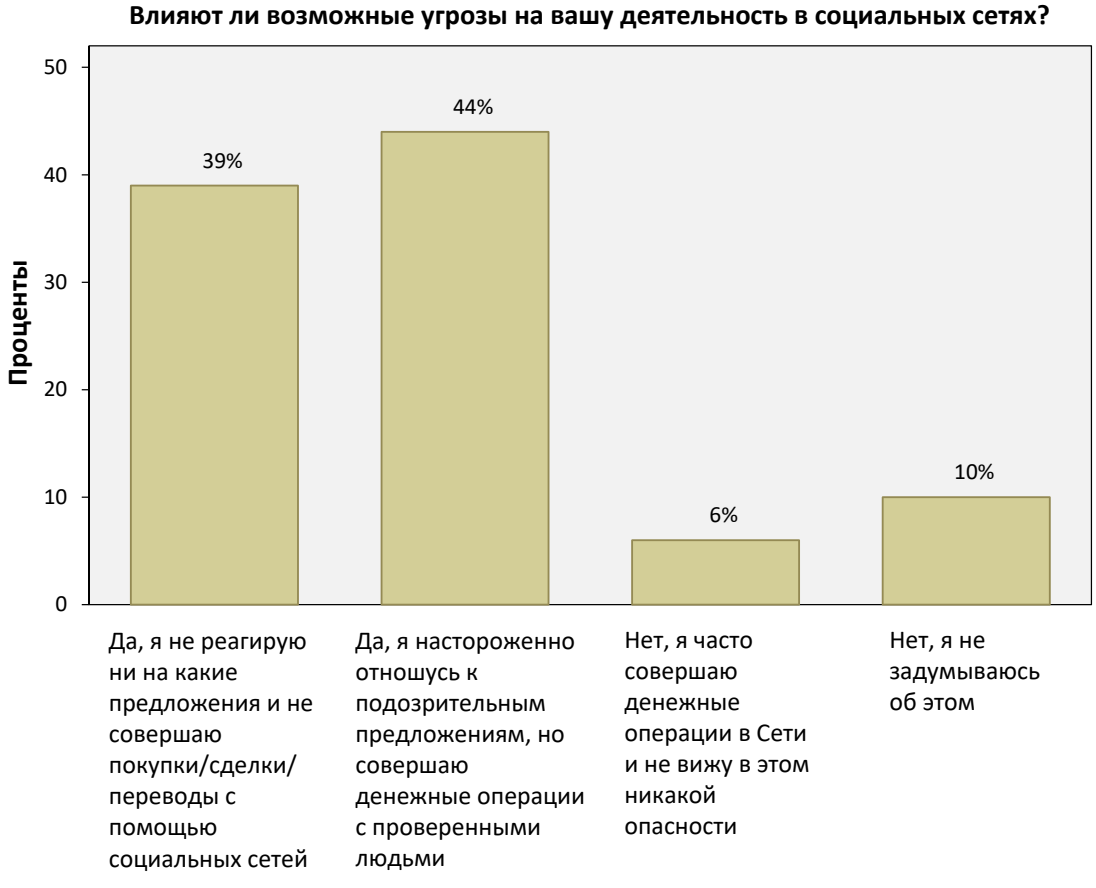


Рис. 6. Распределение мнения респондентов о характере угроз
Fig. 6. Distribution of respondents' views on the nature of threats

