ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

А. А. Романов, В. И. Давлетов

ПРОТИВОДЕЙСТВИЕ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ДЕСТРУКТИВНЫМ ПРОЯВЛЕНИЯМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В СЕТИ ИНТЕРНЕТ КАК ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-практическое пособие

Уфа 2021

УДК 355.01:001.102:004.77-049.5(470)(076.5)
ББК 68.2-3(2Рос)я73-5
Р69

Рекомендовано к опубликованию
редакционно-издательским советом Уфимского ЮИ МВД России

Рецензенты:
М. О. Андреев
(Управление МВД России по г. Уфе);
И. М. Гаскаров
(Отдел полиции № 4 УМВД России по г. Уфе)

Романов, А. А.
Р69 Противодействие органов внутренних дел деструктивным проявлениям социальной инженерии в сети Интернет как элемент обеспечения информационной безопасности : учебно-практическое пособие / А. А. Романов, В. И. Давлетов. – Уфа : Уфимский ЮИ МВД России, 2021. – 64 с. – Текст : непосредственный.

В учебно-практическом пособии представлены основные характеристики ключевых понятий, дано описание методов ведения информационных войн и общая характеристика социальной инженерии. Приводится порядок выявления признаков ложных сообщений и противодействия им.

Предназначено для профессорско-преподавательского состава, обучающихся образовательных организаций МВД России, сотрудников органов, организаций, подразделений МВД России.

УДК 355.01:001.102:004.77-049.5(470)(076.5)
ББК 68.2-3(2Рос)я73-5

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Стратегия национальной безопасности Российской Федерации, утвержденная указом Президента Российской Федерации от 31 декабря 2015 г. № 683[1], в качестве одного из инструментов сдерживания развития России ее геополитическими противниками называет информационное давление. В последние годы мы стали свидетелями целого ряда событий, подтверждающих, что информационные войны становятся для многих стран частью их межгосударственного взаимодействия и отстаивания собственных интересов. В то же время информационные угрозы имеют широкое распространение и внутри нашей страны, в связи с чем повышается роль органов внутренних дел в противодействии им. Вследствие широкого распространения социальных сетей и мессенджеров эти средства позитивной коммуникации между людьми становятся мощным оружием, инструментом ведения информационных войн. Злоумышленниками активно применяются методы социального хакинга, под которыми понимается информационное воздействие на человека с целью провокации его на определенные, выгодные злоумышленникам действия. Для адекватного ответа этим новым угрозам необходимо проводить комплексную работу по их выявлению, купированию и устранению условий, благоприятствующих социальному хакингу. В первую очередь это относится к повышению информационной культуры и грамотности населения.

Социальные сети и Интернет являются сегодня неотъемлемой частью нашей жизни. Более того, ни одна сфера общественных отношений не обходится без удаленной коммуникации. Пандемия, вызванная распространением новой коронавирусной инфекции COVID-19, ярко продемонстрировала, что Интернет не только выступает инструментом который облегчает, ускоряет решение повседневных задач, но в отдельных случаях необходим и позволяет решить многие другие вопросы. В то же время, как справедливо заметил немецкий философ Карл Ясперс, в технике заключены не только безграничные возможности, но и безграничные опасности. В полной мере сказанное относится и к Интернету, являющемуся результатом технической революции.

Вопрос о возможных угрозах безопасности личности и, соответственно, способах защиты от данных угроз, очень объемный, многоаспектный. В данном случае целесообразно говорить о необходимости развития комплексного института информационной безопасности, а также формирования информационной культуры общества. Два этих термина («информационная безопасность» и

[1] О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 31 декабря 2015 г. № 683 // Доступ из справочно-правовой системы «КонсультантПлюс».

«информационная культура») определяют направления общесоциальной профилактики деструктивных проявлений в сети Интернет и иных коммуникационных сетях.

В данном учебно-практическом пособии произведен системный анализ примеров социального хакинга в российском сегменте социальных сетей и мессенджерах, который позволяет по-новому взглянуть на примеры отдельных, на первый взгляд безобидных, ложных информационных сообщений (так называемых «вбросов»); выявлены индикаторы ложных информационных сообщений, позволяющие идентифицировать их как социальный хакинг; выработаны конкретные предложения по противодействию социальному хакингу в социальных сетях и мессенджерах, которые ранее не озвучивались в научной литературе.

Глава 1. ОБЩАЯ ХАРАКТЕРИСТИКА МЕТОДОВ ДЕСТРУКТИВНОЙ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

§ 1. Социальный хакинг (социальная инженерия) как оружие (инструмент) информационной войны

На сегодняшний день многие говорят о влиянии информационных технологий на мир. Обсуждаются такие сферы, как бизнес, экономика, образование, а также личные отношения, которые оказывают значительное влияние на становление информационной эры, поэтому неудивительно, что люди также говорят о влиянии технологий на методы ведения войны. Термин «информационная война» используется уже в течение нескольких десятилетий, под которым понимается любая война, которая развивается в информационном XXI веке. К сожалению, многие люди используют этот термин, не зная его истинное значение**.**

Каждый день мы становимся свидетелями непостижимых возможностей системы управления информацией. По этой причине неудивительно, что часто говорят об «информационной войне». В некоторых случаях это рассматривается в качестве будущих военных доктрин некоторых стран, даже самых развитых. Информационная война влечет за собой огромные политические, технические, оперативные и правовые последствия для участвующих в ней стран.

Нет единого мнения о том, что называется информационной войной, так как это многогранная система мер противоборства, имеющая сложную систему. В своей работе «Информационные войны» Мартин Либицкий дает следующее понятие борьбе с информационной войной: «похожа на попытку слепых людей узнать природу слона: тот, кто коснулся его ноги, назвал его деревом, другой, кто коснулся его хвоста, назвал его веревкой и так далее»[1].

В данном пособии информационная война рассматривается как класс методов, включая сбор, транспортировку, защиту, отрицание, нарушение и обработку информации, с помощью которых человек сохраняет преимущество над своими противниками. Несмотря на то, что данное суждение сосредоточено на более традиционных военных понятиях информационной войны, вышеупомянутое определение, может применяться в любой конкурентной ситуации, государственной или частной, гражданской или военной.

В представленном учебном пособии информационная война рассматривается как серия нападений на гражданское или военное население государства-противника путем дезинформации и пропаганды с

[1] Понятие «Информационная война» в современной лингвистике: новые подходы. URL: https://cyberleninka.ru/article/n/ponyatie-informatsionnaya-voyna-v-sovremennoy-lingvistike-novye-podhody/viewer/ (дата обращения: 25.01.2021).

целью достижения определенных политических или военных целей. Исследователи и военные эксперты различают несколько типов информационной войны, в связи с этим необходимо понимать концепцию информационной войны в ее более широком значении. Информационные войны тесно связаны с психологическими войнами, целью которых является подрыв системы убеждений и ценностей населения, а также влияние на эмоции и рассуждения граждан. Объединяя эти два понятия, можно говорить об информационно-психологических войнах, которые становятся неотъемлемой частью постмодернистской геополитики, в дополнение к традиционным войнам[1].

Информационная война является целенаправленной попыткой подорвать и нейтрализовать систему командования и управления противника с целью манипуляции и управления.

Информационная война может включать в себя:

– сбор тактической информации;

– проверку точности информации;

– распространение пропаганды и дезинформации в целях деморализации или манипуляции противником и обществом;

– подрыв качества информации о противнике;

– лишение противника возможности собирать информацию.

Информация является стратегическим преимуществом любого государства. Этот факт впервые установили компьютерные хакеры, многие из которых в настоящее время отбывают длительные тюремные сроки именно из-за попытки отчуждения конфиденциальной информации.

Информационную войну можно классифицировать на три группы:

1) персональная;

2) корпоративная;

3) глобальная.

Также информационная война классифицируется по следующим формам:

1) война в сфере командования и управления;

2) разведывательная;

3) радиоэлектронная;

4) психологическая;

5) хакерская;

6) экономико-информационная;

7) кибервойна.

---

[1] Информационно-психологические войны. Современные психотехнологии манипулирования. Обсуждение на LiveInternet – Российский Сервис Онлайн-Дневников. URL: https://www.liveinternet.ru/users/adpilot/post283097059/ (дата обращения: 25.01.2021).

Рассмотрим наиболее распространенные типы оружия информационной войны.

1. Сбор информации является частью информационной войны, поскольку «информационная революция подразумевает возникновение способа ведения войны, в котором одна сторона, которая знает больше, чем другая сторона, будет пользоваться решающими преимуществами в ходе войны»[1]. Идея состоит в том, что, чем большим объемом информации обладает человек, тем выше его ситуационная осведомленность, что приводит к лучшим планам боя и, как следствие, лучшим результатам.

В последнее время получение информации о точном расположении стало возможным благодаря системе навигации на основе глобальной системы позиционирования (GPS).

В информационной войне сбор информации менее опасен и более полон по сравнению с традиционными способами сбора и анализа информации, поскольку эти технологии могут быть использованы для сбора точной информации с минимальной потерей точности. В связи с этим защита передачи информации через сеть имеет большое значение, так как от этого зависит конечный результат.

Таким образом, способность своевременно передавать информацию в руки тех, кто в ней нуждается, является еще одним важным аспектом информационной войны. Инструментами, используемыми в этой области, являются не только оружие, но и гражданские технологии, применяемые в военных ситуациях. Наиболее важным из этих инструментов является инфраструктура связи, состоящая из сетей компьютеров, маршрутизаторов, телефонных линий, волоконно-оптического кабеля, телефонов, телевизоров, радиоприемников, других технологий и протоколов передачи данных. Без этих технологий невозможно обеспечение передачи информации в режиме реального времени, как этого требуют современные стандарты.

2. Одним из наиболее важных аспектов информационной войны является необходимость сократить объем информации, к которой имеет доступ противник, поэтому важным оружием информационной войны является защита имеющейся информации от захвата другой стороной. Методы, применяемые для защиты информации, делятся на два класса.

Во-первых, это использование технологий, которые физически защищают наши жизненно важные объекты хранения данных (компьютеры и транспортные механизмы, включая бомбы и

[1] Информационная война: эволюция форм, средств и методов – тема научной статьи по истории и археологии читайте бесплатно текст научно-исследовательской работы в электронной библиотеке КиберЛенинка. URL: https://cyberleninka.ru/article/n/informatsionnaya-voyna-evolyutsiya-form-sredstv-i-metodov/ (дата обращения: 25.01.2021).

пуленепробиваемые оболочки), а также механизмы предотвращения вторжений (к примеру, замки, технология сканирования отпечатков пальцев).

Во-вторых, используются технологии, которые предотвращают возможность информации быть замеченной и перехваченной врагом. Этот метод включает в себя применение основных технологий компьютерной безопасности (например, пароли, а также более сложные технологии – шифрование).

Зашифровывая свои собственные сообщения и расшифровывая сообщения другой стороны, каждая сторона выполняет основные задачи информационной войны, защищая свой собственный взгляд на реальность и одновременно занижая взгляд другой стороны.

3. Следующий тип оружия в контексте информационной войны – манипулирование информацией. Манипулированием информации называется изменение информации с целью искажения реального видения картины противника. Изменение информации становится возможным при использовании ряда технологий, в том числе компьютерных программ для редактирования текста, графики, видео, аудио и других форм передачи информации. Дизайн данных выполняется вручную, в связи с чем у манипуляторов имеется высокий уровень контроля настроений целевой аудитории предоставляемой информацией. Вышеупомянутые технологии обычно используются для ускорения процесса физического манипулирования после того, как контент был загружен.

Изменение, совершенствование и отрицание какой-либо информации являются средствами достижения одной и той же общей цели – предотвращения получения врагом полной, достоверной информации.

Наиболее популярными видами оружия, используемыми для ведения информационной войны, являются:

1) заклинивание – метод, который используется для достижения отрицания и включает перехват сигналов, передаваемых между двумя каналами связи или между датчиком и каналом;

2) другим способом нарушения информации, получаемой оппонентом является введение шума в используемую частоту. Фоновый шум затрудняет для противника отделение фактического сообщения от шума. Этот метод наиболее эффективен в момент когда противник использует формы беспроводной связи, так как эти частоты можно использовать без необходимости подключения к физической сети кабелей;

3) спуфинг используется для снижения качества информации, отправляемой противнику. Поток данных противника нарушается введением в этот поток «пародии» или фальшивого сообщения. Таким образом метод спуфинга позволяет предоставлять «ложную информацию

целым системам, чтобы побудить эту организацию принимать неправильные решения на основе этой ошибочной информации»[1].

Существуют две контрмеры для защиты от спуфинга.

Во-первых, необходимо минимизировать возможность противника перехватить имеющуюся информацию. Здесь наиболее эффективны методы защиты информации, так как они не дают врагу возможности ни получить доступ, ни узнать исходный смысл сообщения или первоначальные данные.

Во-вторых, ключ к защите от манипулирования данными заключается в предотвращении повторного внедрения измененных данных в поток реальной информации. Для этого существует несколько методов, наиболее распространенным из которых является конечность. Собирая одну и ту же информацию из нескольких избыточных источников, повышается вероятность получения правильной информации. К примеру, при успешном изменении данных противником на одной линии связи, союзник может легко обнаружить неверные данные, так как они отличаются от изображения, выполненного остальными источниками.

Вопрос защиты информации в настоящее время является одним из самых актуальных. В погоне за усовершенствованием технологий защиты информации забывается человеческий фактор, который является одним из самых уязвимых элементов системы защиты информации. Злоумышленники строят свои действия на методах, основанных на социальной инженерии, приемы которой учитывают особенности психологии человека и направлены на определенные особенности личности (жадность, невнимательность, любопытство, наивность, безграмотность и другие). Методы социальной инженерии активно используются как в сети Интернет, так и за её пределами.

Понятие «социальная инженерия», которое распространено в настоящее время, появилось относительно недавно, однако похожие техники существуют с давних пор. В Древней Греции и Риме имели уважение и почет люди, которые решали сложные проблемы с помощью лжи и лести. В среде шпионов социальная инженерия также играет немаловажную роль. Выдавая себя за другого человека, агенты спецслужб могли получить информацию, содержащую в себе государственную тайну. Данная проблема касается не только государств, многие организации также подвергаются атакам в целях получения информации и совершенствуют свою корпоративную безопасность.

В сфере информационной безопасности данный термин был разработан бывшим компьютерным преступником, ныне консультантом по

[1] Актуальные методы спуфинга в наши дни — «Хакер» / URL: https://xakep.ru/2013/10/16/relevant-spuffing/ (дата обращения: 25.01.2021).

безопасности информации Кевином Митником. Он утверждал, что самым уязвимым местом любой системы безопасности является человеческий фактор. Кевин Д. Митник, сумевший проникнуть в компьютерную сеть Пентагона, в своей книге «Искусство обмана» впервые ввел понятие социальной инженерии, которая представляет собой метод получения информации путем обмана посредством использования человеческого фактора[1].

Социальная инженерия – это термин, используемый для широкого спектра вредоносных действий, которые осуществляются через взаимодействие с людьми. В социальной инженерии используются психологические манипуляции с целью обмана пользователей в совершении ошибок безопасности или распространения конфиденциальной информации. Атаки социальной инженерии происходят в один или несколько шагов: преступник сначала собирает информацию о предполагаемой жертве (потенциальные точки входа в сеть и слабые протоколы безопасности, необходимые для продолжения нападения), а затем злоумышленник переходит к завоеванию доверия жертвы и предоставляет стимулы для последующих действий, нарушающих правила безопасности (раскрытие конфиденциальной информации или предоставление доступа к критически важным ресурсам).

Социальная инженерия существует в различных формах и может быть использована в любом месте, где задействовано человеческое общение. Рассмотрим наиболее распространенные методы цифровой социальной инженерии.

1. Метод травли заключается в ложном обещании, которое направлено на такие черты характера человека, как жадность или любопытство. Таким образом, злоумышленники обманным путем получают личную информацию граждан или наносят вред их системам.

2. Самым распространённым методом социальной инженерии является использование физических носителей для внедрения вредоносных программ. Так, злоумышленники оставляют в качестве приманки зараженные вредоносными программами флэш-накопители в заметных местах, где потенциальные жертвы наверняка их увидят (например, ванные комнаты, лифты или парковка целевой компании). Приманка имеет аутентичный вид, например, ярлык, представляющий его как список заработной платы сотрудников компании. Жертвы берут приманку из любопытства, вставляют ее в рабочий или домашний компьютер, в

[1] Искусство обмана онлайн. URL: https://bookshake.net/r/iskusstvo-obmana-kevin-mitnik/ (дата обращения: 25.01.2021).

результате чего происходит автоматическая установка вредоносного программного обеспечения (далее – ПО) в систему.

Приманка мошенников не обязательно может иметь физическую форму. Онлайн-формы обмана состоят из заманчивых объявлений, которые содержат ссылку на вредоносные сайты или под видом какого-либо объявления (предложения) побуждают пользователей загружать вредоносное приложение.

3. Другим видом обмана в сети является подведение жертвы к ложным тревогам и фиктивным угрозам. Жертвы обманываются, полагая, что их система заражена вредоносными программами, и тем самым решают установить ПО, которое не имеет реальной выгоды (кроме как для преступника) или является вредоносным. Вскоре после установки такой программы преступник похищает интересующую его информацию. Распространенным примером внушения для обывателя являются всплывающие баннеры, появляющиеся в браузере во время работы в Интернете, отображая такой текст, как «ваш компьютер может быть заражен вредоносными программами-шпионами». Такие баннеры содержат предложения установить инструмент «очистки» (часто зараженный вредоносными программами), либо направить на вредоносный сайт, где компьютер подвергается повреждению вредоносной программой.

4. Следующим видом обмана является предлог. В этом случае злоумышленник получает информацию с помощью лжи. Мошенничество часто инициируется преступником под видом срочной необходимости получения конфиденциальной информации от жертвы, чтобы решить критическую задачу. Как правило, злоумышленник начинает с установления доверия со своей жертвой, выдавая себя за коллег жертвы, сотрудников полиции, банковских и налоговых органов или других лиц, имеющих право на получение данной информации. Все виды соответствующей информации и записей собираются с помощью этой аферы: номера социального страхования, личные адреса и номера телефонов, телефонные записи, даты отпуска персонала, банковские записи, информация о безопасности.

5. Одним из самых популярных видов атак в социальной инженерии является фишинг, или мошенничество, который заключается во внушении человеку чувства срочности, страха или любопытства с помощью электронной почты и текстовых сообщений. Затем он побуждает жертву раскрывать конфиденциальную информацию, переходить по ссылкам на вредоносные веб-сайты или открывать вложения, содержащие вредоносные программы. Примером может служить сообщение электронной почты, отправленное пользователям онлайн-службы, которое предупреждает их о нарушении политики и требует немедленных действий

с их стороны, например, срочно изменить пароль. Такое сообщение включает в себя ссылку на незаконный веб-сайт, почти идентичный по внешнему виду его законной версии, побуждая ничего не подозревающего пользователя ввести свои текущие учетные данные и новый пароль. После отправки формы информация направляется злоумышленнику. Учитывая, что идентичные или почти идентичные сообщения отправляются всем пользователям, обнаружить и заблокировать их гораздо проще для почтовых серверов, имеющих доступ к платформам обмена угрозами.

Существуют более целенаправленные версии фишинга, когда злоумышленник выбирает объектом атаки конкретных лиц или предприятия. Затем преступник адаптирует свои сообщения на основе характеристик, должностей и контактов, принадлежащих их жертвам для того, чтобы сделать нападение менее заметным. Фишинг требует гораздо больше усилий от преступника и может занять недели и месяцы до достижения результата. Злоумышленников, использующих такой вид фишинга, гораздо труднее обнаружить, и они имеют лучшие показатели успеха.

Сценарий фишинга может включать самого злоумышленника, который, выдавая себя за консультанта организации, отправляет электронное письмо одному или нескольким сотрудникам, которое написано и подписано точно так же, как официальное письмо компании, тем самым вводя получателей в заблуждение о том, что это подлинное сообщение. Сообщение содержит предложение изменить пароль и ссылку, которая перенаправляет их на вредоносную страницу, где злоумышленник захватывает их учетные данные.

Социальные инженеры манипулируют человеческими чувствами, такими как любопытство или страх, для осуществления схем и заманивания жертв в ловушки. По этой причине важно быть осторожным при возникновении сомнений в подлинности сайтов или при нахождении цифровых накопителей. Обратите внимание на следующие советы, которые помогут обезопасить себя от социально-инженерных атак.

1. Не открывайте сообщения электронной почты и не загружайте вложения из подозрительных источников, если вы не знакомы с отправителем или если вы не ждете письма по электронной почте. Даже если вы знакомы и подозреваете, что в сообщении может содержаться вредоносная программа, перепроверьте и подтвердите информацию из других источников, например, по телефону или непосредственно с сайта поставщика услуг. Помните, что адреса электронной почты подделываются все время. Письмо, поступающее из предположительно надежного источника, может быть фактически инициировано злоумышленником.

2. Одна из наиболее ценных частей информации, которая нужна злоумышленникам – это учетные данные пользователя. Использование многофакторной аутентификации помогает обеспечить защиту учетной записи в случае компрометации системы.

Обновляйте антивирусное ПО. Убедитесь, что автоматические обновления включены, возьмите за правило загружать последние обновления антивируса ежедневно. Периодически проверяйте, применены ли обновления, проверяйте систему на наличие возможных заражений.

Вопросы для проверки знаний

1. Какие элементы включает в себя информационная война?
2. На какие группы можно классифицировать информационную войну?
3. Назовите наиболее распространенные типы оружия информационной войны.
4. Раскройте понятие социальной инженерии, перечислите наиболее распространенные методы.

§ 2. Обнаружение, анализ и характеристика примеров социального хакинга в российских социальных сетях и мессенджерах

В данном разделе говорится об обнаружении и идентификации тех или иных публикаций в Интернете или сообщений в мессенджерах, как примеров социального хакинга, рассматриваются примеры рассылок, которые были получены в процессе повседневной жизнедеятельности через «родительские группы» или «группы по интересам» в Сети, без выполнения целенаправленных поисковых действий, выявляя таким образом, подложность информации и определяя цели распространения подобных сообщений.

По цели распространения можно выделить две группы ложных публикаций. Первая группа – это контент, направленный на завладение материальными ценностями в целях мошенничества. Такие сообщения имеют ярко выраженную корыстную цель.

Примерами подобных ложных сообщений являются следующие:

1) через взломанную личную страницу в социальной сети мошенники от имени жертвы рассылают сообщения контактам с просьбой одолжить денег (несмотря на то, что данный способ не является новым, по-прежнему встречаются люди, попадающие в данную ловушку);

2) мошенники распространяют информацию о благотворительных фондах, собирающих средства на социально полезные цели, однако в

платежных реквизитах указывают собственные или подконтрольные счета, не имеющие отношения к благотворительным организациям (общественная опасность данного вида мошенничества выше за счет того, что подрывается доверие в обществе к реальным благотворительным фондам и их мероприятиям);

3) человеку, выставившему частное объявление о продаже каких-либо товаров, приходит сообщение от потенциального покупателя, который желая внести задаток или полностью оплатить товар, просит жертву прислать ему фото банковской карты с обеих ее сторон (на оборотной стороне карты имеется защитный cvc/cvv код, зная который мошенник может получить доступ к управлению средствами на карте).