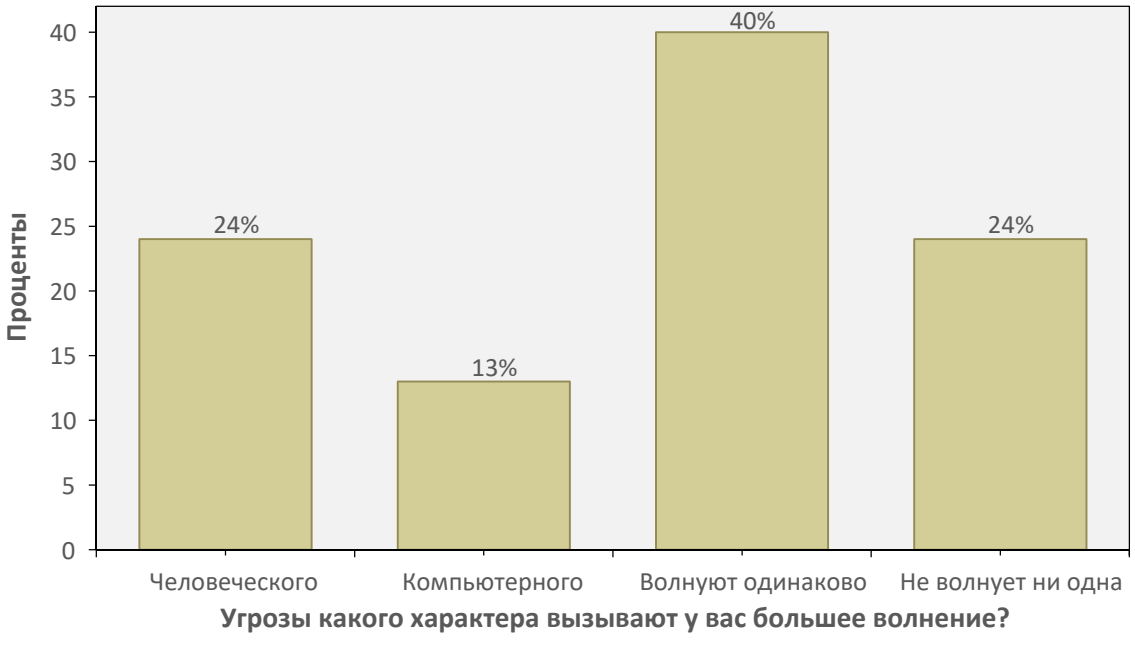
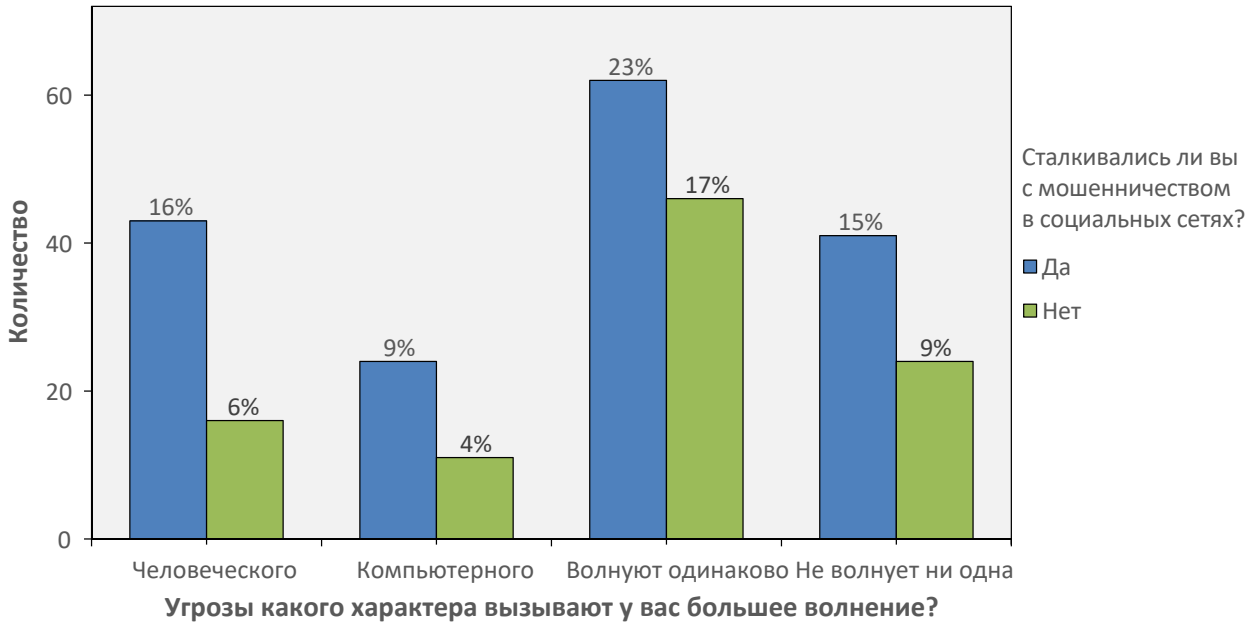


Рис. 7. Распределение характера угроз в соответствии с личным опытом пользователя
Fig. 7. Distribution of the nature of threats according to the personal user experience



Из вышеописанных графиков можно заметить, что в общем — вне зависимости от возраста, предпочитаемой социальной сети или опыта столкновения с мошенническими действиями — преобладающую долю пользователей волнуют именно угрозы человеческого характера, что может говорить об актуальности проблемы мошенничества на сайтах социальных сетей и необходимости поиска ее решения как средствами администрации сайтов социальных сетей, так и органами власти с подключением самих пользователей. На данном этапе развития законодательства в этой области, а также технологических средств предотвращения преступных действий в Сети, наиболее удачным решением нам представляется диалог.

Существование угроз, связанных с утратой финансовых средств, названо актуальной проблемой для трети пользователей в социальных сетях (рис. 8). Интересно распределение значений, показанное на рис. 9. 26% опрошенных считают проблему мошенничества в социальных сетях актуальной и сталкивались с ней лично. 37% опрошенных сталкивались с проблемой мошенничества лично, но полагают, что это случайность, и игнорируют риски. 12% не сталкивались с проблемой мошенничества лично, но оценивают риски как актуальные. Эта группа находится в наибольшей безопасности, многие настороженно относятся к сервисам и платформам по переводу денежных средств или оплате продукта и услуги, предлагаемым различными социальными сетями. И 25%, на наш взгляд, составляют группу риска, поскольку эти пользователи не сталкивались с проблемой лично и не считают ее актуальной, что может вести за собой снижение минимально необходимой осторожности поведения в сети (рис. 9).

Несмотря на большую распространенность мошенничества на сайтах социальных сетей, а также на опыт пользователей в столкновении с данным явлением, для большинства оно не является актуальным, что опять же может быть связано с малой информированностью респондентов о возможных опасностях (рис. 9).

Среди опрошенных, имевших опыт столкновения с мошенничеством на сайтах социальных сетей, больший процент считает, что они слабо защищены средствами администрации социальных сетей от различного рода преступных действий, направленных на кражу личных данных или злоупотребление доверием (рис. 10).

Данное эмпирическое исследование позволило установить ряд тенденций отношения пользователей к данному явлению и его влиянию на их деятельность внутри сети.

Рис. 8. Актуальность проблемы мошенничества для пользователей
Fig. 8. The urgency of fraud for users

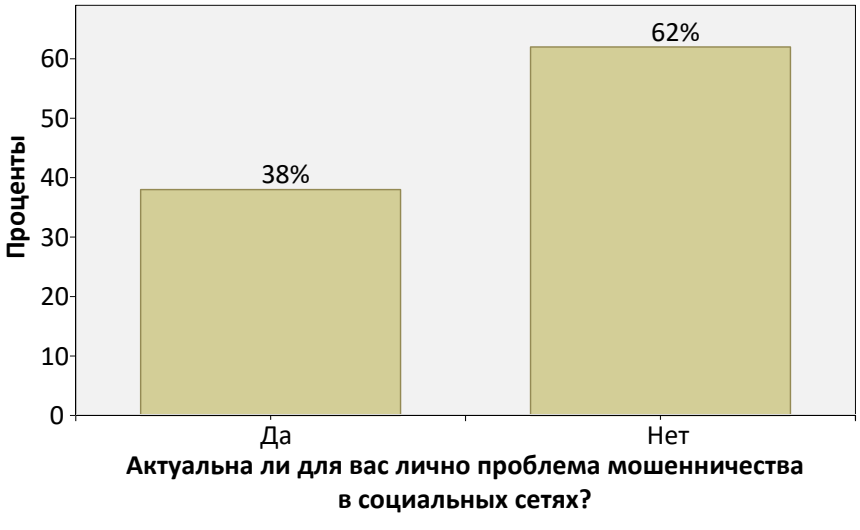


Рис. 9. Распределение мнений пользователей об актуальности проблемы мошенничества в соответствии с их личным опытом

Fig. 9. Distribution of user opinions on the urgency of fraud according to their personal experience