Характерной чертой писем, рассылаемых в корыстных целях, является либо прямая просьба о переводе денежных средств, либо попытка получить критические сведения о финансовых инструментах жертвы. Универсальной рекомендацией в такой ситуации является проявление бдительности при любых финансовых расчетах и недопущение утечки информации о средствах обеспечения безопасности финансовых инструментов.

Вторая группа ложных информационных сообщений – это сообщения тревожного характера. Так, в мессенджере WhatsApp родительских групп школ и детских садов замечено периодическое появление массовых рассылок ложных сообщений, предупреждающих о какой-либо опасности для детей (рис. 1).

Получая подобные сообщения, родители, желая обезопасить своих детей и окружающих, стараются распространить их, помогая тем самым злоумышленникам. Можно было бы предположить, что создатели таких ложных сообщений преследуют цель научить детей и их родителей бдительности, осторожности, однако этого не подтверждает наличие других ложных сообщений, описывающих либо совершенно нереальные угрозы (например, сообщение о жуке-убийце) (рис. 2), либо об оказании мнимой помощи нуждающимся путем пересылки сообщения (рис. 3) или предоставлении определенных бонусов тем, кто сделает «репост» (рис. 4).

Анализ указанных сообщений показывает, что их авторы с целью распространения подобных ложных сообщений воздействуют на чувства людей: желание помочь, защитить, предупредить и т. п. Однако сами эти сообщения не нацелены на достижение какой-либо позитивной цели.

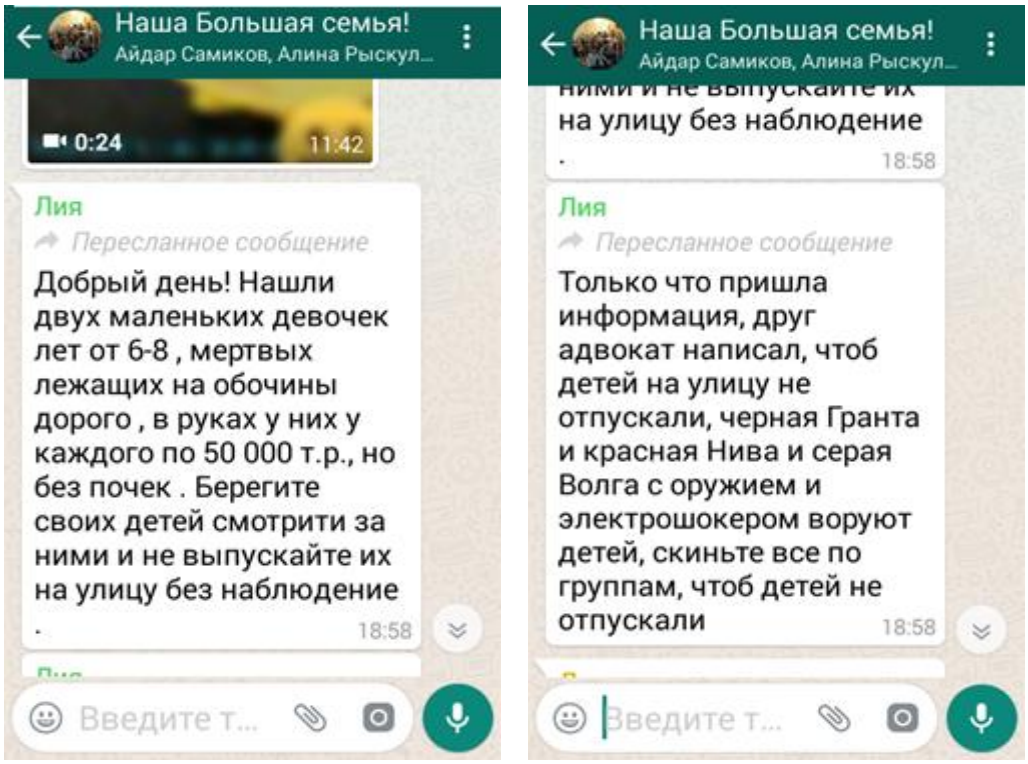

Рис. 1. Примеры ложных сообщений из чатов для родителей в мессенджере WhatsApp

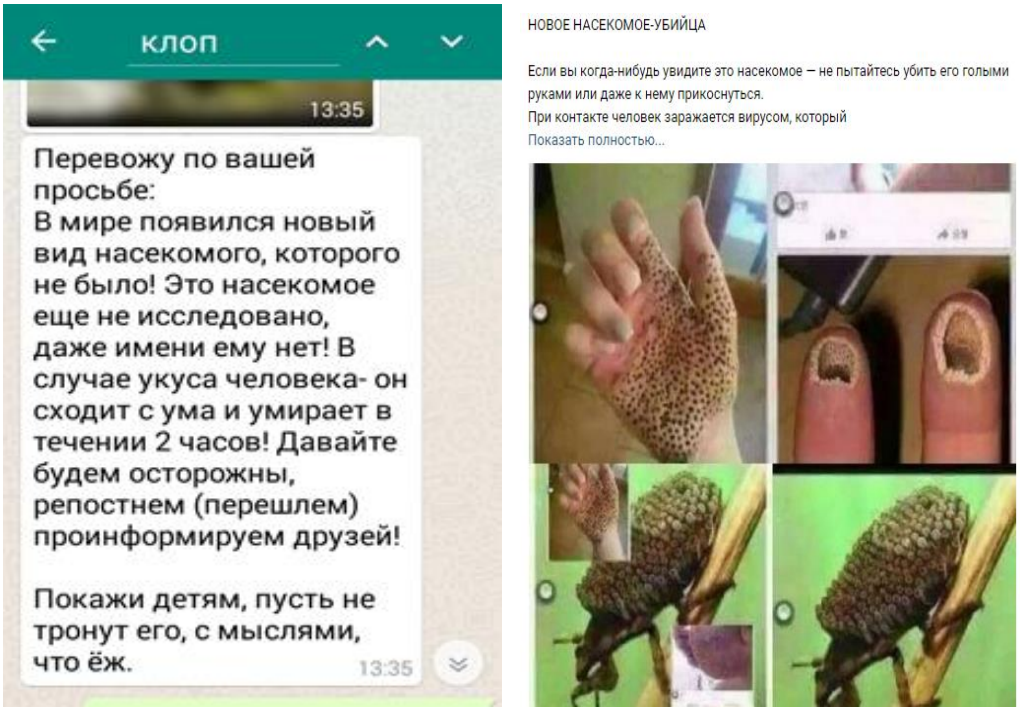

Рис. 2. Ложное сообщение о жуке-убийце, сопровождающееся подборкой ложных фотографий

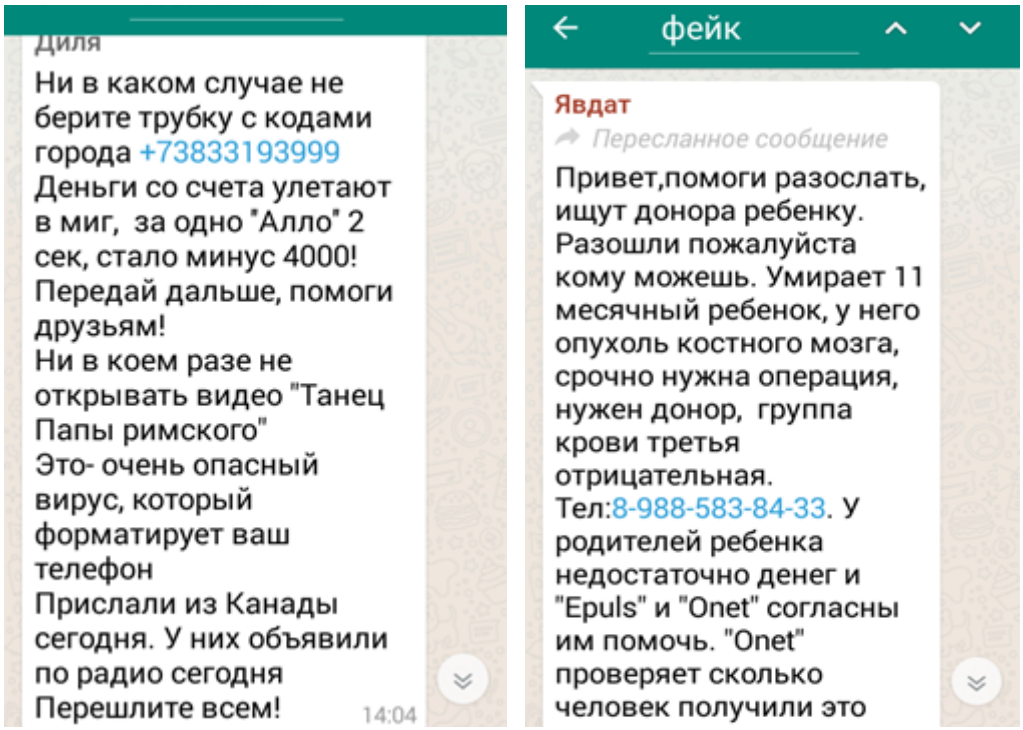

Рис. 3. Примеры ложных сообщений, манипулирующих чувствами людей

Следует отметить, что подобные рассылки не являются подростковой шалостью, как может показаться на первый взгляд (хотя, вероятно, можно встретить и такие). На это указывают следующие особенности.

Во-первых, ряд подобных сообщений помимо текста сопровождается фотографиями, аудио или видео материалами, смонтированными или скомпилированными таким образом, чтобы создавалось впечатление достоверности распространяемой лжи. Такие рассылки сделаны с затратой определенного времени и с использованием технических навыков.

Во-вторых, не смотря на широкий спектр тем, на которые можно найти ложные сообщения, они имеют общие признаки, схожую структуру, что указывает на их подготовку по единым алгоритмам.

В-третьих, при системном рассмотрении вопроса за определенный промежуток времени, можно заметить, что появление подобных сообщений имеет не хаотичный, а периодический характер. Так, например, сообщение о раздающейся детям возле школ жевательной резинке или конфетах с наркотиками периодически появляется в сетях и группах уже около десяти лет. Почти каждый раз текст и прилагаемые к нему фотографии незначительно изменяются. Сообщение редактируется и вновь возвращается в города, где уже появлялось ранее. При этом, как правило, запускаются сразу несколько ложных сообщений одновременно или с незначительным промежутком времени. Известны случаи, когда одному и тому же человеку в течение одного дня приходило три ложных сообщения

на разную тему. Данный факт также указывает на скоординированность действий злоумышленников.

«Terror» в переводе с латинского языка означает «страх», «ужас». Терроризм имеет своей целью воздействие на принятие решений органами власти или организациями, либо месть за их деятельность, основывающееся на распространении чувства страха. Ложные сообщения направлены на внушение страхов и создание тревожной атмосферы в обществе. Кроме того, после очередной волны информационных «вбросов» о наркотиках в конфетах или похитителях детей следом, как правило, приходят ложные сообщения политического и экстремистского характера, либо сообщения, направленные на внушение недоверия к органам власти. Так, например, накануне 2018–2019 учебного года в городе Уфе вновь были разосланы сообщения о распространении наркотиков и оставленных в людных местах иглах с ВИЧ-инфицированной кровью. Следом появилось ложное сообщение о том, что глава Центрального Банка России Э. С. Набиуллина будто сбежала в США. В конце 2018 года после сообщения о потерявшейся возле магазина «Ашан» школьнице пришло сообщение о том, что бывший служащий органов внутренних дел Д. В. Захарченко пояснил на следствии, что найденные у него денежные средства являются выигрышем в казино, и отпущен на свободу.