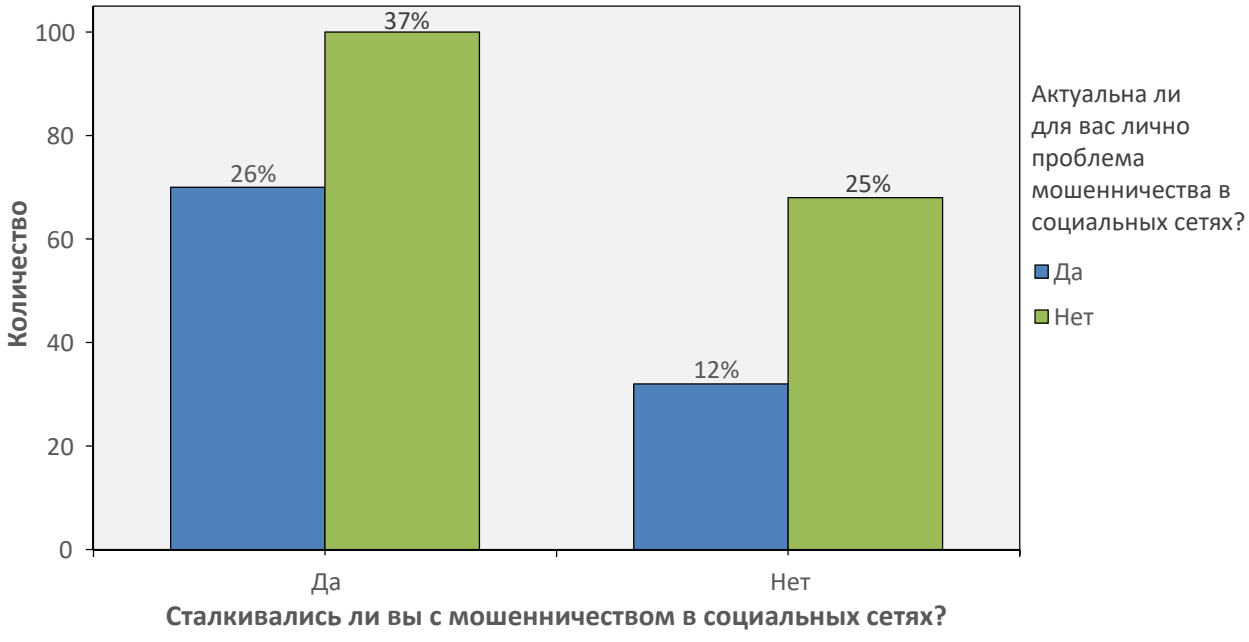
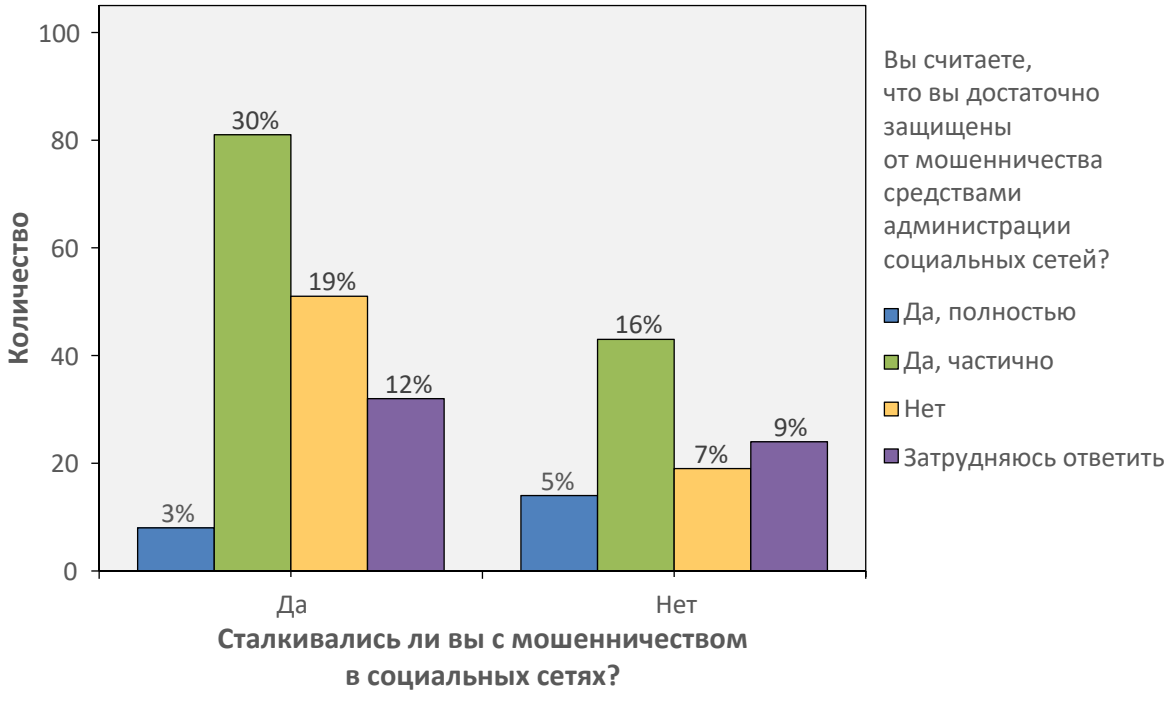


Рис. 10. Распределение ощущения защищенности в соответствии с личным опытом пользователей

Fig. 10. Distribution of the sense of security according to the personal experience of users



Во-первых, большинство пользователей склонно считать угрозы человеческого характера, возможные внутри социальных сетей, наиболее опасными для себя лично. Очевидно, проблема компьютерных угроз постепенно и успешно решается посредством создания и совершенствования различных технических средств (например, антивирусы или клининговые программы), но проблема мошенничества и злоупотребления доверием на данный момент находится на низком уровне разработанности и требует дальнейшего освещения и поиска решения.

Во-вторых, значительная доля пользователей прямо или косвенно сталкивалась с мошенническими действиями на сайтах социальных сетей, из чего следует вывод о широком распространении данного явления в Интернете и на различных платформах, вне зависимости от страны-разработчика и попыток администрации социальных сетей создать защитные меры. Мошенничество представляет собой транснациональное явление, поэтому для поиска решения данной проблемы возникает необходимость согласованности действий правоохранительных и правительственных систем различных стран.

В-третьих, потенциальные угрозы, связанные с денежными средствами, не дают пользователям полностью реализовать все возможности и сервисы социальных сетей.

В-четвертых, несмотря на широкое распространение явления мошенничества на сайтах социальных сетей, более 60% пользователей не считают проблему, связанную с мошенническими действиями в сети, актуальной для себя лично, склоняясь к рассуждениям наподобие «меня это не коснется». Данная статистика позволяет сделать предположение о малой информированности и низкой информационной культуре и грамотности пользователей, поэтому представляется важным своевременное распространение информации, связанной с теми или иными видами мошенничества на сайтах социальных сетей и его предупреждением.

ЗАКЛЮЧЕНИЕ

Итак, сайты социальных сетей становятся неотъемлемой частью жизнедеятельности людей, значимость которой непрерывно растет во всех сферах современной общественной жизни. Однако влияние социальных сетей на общественное развитие остается неоднозначным. С одной стороны, сети интернет-среды помогают более интенсивной коммуникации между людьми, быстрой передаче информации и доступу к ресурсам, необходимым для успешной жизнедеятельности индивида и удовлетворения его потребностей. С другой, виртуальное общение отличается от реального. Оно в меньшей степени подвержено контролю и регулированию, что может порождать всяческого рода риски и угрозы, связанные с потерей личных данных и формированием у индивида различных черт девиантного поведения.

Взаимодействие на сайтах социальных сетей остается одним из самых незащищенных видов человеческих взаимоотношений, создавая все новые угрозы как технического, так и, в большей степени, человеческого характера. Несмотря на развитие технологий и общества знаний, общий уровень эрудированности и образованности в котором с каждым годом должен повышаться, на данный момент далеко не все пользователи социальных сетей интернет-среды являются компетентными в области информационной грамотности и защиты личных данных. Многие не считают необходимым скрывать из общего доступа личную информацию, которая может быть использована злоумышленниками в коммерческих целях или против самих владельцев. Кроме того, большой процент пользователей не считает для себя актуальной проблему мошенничества в сети, а также проблему компьютерной безопасности.