Таким образом, распространяемые в социальных сетях и мессенджерах ложные сообщения, независимо от конкретного их содержания, являются инструментами информационного давления и создания нестабильной ситуации в обществе. Подобные рассылки воздействуют на людей через эмоции и имеют своей целью внушить определенные чувства, подтолкнуть к совершению определенных действий.

Распространение ложных сообщений может решать несколько задач злоумышленников:

– протестировать уровень информационной культуры людей и выявить их готовность распространять непроверенную информацию;

– сформировать благоприятную атмосферу для последующего распространения ложных сообщений политического и экстремистского характера;

– создать и поддерживать в обществе чувство страха, собственной незащищенности;

– способствовать снижению уровня доверия к институтам власти, обострять противоречия, способствовать возникновению конфликтов в обществе на основе различий в национальности, религии, политических взглядов и т. п.

В связи с тем, что ложные сообщения, как правило, готовятся по определенным алгоритмам, они имеют некоторые схожие признаки, по

наличию которых возможно идентифицировать их и отличить от достоверной информации. Рассмотрим такие признаки-индикаторы подробнее.

1. Отсутствие указания времени и места описываемого события. Цель таких сообщений – распространение в разных городах в течение продолжительного времени. Например, если человек получит сообщение о том, что на автовокзале нашли девочку и ищут ее родителей (рис. 4), но с момента события прошло уже две недели, он вероятнее всего не станет пересылать это сообщение по причине его неактуальности. Если в ложном сообщении и имеется указание на какое-либо место события, то только такое, которое не добавляет конкретики: возле «Ашана», «на улице Ленина», «на автовокзале», «недалеко от музыкальной школы» и т. п. Все перечисленные места и объекты есть во всех крупных городах России. В указанном правиле имеются и исключения. Так, например, в рассылке о том, что группа «Кит» планирует организовать массовое самоубийство подростков, была указана конкретная дата (рис. 5). Возможно, конкретная дата в этом сообщении была внесена одним из родителей до того, как он дальше стал его распространять. Однако благодаря именно этому обстоятельству по прошествии указанной даты дальнейшее распространение ложного сообщения в первоначальной редакции прекратилось.

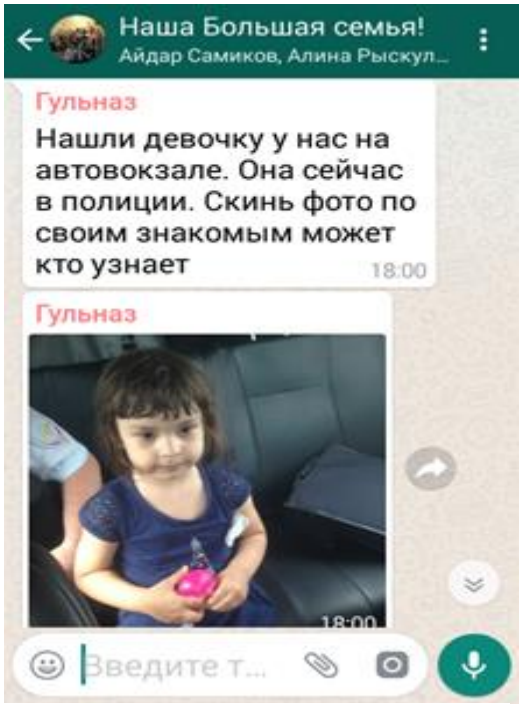

Рис. 4. Сообщение о девочке, которую в течение нескольких лет «находили» в разных городах России

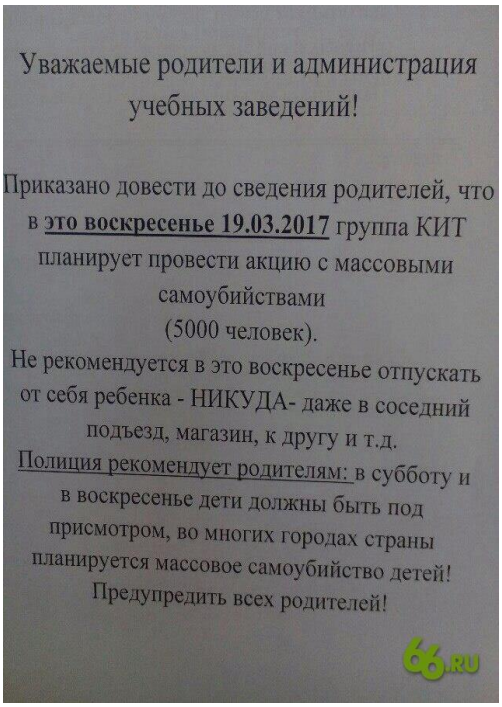

Рис. 5. Объявление о ложном массовом самоубийстве подростков

2. Ложные сообщения для придания вида достоверности часто содержат ссылку на мнимые авторитетные источники информации: «брат в полиции работает», «друг адвокат сообщил», «из управы позвонили» или просто «из достоверных источников» (рис. 6). Злоумышленники редко указывают данные людей, от которых получена информация. В то же время существуют примеры рассылки, в которых указывается конкретное лицо (рис. 7). При этом место работы скорректировано таким образом, чтобы не было привязки к конкретному городу (данный пример содержит признак № 1), ведь Кировские районы, встречаются во многих крупных городах России. В данном случае социальные хакеры указали данные настоящего сотрудника Кировского территориального управления департамента по образованию Администрации города Волгограда. Рассчитывая на то, что люди не станут самостоятельно искать контакты упомянутого в сообщении человека и перепроверять информацию. Ссылка на настоящего человека и его настоящая должность должны были придать достоверности ложному сообщению. Однако представители СМИ и более ответственные в плане информационной культуры родители все же связались с указанным сотрудником, благодаря чему масштабы распространения «фейка» удалось снизить.

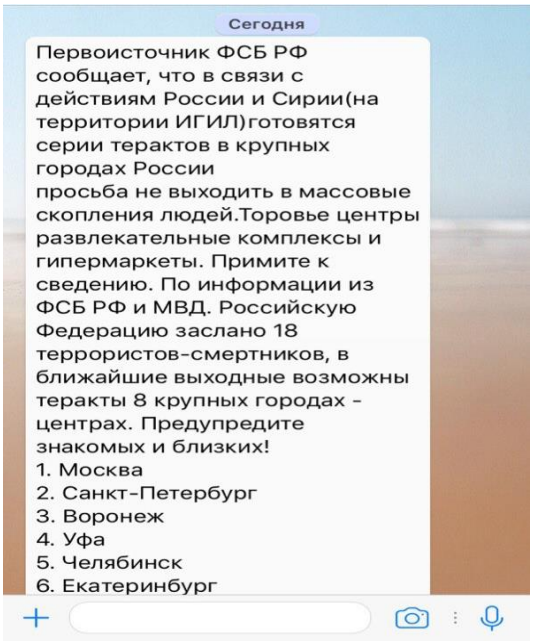

Рис. 6. Ложное сообщение со ссылкой на «достоверный» источник

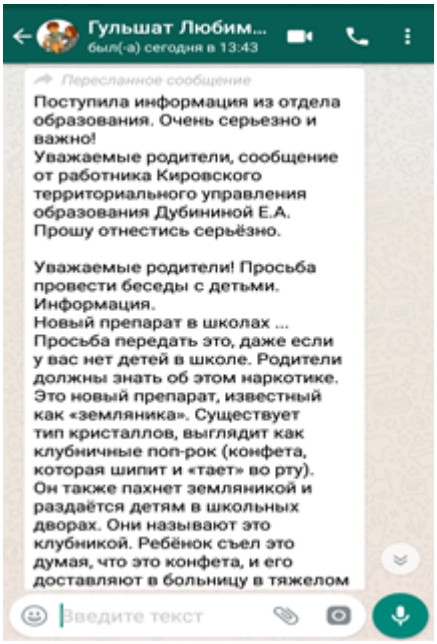

Рис. 7. Ложное сообщение со ссылкой на настоящего человека

3. Поскольку задачей социальных хакеров является воздействие на чувства, эмоции человека, то распространяемые ими сообщения отличаются повышенной эмоциональностью, что подчеркивается использованием эмоционально окрашенных слов («ужасно», «страшно подумать», а также «срочно», «внимание» и т. п.), использованием

заглавных букв, особых шрифтов, смайлов и стикеров, воззванию к благородным чувствам («от нас не убудет…») или страху («ни в коем случае не открывайте…») и т. п. (рис. 8).

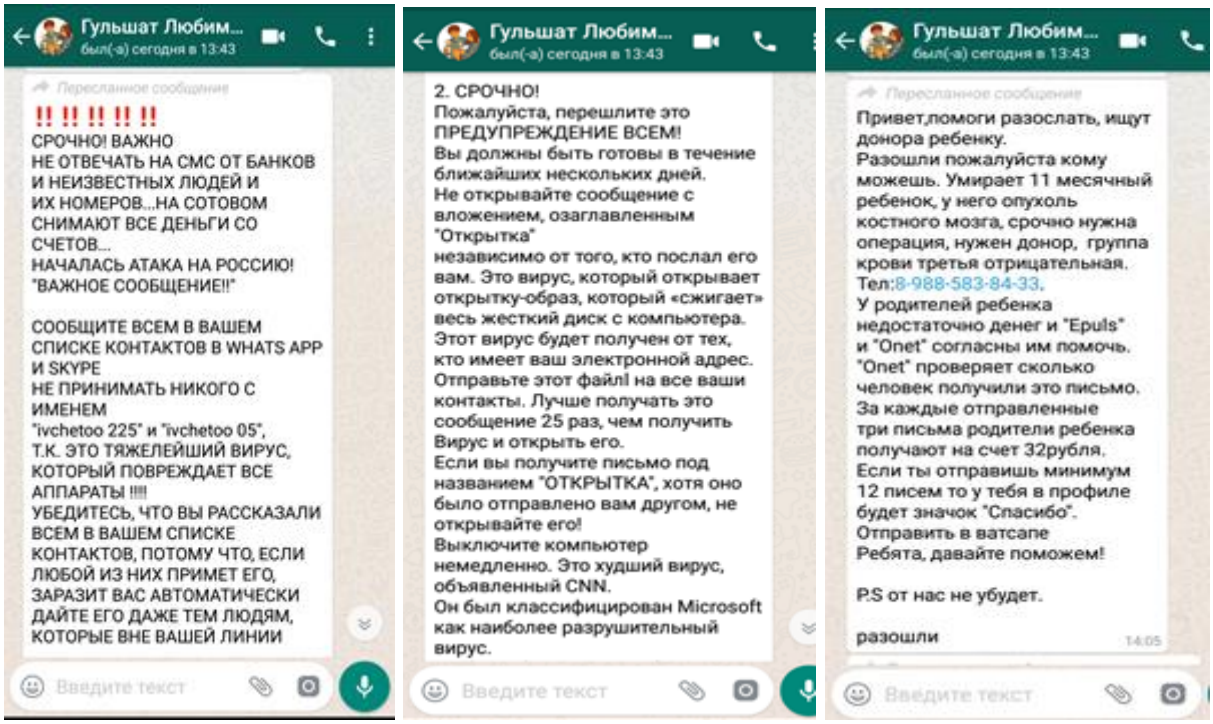

Рис. 8. Примеры эмоционально окрашенных ложных сообщений

4. Обязательным элементом ложного сообщения является призыв распространять его: «разошли всем», «предупреди друзей», максимальный репост» и т. д. Именно в дальнейшем добровольном распространении лжи сотнями и тысячами людей и заключается смысл таких спам-рассылок. И именно в таком распространении заключается слабое место социального хакинга – при ответственном отношении людей к получаемой информации и проверке ее достоверности распространение ложных сообщений потеряет свою эффективность как инструмента информационной войны.

5. При спокойном и внимательном прочтении можно обнаружить и некоторые другие признаки подложности сообщения: явная нереалистичность описываемых событий (например, дезинформация о бегстве Эльвиры Набиуллиной за границу вместе с золотовалютным резервом страны), или несогласованность текста (например, сообщение, которое написано не обычным литературным или разговорным языком, а имеет признаки некачественного перевода на русский язык. Исходя из смысла можно предположить, что автор такого сообщения находится за границей, а описываемое событие не имело место в действительности) (рис. 9).

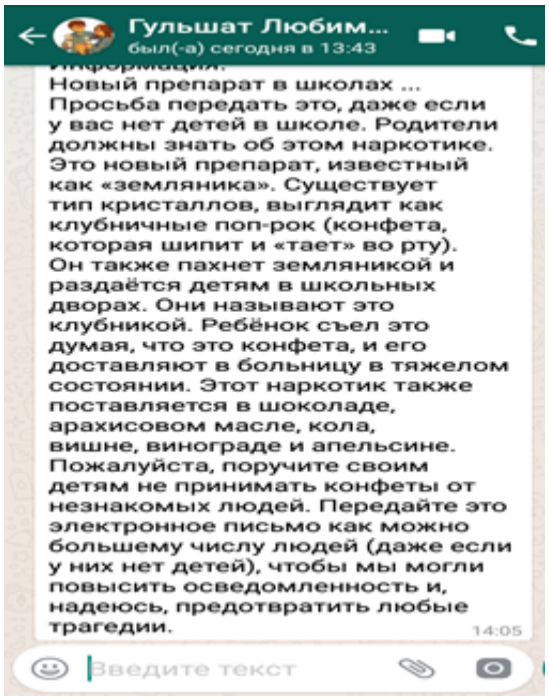

Рис. 9. Пример ложного сообщения, имеющего признаки перевода с иностранного языка

Таким образом, знание характерных особенностей распространения ложных сообщений предоставляет возможность создания надежной защиты, выработки конкретных мер противодействия и устранения условий, благоприятствующих широкому тиражированию ложных публикаций.

Вопросы для проверки знаний

1. Назовите основные методы обнаружения социального хакинга в социальных сетях и мессенджерах.
2. Перечислите цели социального хакинга в социальных сетях и мессенджерах.
3. Назовите основные признаки ложных сообщений.

§ 3. Приемы социальной инженерии, применяемые для дестабилизации гражданского общества и дискредитации правоохранительных органов

Интернет и информационно-коммуникационные технологии выступили орудием и ресурсом, которые позволили значительно усовершенствовать методику и тактику «революций». Посредством информационных технологий организаторы попыток дестабилизации общества осуществляют как воздействия на широкий круг населения, так и пытаются осложнить работу правоохранительных органов. Так, регулярно предпринимаются попытки массового психологического давления на сотрудников полиции, принимающих участие в охране общественного

порядка, организуется их травля, совершаются угрозы, направленные на отказ сотрудников полиции от выполнения своих обязанностей по защите покоя граждан.

Одним из часто применяемых злоумышленниками на несанкционированных массовых мероприятиях методов является провокация насилия и формирование медийной картины применения силы сотрудниками правопорядка, дискредитация образа правоохранителей. На протестных акциях и несанкционированных публичных мероприятиях регулярно совершаются провокации сотрудников правоохранительных органов с целью вызвать их ответную жесткую реакцию. Применяется прием «карусель», когда из-за рядов протестующих, не совершающих активных действий, выбегают отдельные лица, выкрикивают угрозы, оскорбления в адрес сотрудников полиции, толкают их или наносят удары, вызывая ответную реакцию, и скрываются за спины окружающих людей. Под ответные действия сотрудников полиции могут попасть и мирные протестующие. Этот момент снимается на видео, однако в записи демонстрируется только момент ответных действий сотрудника полиции без момента самой провокации. Кадры подобных видео начинают активно тиражироваться в сети Интернет и ангажированных средствах массовой информации (далее – СМИ). Так, военный журналист Семен Пегов, следивший за событиями в Минске летом 2020 года, отмечал: «Из толпы периодически выбегали провокаторы, я их видел. Молодые люди, которые подбегали вплотную к милиционерам, что-то оскорбительное им кричали и убегали. Такая карусель продолжалась»[1]. Аналогичный прием применялся и в нашей стране (рис. 10).

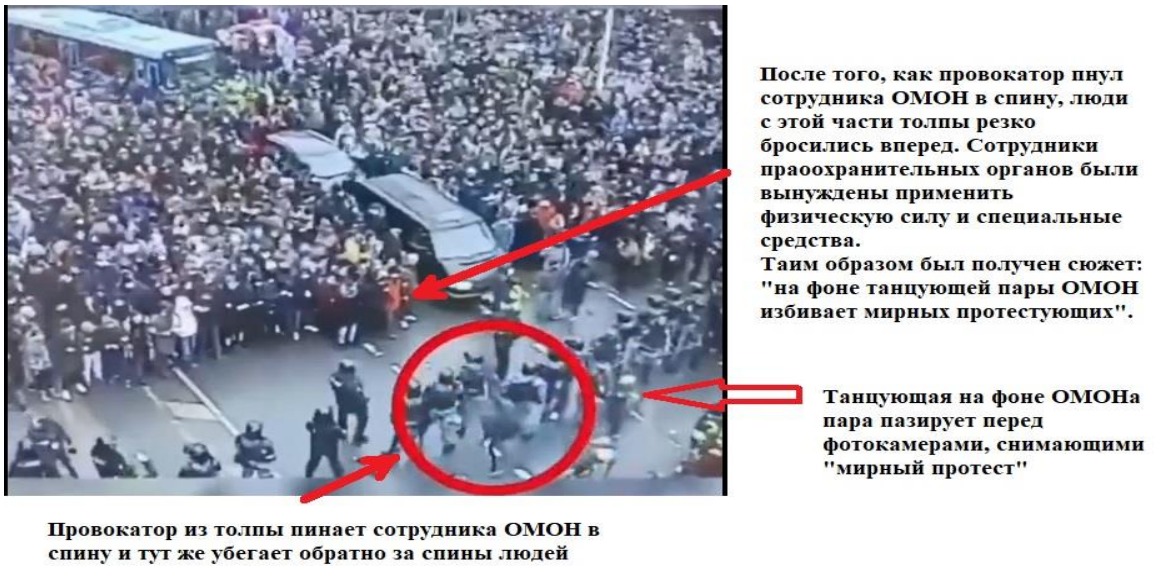

Рис. 10. Схема провокаций на протестной акции 23 января 2021 г.

[1] «Выбегали провокаторы» : Семен Пегов рассказал о протестах в Минске // Звезда. 18 августа 2020 г. URL:https://tvzvezda.ru/news/vstrane_i_mire/content_/20208121738–SkImy.html.

Такие провокации преследуют следующие цели. Во-первых, под воздействием психологии толпы подтолкнуть к агрессивным действиям других людей, которые изначально не планировали совершать насильственные действия. Во-вторых, вызвать у внешних наблюдателей чувство несправедливости. Внушить именно это чувство пытаются организаторы незаконных акций, выставляя в первые ряды протестующих женщин, пожилых людей и даже детей.

Также совершаются и попытки ложного представления незаконности действий сотрудников правоохранительных органов, противопоставление их обществу и призывы к самим сотрудникам «переходить на их сторону». Примером этого является перформанс Ольги Мисик по чтению сотрудникам ОМОНа Конституции Российской Федерации. Участники несанкционированных публичных мероприятий наиболее часто ссылаются на 31 статью Конституции Российской Федерации[1], пытаясь представить ограничения их противоправных действий незаконными, однако, при этом игнорируют положения других статей (в частности, ст. 17, ст. 55).

Другим методом дискредитации сотрудников правоохранительных органов и оказания психологического давления на них являются показательные выбрасывания форменной одежды сотрудниками в отставке различных подразделений полиции, Росгвардии и др. Не исключены единичные увольнения сотрудников правоохранительных органов (при этом такие увольнения вероятно давно планировались по естественным обстоятельствам, однако по случаю проходящих протестов могут быть представлены как выражение политической позиции). Тенденция таких увольнений будет многократно преувеличиваться сторонниками протестов, чтобы подрывать уверенность сотрудников правоохранительных органов в правильности своих действий по защите страны.

Одновременно с описанными выше методами осуществляются попытки манипуляции общественным сознанием в информационно-коммуникационных сетях путем дискредитации как сотрудников правоохранительных органов, так и всех, кто не поддерживает протест. С этой целью в сети Интернет и мессенджерах рассылается ложная информация о пострадавших от действий органов власти (рис. 11). Часто к подобным сообщениям прикреплены постановочные или вовсе не относящиеся к протестным событиям фотографии с изображением травмированных людей (с ложной информацией о том, что к ним применялось незаконное насилие, пытки). К примеру, для дискредитации противников протеста в Республике Беларусь распространялись ложные сведения о том, что за политическую позицию на сторонников протеста

[1] Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Доступ из справочно-правовой системы «КонсультантПлюс».

пытались воздействовать, используя их детей. В России после незаконных митингов 23 и 31 января 2021 года также в популярной в молодежной сети TikTok появилось множество ложных сообщений о гражданах, которым будто были нанесены телесные повреждения или даже причинена смерть[1].


ранениями. По непроверенной информации, вчера карателиубили трёх демонстрантов. Один погиб от наезда автозака, второго до смерти избили сотрудники ОМОНа, а третий скончался от ожогов после взрыва гранаты.

А вот данные некоторых пострадавших:

Валерия Я., 19 лет. Осколочные ранения лица.

Владислав Ч., 25 лет. Ожоги верхних конечностей и живота.

Евгений Ю., 23 года. Огнестрельное проникающее ранение живота. В очень тяжелом состоянии. Выполнена резекция тонкой кишки.

Среди пострадавших также 40-летняя гражданка Нидерландов.

Рис. 11. Сообщения, рассылаемые с целью дискредитации сотрудников правоохранительных органов, имитирующие их несправедливые действия

Деятельность по организации «цветных революций» в информационно-коммуникационной сфере разнообразна и является особенностью попыток дестабилизации гражданского общества. Сферы проявления деструктивного влияния с помощью виртуального пространства только множатся. В связи с широким использованием сети Интернет в данной сфере увеличивается удаленная организация противоправных акций и координация действий рядовых участников протеста через мессенджеры (в том числе из-за границы).

Так, основную организаторскую, координирующую роль протестов в Республике Беларусь в августе-сентябре 2020 года сыграл телеграм-канал Nexta[2]. Призывы к несанкционированным митингам 23 и 31 января 2021 года в России и их координацию Леонид Волков и Иван Жданов

[1] Диванные страдальцы. Откуда появились «жертвы кровавого режима» из «Тиктока» // Life. 25.01.2021. URL: https://life.ru/p/1364482.

[2] Два «нехта» из Польши : как Телеграм–канал Nexta управляет протестами оппозиции в Белоруссии и кто за ним стоит // Информационное агентство «NewsFront». 11.08.2020. URL: https://news–front.info/2020/08/11/dva–nehta–iz–polshi–kak–telegram–kanal–nexta–upravlyaet–protestami–oppoziczii–v–belorussii–i–kto–za–nim–stoit/.