Компьютерное мошенничество сегодня носит массовый характер, и в большинстве случаев мошеннические действия путем непосредственного взаимодействия с пользователем имеют положительный для злоумышленника исход. Мошенничество на сайтах социальных сетей развивается динамически, территориально распространено и имеет латентный характер, что затрудняет правовое регулирование и заставляет рядового пользователя принять на себя всю ответственность за защиту собственных персональных данных и финансов.

СПИСОК ЛИТЕРАТУРЫ

1. Винник Д. В. Социальные сети как феномен организации общества: сущность и подходы к использованию и мониторингу / Д. В. Винник // Философия науки. 2012. С. 110-126.
2. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).
3. Дремлюга Р. И. Интернет-преступность: монография / Р. И. Дремлюга // Владивосток: Изд-во Дальневосточного ун-та, 2008. 240 с.
4. Ефимов Е. Г. Социальные интернет-сети (методология и практика исследования) / Е. Г. Ефимов. Волгоград: Волгоградское научное изд-во, 2015. 168 с.
5. Каталог пользователей // ВКонтакте. URL: https://vk.com/catalog.php
6. Коликов Н. Л. Профессиональная компьютерная преступность и мошенничество / Н. Л. Коликов // Вестник Южно-Уральского государственного университета. Серия: Право. 2011. № 28. С. 61-64.
7. Морозова А. А. Социальная сеть: к вопросу о безопасности пользователя / А. А. Морозова // Знак: проблемное поле медиаобразования. 2017. № 3. С. 201-205.
8. Ненашев С. М. Информационно-технологическая и информационно-психологическая безопасность пользователя социальных сетей / С. М. Ненашев // Вопросы кибербезопасности. 2016. № 5. С. 65-72.
9. Никитина И. А. Финансовое мошенничество в сети Интернет / И. А. Никитина // Вестник Томского государственного университета. 2010. С. 122-124.
10. Селезенев Р. С. Социальные сети как феномен информационного общества и специфика социальных связей в их среде / Р. С. Селезенев, Е. И. Скрипак // Вестник Кемеровского государственного университета. 2013. № 2 (54). С. 125-131.
11. Сергеева Ю. Социальные сети в 2018 году: глобальное исследование / Ю. Сергеева. URL: https://www.web-canape.ru/business/socialnye-seti-v-2018-godu-globalnoe-issledovanie/
12. Фомина Н. А. Использование методов социальной инженерии при мошенничестве в социальных сетях / Н. А. Фомина // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи. 2015. С. 443-453.
13. Шилкина Н. Е. Чем «карьерист» отличается от «киллера»? Социальная адаптация в компьютерно-моделируемом виртуальном мире / Н. Е. Шилкина // Казанская наука. 2014. № 1. С. 266-268.
14. Boyd D. M. Social network sites: Definition, history, and scholarship / D. M. Boyd, N. B. Ellison // Journal of Computer-Mediated Communication. 2008. No 13. Pp. 210-230.
15. Hogan B. Analysis of social networks on the Internet / B. Hogan // Sage Handbook of Online Research Methods. Thousand Oaks, CA: Sage, 2008.
16. Sage Handbook of Online Research Methods / N. G. Fielding, R. M. Lee (eds.). Thousand Oaks, CA: Sage, 2008. 592 pp. DOI: 10.4135/9780857020055

RESEARCH ARTICLE

DOI: 10.21684/2587-8484-2018-2-4-42-58 **UDC** 316.334.4

Social networking sites as a platform for fraud

Alexandra I. Kukhto[1], Anna V. Maltseva[2]

[1] Undergraduate Student, Department of Social Analysis and Mathematical Methods in Sociology, Saint Petersburg State University (Saint Petersburg, Russian Federation) a-kuh@bk.ru

[2] Dr. Sci. (Soc.), Associate Professor, Department of Social Analysis and Mathematical Methods in Sociology, Saint Petersburg State University (Saint Petersburg, Russian Federation) annamaltseva@rambler.ru