осуществляли, находясь в одной из стран Европы[1].

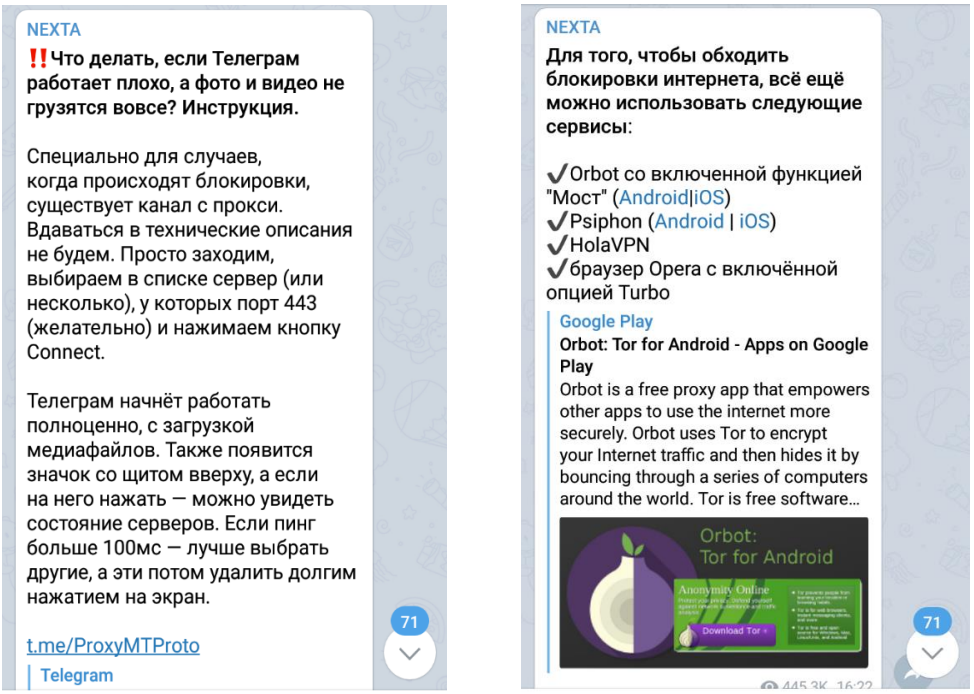

Рис. 12. Инструкции по обходу блокировок сети Интернет

Призванные затруднить такую удаленную координацию ограничение связи и блокировка работы сети Интернет, с одной стороны, создают неудобства для большого количества людей, не участвующих в незаконных акциях и находящихся поблизости с местом их проведения, с другой – не всегда эффективны, поскольку протестующие стараются обойти имеющиеся блокировки различными способами. Так, протестующие распространяют инструкции по скрыванию ip-адресов своих устройств, использованию различных сервисов, позволяющих обходить блокировки, призывают имеющих проводной интернет людей и организации, находящиеся поблизости с местом проведения незаконной акции, раздавать бесплатно WI-FI и т. д. (рис. 12).

Следующим методом дестабилизации ситуации в стране являются хакерские атаки на сайты органов власти для затруднения их деятельности и похищения служебной информации. Помимо затруднения организованной работы сил правоохранительных органов хакерские атаки могут быть нацелены на сайты местных администраций, учреждений, оказывающих государственные услуги населению. Серьезную опасность представляет похищение служебной информации, в том числе персональных данных, которые могут использоваться как для

[1] Бежавшие в Европу Жданов и Волков на стриме координируют митингующих в РФ // Федеральное агентство новостей. 31.01.2021. URL: https://riafan.ru/1378920–bezhavshie–v–evropu–zhdanov–i–volkov–na–strime–koordiniruyut–mitinguyushikh–v–rf.

мошеннических действий, так и для психологического давления на граждан.

Похищенные личные данные впоследствии размещаются на специально создаваемых для этих целей сайтах или группах в социальных сетях. Так, на Украине после государственного переворота 2014 года был создан сайт «Миротворец». В Республике Беларусь личные данные сотрудников правоохранительных органов и не только размещаются в группе «Черная книга Беларуси», созданной в мессенджере Telegram. На таких сайтах и группах размещаются фамилии, адреса, служебные и личные телефоны, ссылки на личные страницы в социальных сетях как самих несогласных с протестующими людей, так и их родственников, фотографии, включая фотографии с родителями, супругами и детьми. Примечательно, что в таких группах размещают данные не только сотрудников правоохранительных органов, но и всех людей, кто не согласен с их позицией: работников администраций, журналистов, представителей бизнеса, не поддержавших протест, блогеров и т. д. (рис. 13, 14).

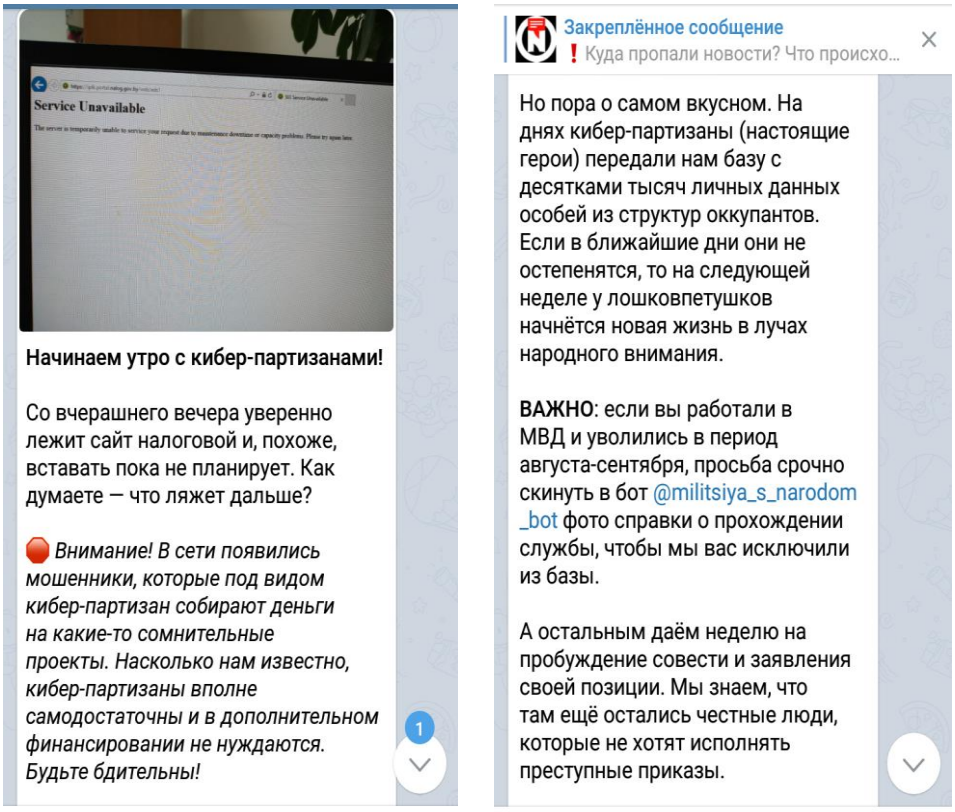

Рис. 13. Примеры кибератак с целью нарушения работы органов и учреждений и похищения служебной информации

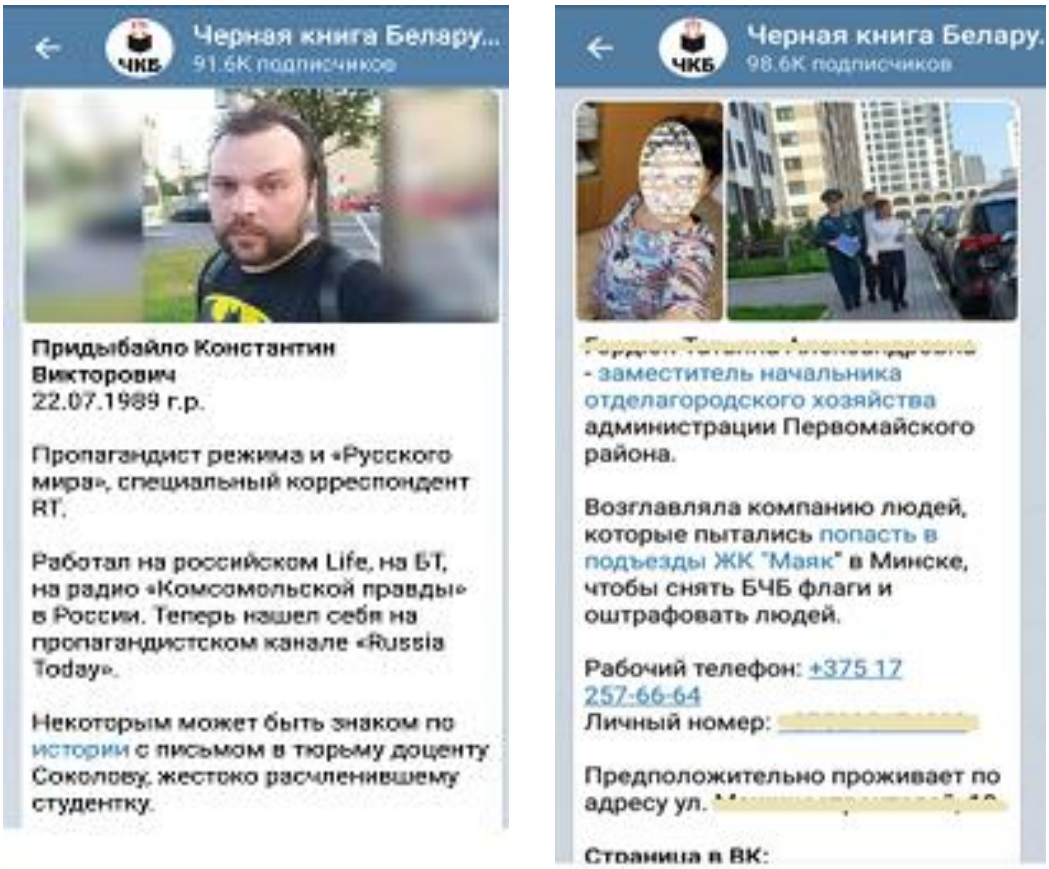

Рис. 14. Личные данные журналиста
и работника местной администрации,
размещенные в группе «Черная книга Беларуси»

Указанная незаконная деятельность опасна тем, что, получив личные данные противников протеста и членов их семей, сторонники протеста оказывают психологическое давление: звонки, сообщения в социальных сетях с оскорблениями, угрозами. При этом травля осуществляется также в отношении членов семей и даже детей, что формирует колоссальное психологическое воздействие, внушая опасение за жизнь и здоровье. В некоторых случаях протестующие переходят к конкретным нападениям, порче имущества (рис. 15, 16).

Так, в России после незаконных акций 23 и 31 января 2021 года дошло до прямых нападений. Двое неизвестных напали с ножом на курсанта Санкт-Петербургского университета МВД России. Девушка не пострадала, поскольку прохожие стали свидетелями нападения. Следственным комитетом России по данному факту возбуждено уголовное дело[1].

[1] В Петербурге угрозы курсантке Университета МВД легли в основу уголовного дела 2 февраля 2021 г. – Происшествия – Новости Санкт-Петербурга – Фонтанка.Ру. URL: https://www.fontanka.ru/2021/02/02/69745127/ (дата обращения: 25.01.2021).

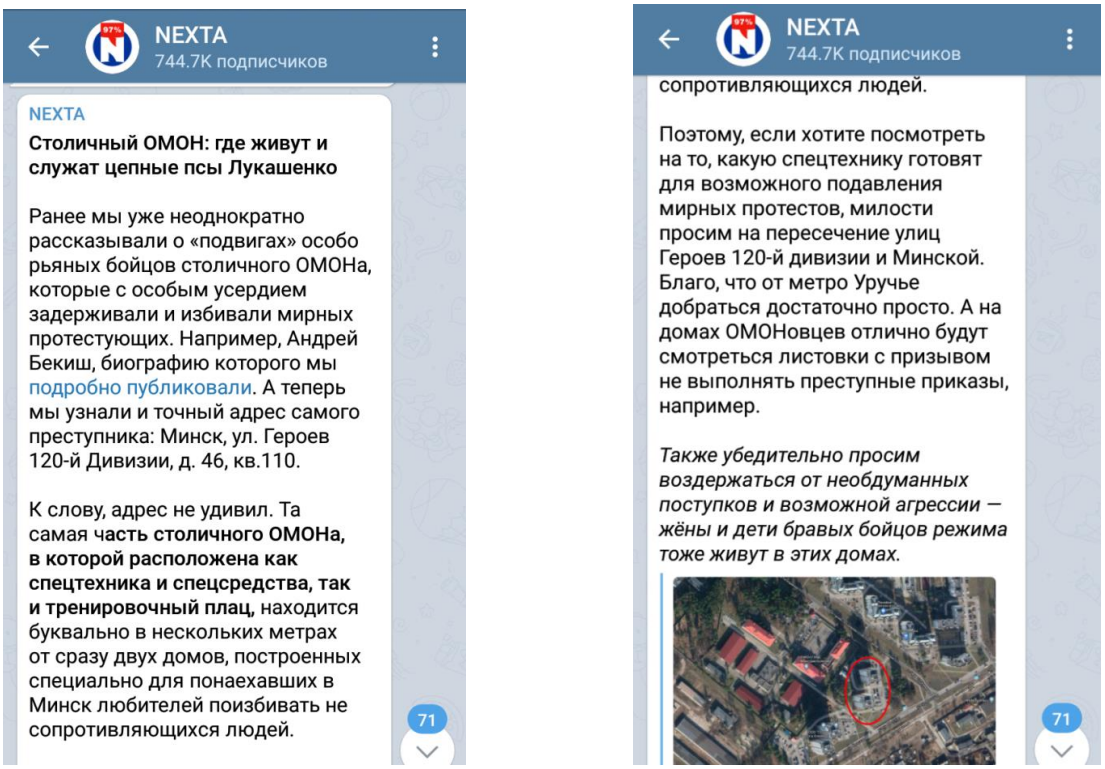

Рис. 15. Призывы посетить место жительства сотрудников ОМОН в период незаконных акций

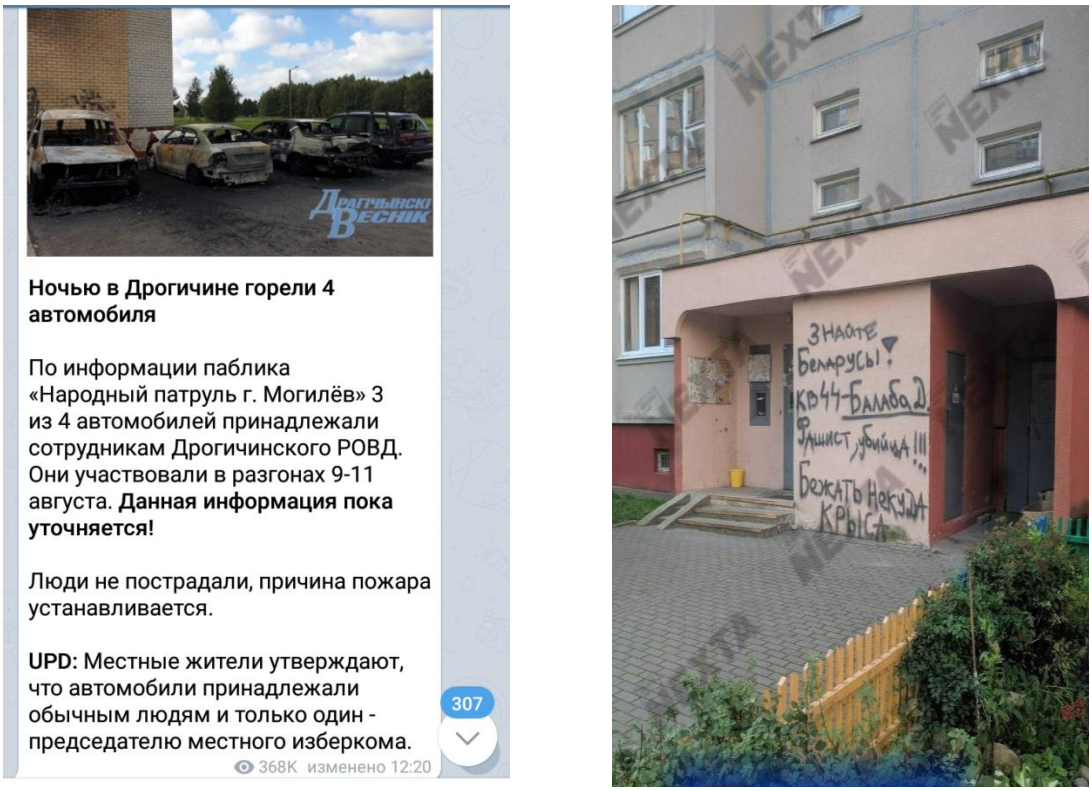

Рис. 16. Сообщение о поджоге автомобиля с фотографией, угрозы и оскорбления на стене подъезда

Наиболее часто нападения происходят на просторах виртуального пространства на тех, кто высказывает точку зрения, не совпадающую с протестующими. Протестное меньшинство в сети Интернет ведет себя очень агрессивно. Под новостными публикациями оставляется большое количество комментариев в поддержку протеста и против действия властей. На любые альтернативные комментарии тут же реагируют оскорблениями и сообщениями манипуляционного характера, приводимые такими комментаторами аргументы содержат большой объем ложной информации, а также описаний повседневной жизни крайне негативного окраса (к примеру, формулировки: «никогда так плохо не было», «хуже уже некуда», «в стране полный упадок» и т. п.), приводятся обобщения («весь народ против власти», «все знают, что ничего хорошего не делается» и т. п.). При этом задача организаторов протестных акций состоит в создании условий невозможности высказывать контраргументы и демонстрировать наличие альтернативных мнений. В связи с этим на тех, кто проявляет активность в сети Интернет на противоположной стороне, отправляют жалобы, их аккаунты стараются заблокировать (рис. 17). Данные действия совершаются с целью манипулирования сознанием людей, формирования иллюзии того, что сторонники протестных акций составляют большинство в обществе, что не соответствует действительности.

Формируемые таким образом в социальных сетях и мессенджерах настроения активно стараются поддержать и развить в зарубежных и ангажированных местных СМИ. Следует отметить, что стандарты журналистской этики, требующие непредвзятого освещения событий, в настоящее время не соблюдаются. Одни и те же события в разных СМИ имеют совершенно противоположный смысл, информация представляется заинтересовано. В случае реализации попыток дестабилизации общества организуются агрессивные информационные атаки. К таким атакам подключаются сервисы YouTube, Facebook и Twitter, где активно продвигаются новостные публикации и иной контент, способствующий разрастанию протестных настроений, и блокируется контент противоположного содержания и характера.

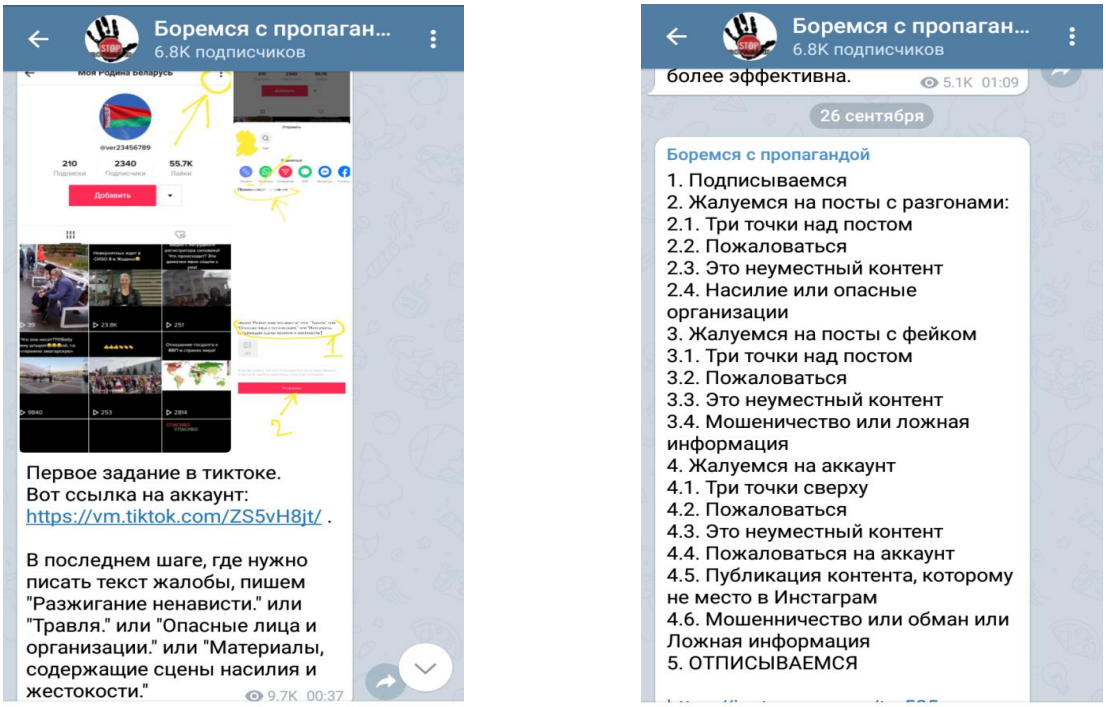

Рис. 17. Распространяемая инструкция для протестующих о том, как массово блокировать сторонников альтернативных мнений

Вопросы для проверки знаний

1. Перечислите основные приемы социальной инженерии.
2. В каких целях социальные инженеры получают личные данные?
3. Как можно бороться в социальных сетях и мессенджерах с дискредитацией правоохранительных органов?

§ 4. Интернет-пространство как среда для распространения идей экстремизма и терроризма

Проблема, связанная с распространением и развитием терроризма в сети Интернет, согласно отчетам We Are Social и Hootsuite о глобальном состоянии цифровых технологий на 2019 год, в настоящее время приобретает большие обороты (в течение дня с января 2018 года около одного миллиона человек открывали для себя пространство сети Интернет, а это около 11 человек в секунду)[1]. Аудитория сети Интернет увеличивается с каждой секундой, в связи с этим терроризм, тактика терроризма подверглись изменениям: затяжные войны и открытые столкновения в настоящее время не представляют интерес для террористов. Происходит трансформация терроризма, так как времена тайных встреч ушли в прошлое, сейчас вербовка происходит открыто в социальных сетях.

[1] Digital 2019 : Глобальное использование интернета. URL: https://wearesocial.com/blog/ 2019-global-internet-use-accelerates (дата обращения: 20.03.2021).

На сегодняшний день в связи с расширением аудитории сети Интернет повышается роль Всемирной паутины в жизни человека и общества. Вследствие широкого распространения социальных сетей и мессенджеров эти средства позитивной коммуникации между людьми становятся мощным оружием, которым могут воспользоваться также террористические организации.

Нет единого мнения о том, как определять понятие «терроризм», так как многие авторы не приводят различий между такими смежными понятиями, как «террор», «терроризм», «террористический акт» и другими схожими категориями, что значительно осложняет выработку единообразного подхода к пониманию проблем терроризма.