Abstract. This article studies the use of social networks as new forms of virtual social space, which allows realizing different types of fraud. The issue is especially urgent due to the actions of users and organizations on social networks and their insufficient level of information literacy about computer security. This research aims to provide a social analysis of computer criminality before devising any effective actions for increasing security level of interactions in social networks and preventing Internet crime. This article depicts some general principles, including negative and positive features of user interactions on social networks, accounting for real public relations and government regulations in Internet security and computer crime. The results of the research have revealed the contemporary distinctive conditions for implementing, increasing, and developing computer crime on social networks, its specifics, aims, and technological components. The authors describe different kinds of criminal acts on social networks, their typology, and the fraudulent methods. This research emphasizes the deficiency of knowledge on information security, demonstrated by the Internet users. Based on the data acquired during social analysis, the authors recommend a number of personal, legal, and public actions for protecting user personal data and preventing computer crime on the Internet and social networks.

Keywords: social networks, Internet, information, Internet fraud, cybercrime, information threats, information security.

Citation: Kukhto A. I., Maltseva A. V. 2018. "Social networking sites as a platform for fraud". Siberian Socium, vol. 2, no 4, pp. 42-58.
DOI: 10.21684/2587-8484-2018-2-4-42-58

REFERENCES

1. Vinnik D. V. 2012. "Social networks as a phenomenon of the organization of society: the essence and approaches to the use and monitoring". Filosofiya nauki, no 4 (55), pp. 110-126. [In Russian]
2. Doctrine of Information Security of the Russian Federation (approved by the RF President's Decree No 646 of 5 December 2016). [In Russian]
3. Dremlyuga R. I. 2008. Internet Crime. Vladivostok: Izdatelstvo Dalnevostochnogo universiteta. [In Russian]
4. Efimov E. G. 2015. Social Internet Networks (Research Methodology and Practice). Volgograd: Volgogradskoye nauchnoye izdatelstvo. [In Russian]

5. VKontakte. “Users’ catalogue”. https://vk.com/catalog.php [In Russian]
6. Kolikov N. L. 2011. “Professional computer crime and fraud”. Vestnik Yuzhno-Ural’skogo gosudarstvennogo universiteta. Seriya: Pravo, no 28, pp. 61-64. [In Russian]
7. Morozova A. A. 2017. “Social network: on the issue of user security”. Znak: problemnoye pole mediaobrazovaniya, no 3, pp. 201-205. [In Russian]
8. Nenashev S. M. 2016. “Information-technological and information-psychological safety of the user of social networks”. Voprosy kiberbezopasnosti, no 5, pp. 65-72. [In Russian]
9. Nikitina I. A. 2010. “Financial fraud on the Internet”. Vestnik Tomskogo gosudarstvennogo universiteta, pp. 122-124. [In Russian]
10. Selezenev R. S., Skripak E. I. 2013. “Social networks as a phenomenon of the information society and specificity of social connections in their environment”. Vestnik Kemerovskogo gosudarstvennogo universiteta, no 2 (54), pp. 125-131. [In Russian]
11. Sergeeva Yu. “Social networks in 2018: global studies”. https://www.web-canape.ru/business/socialnye-seti-v-2018-godu-globalnoe-issledovanie/ [In Russian]
12. Fomina N. A. 2015. “The use of social engineering methods for fraud in social networks”. Proceedings of the Conference “Informatsionnaya bezopasnost’ i voprosy profilaktiki kiber·ekstremizma sredi molodezhi” (9-12 October), pp. 443-453. [In Russian]
13. Shilkina N. E. 2014. “What is the difference between a ‘careerist’ and a ‘killer’? Social adaptation in a computer-simulated virtual world”. Kazanskaya nauka, no 1, pp. 266-268. [In Russian]
14. Boyd D. M., Ellison N. B. 2008. “Social network sites: definition, history, and scholarship”. Journal of Computer-Mediated Communication, no 13, pp. 210-230.
15. Hogan B. 2008. “Analysis of social networks on the Internet”. In: Fielding N., Lee R. M. Blank G. (eds.). Sage Handbook of Online Research Methods. Thousand Oaks, CA: Sage.
16. Fielding N. G., Lee R. M., Blank G. (eds.). 2008. Sage Handbook of Online Research Methods. Thousand Oaks, CA: Sage. DOI: 10.4135/9780857020055