По мнению В. П. Емельянова, террор – это деятельность государственной власти в различные периоды существования государства. Однако и негосударственные террористические структуры могут насаждать повсеместный террор, внушая страх и ужас по всему миру. Автор выделяет государственный и негосударственный терроризм, который олицетворяет собой акции массового насилия над находящимся в их поле деятельности контингентом[1]. Как отмечает А. И. Моисеенко, терроризм – не уголовно-правовое понятие, а социально-политическое явление, включающее в себя террористически направленную идеологию, организационную структуру и практическую террористическую деятельность[2].

Терроризму, как уголовно-правовому явлению, свойственны следующие отличительные признаки:

1) публичный и демонстративный характер терроризма;

2) терроризм создает и поддерживает обстановку паники, подавленности, страха и парализует социально полезную деятельность населения, нормальное функционирование органов власти и управления, а также общественных формирований и объединений;

3) создается общая опасность, заключающаяся в гибели людей или наступлении иных общественно опасных последствий;

4) психологическое воздействие играет большую роль, так как насилие и жестокость, вызывающие в обществе страх, вынуждают людей действовать непосредственно.

В настоящем учебно-практическом пособии терроризм определяется как идеологически обоснованное систематическое насилие в отношении граждан для выполнения социально-политических условий.

Таким образом, терроризм определяется, во-первых, как идеологически обоснованное насилие; во-вторых, как периодическое, т. е.

---

[1] Емельянов В. П. Терроризм и преступление с признаками терроризирования. СПб, 2010. С.17.

[2] Моисеенко А. И. Уголовно-правовая и криминологическая характеристика терроризма (по материалам Южного федерального округа России) : дис. … канд. юрид. наук. Ставрополь, 2006. С. 9.

систематическое насилие; в-третьих терроризм априори имеет политический характер.

Интернет на сегодняшний день является идеальной средой для пропаганды террористической и экстремистской деятельности по нескольким основным причинам:

1) возможность оставаться анонимным;
2) высокая скорость распространения информации;
3) возможность без значительных затрат создавать собственные пропагандистские Интернет-ресурсы;
4) использование неточностей, неоднозначных формулировок в закрытых актах, касающихся проблем несогласованности в законодательствах стран в сфере информационной безопасности;
5) шифрование сообщений и материалов.

Согласно данным «Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет»[1] за 2019 год, наблюдаются следующие тенденции в интернет пространстве:

1. Аудитория русскоязычного сегмента сети Интернет увеличивается. Так, в 2011 году количество интернет-пользователей составляло 49 % от населения России, а в 2019 году их количество увеличилось до 76%.

2. Рост преступлений экстремистской направленности связан с усилением деятельности террористических организаций в информационной среде. Вербовка проходит через популярные мессенджеры.

В 2018 году Американское издание The Wall Street Journal разместило список мобильных приложений и мессенджеров для общения, отсортированных по степени их шифрования и безопасности передачи информации. Некоторые из них признаны хорошо защищенными от перехвата спецслужбами, что создает благоприятные условия для сторонников терроризма координировать свои действия и передавать информацию. Безопасными приложениями для шифрованной связи были названы Telegram, SilentCircle и Signal. Популярные приложения WhatsApp, Viber или WeChat считаются небезопасными по передаче информации абонентами[2].

Предположительно лица, причастные к террористической деятельности, используют шифрование – преобразование текста для

---

[1] Обзор информационного центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет. URL: https://ncpti.su/ (дата обращения: 15.03.2021).

[2] Шифровка для террориста : одобренные приложения для защищенности связи и новый раунд дебатов о безопасности. URL: https://www/wsj.com/ (дата обращения: 19.03.2021).

обеспечения секретности передаваемой информации таким образом, при котором только авторизованные стороны могут получить к нему доступ для связи.

Процесс радикализации, в результате которого человек приходит к пропаганде терроризма и экстремистской идеологии, не является статичным, он развивается со временем, поэтому процесс формирования террориста – не просто крайняя форма религиозных убеждений, но и полная смена сознания человека, его ценностных ориентаций и убеждений, в результате которых первоочередное значение играет влияние окружающего общества.

Пространство Сети сегодня расценивается как новый вид инструмента террористов для достижения своих целей. Экстремистов воспитывают не в подпольных лагерях и конспиративных квартирах, а через сознание будущих террористов, проникая через компьютеры и смартфоны. Именно с помощью мессенджеров вербовщики дают указания о том, где провести террористический акт, как собрать взрывное устройство. Так происходит интеграция идей в приложения. Людей, которых планируют завербовать, находят при помощи своих специальных сайтов: собирается информация о пользователях, которые заинтересованы в деятельности организации, после чего они добавляются под каким-либо предлогом в список контактов в социальной сети, начинается безобидное бытовое общение, постепенное склонение сначала к одобрению террористической деятельности, а затем переход в закрытые группы с высокой степенью криптозащиты, где непосредственно происходит вербовка. Следует отметить, что так работает не один террорист-вербовщик, а целая информационно-пропагандистская сеть профессиональных психологов с использованием методов психологического воздействия. Материалы, используемые в качестве пропаганды и оправдания терроризма, подменяют понятия и создают образ позитивного экстремизма.

Сайты и платформы, пропагандирующие и распространяющие в сети Интернет материалы, которые способствуют развитию экстремизма и терроризма, можно разделить на следующие группы:

1) непосредственно распространяющие идеи терроризма и экстремизма;

2) информационные ресурсы, через которые происходит финансовая поддержка террористических организаций;

3) сайты, содержащие контент, направленный на разжигание ненависти на основе расовой или национальной принадлежности.

На данных террористических сайтах можно найти подробную информацию о том, как в кустарных условиях изготовить химические соединения, обладающие высокой токсичностью, как собрать самодельное взрывное устройство из бытовых предметов, даются рекомендации по тактике проведения террористических акций, по вербовке новых членов

преступных организаций. Интернет-сайты, относящиеся к этой группе, могут быть расположены в любой точке сети, так как содержащаяся в них информация представляется как справочная. Такие сайты многочисленны и недолговечны, так как доменные имена часто изменяются.

Проблема обнаружения и ликвидации сетевых центров (серверов, доменов, веб-сайтов) является главной причиной использования террористами Интернет-технологий. Используются особенности технической организации Интернета, позволяющие создавать доменные имена сайта в одной стране, а размещать информацию в другой. При этом доступ к нему может быть обеспечен практически из любой точки мира, имеющей подключение к сети, данное обстоятельство позволяет членам преступных организаций создавать закрытые каналы для передачи информации.

В настоящее время в таких социальных сетях, как Facebook и Twitter, отсутствуют данные категории разграничения информации, чтобы отмечать или сообщать о террористическом контенте на своих платформах. На видеохостинговом сайте YouTube можно пометить только одну категорию. Например, видео может быть отмечено как: «насильственное или отвратительное», «пропаганда терроризма» и «ненавистный или оскорбительный контент». Это, в свою очередь, требует незамедлительного разрешения в целях недопущения развития терроризма в сети Интернет.

Рекомендации по пресечению деятельности террористических организаций через сеть Интернет

1. Создание определенных групп, систем упорядоченности и автоматизации информации глобальными информационными и технологическими компаниями. Этот способ позволил бы автоматически генерировать такие категории распространения информации, как «экстремизм» или «терроризм» в рамках своих существующих систем отчетности, что дало бы возможность пользователям сообщать о подобных материалах.

2. Создание более совершенного и более последовательного процесса подачи апелляций и механизма обратной связи. Пользователи должны иметь возможность непосредственного взаимодействия с лицами, представляющими технологические компании и принимающими решения в области размещения, распространения информации на данном ресурсе. Эти решения должны быть подробно, отчетливо и объективно обоснованы, с уточнением причины получения доступа или его отсутствия на размещение.

3. Обеспечение пользователей сети Интернет своевременной помощью и поддержкой, в случае распространения и пропаганды террористического или экстремистского контента на определенные группы

людей (консультация, онлайн-беседа, введение возрастных ограничений, возможность ограничения просмотра и комментирования). Американская транснациональная публичная корпорация Google является лидером в этом направлении, применяя метод «перенаправления» и предоставляя различные ограничения для пользователей в отношении определенного контента, включая контент с ограничением по возрасту, где удаляются комментарии или предлагаемые видео[1].

В настоящий момент при нынешнем развитии технологий и методов передачи информации в сети Интернет возникает необходимость в превентивной антиэкстремистской работе, которая позволила бы оперативно воздействовать на каналы распространения такой информации и нивелировать его эффект. Использование технологий сетевого маркетинга (Social Media Marketing – SMM) позволит расширить аудиторию охвата и увеличит уровень лояльности к данному контенту. Таким образом, осознав сущность развития данной проблемы, вовлекая определенные службы и совершенствуя системы, возможно более эффективно выявлять экстремистский и террористический контент и препятствовать его распространению. С этой целью возможно привлечение к антиэкстремистской работе популярных в сети Интернет блогеров и известных личностей, которые могли бы проводить информирование пользователей сети Интернет об опасности терроризма, тем самым формируя антитеррористическое сознание у населения нашей страны.

Вопросы для проверки знаний

1. Какие отличительные признаки свойственны терроризму как уголовно-правовому явлению?
2. Назовите причины, по которым Интернет стал средой для пропаганды террористической и экстремистской деятельности.
3. Выделите группы, распространяющие идеи терроризма и экстремизма в Интернете.

[1] Муртазин А. И., Давлетов В. И. Интернет-пространство как среда для распространения идей экстремизма и терроризма // Актуальные проблемы государства и общества в области обеспечения прав и свобод человека и гражданина. 2020. С. 73.

ГЛАВА 2. НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ ДЕСТРУКТИВНОЙ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

§ 1. Пути противодействия деструктивному социальному хакингу в социальных сетях и мессенджерах

Публичное распространение ложной информации известно с давних пор. Так, по одной из версий устоявшееся международное выражение «газетная утка», обозначающее недостоверные сведения, берет свое начало с XVIII века, когда в только набирающих широкое распространение периодических печатных изданиях подозрительные статьи помечались буквами «NT» – «non testatum», что в переводе с латинского означает «не проверено»[1]. Указанная аббревиатура по звучанию схожа с немецким словом «ente» – «утка», в связи с чем сенсационные, но ложные сообщения, в обществе и стали называть коротко – «утка».

Рассматриваемое деструктивное явление известно уже несколько столетий. И уже в тот период люди с большей или меньшей эффективностью научились выявлять и давать оценку ложной информации. Но если тогда создание «газетных уток» делалось в погоне за сенсацией или, возможно, герастратовой славой, либо просто из шалости, то сегодня в век информационных и цифровых технологий дезинформация стала мощным оружием в информационных войнах.

Определение «non testatum» раскрывает суть ложных сообщений и указывает на основной способ противодействия им. Любая информация должна тщательно проверяться. Первичная проверка начинается с ее восприятия, анализа, оценки по наличию имеющихся в ней индикаторов (приведенных в пример ранее). Процесс вдумчивого критичного прочтения полученного сообщения может определить степень ее достоверности.

Наличие в сообщении приведенных ранее индикаторов, однако, не указывает однозначно на этот факт, свидетельствует о высокой вероятности его ложности. Для более тщательной проверки сообщения есть простой способ, многократно описанный на сайтах гражданских активистов «Лиги безопасного интернета» или «Молодежной службы безопасности»: необходимо в поисковой строке любого браузера напечатать какую-либо короткую фразу в точном соответствии с проверяемым сообщением[2]. Эффективнее этого выбирать фразу, где содержатся ключевые или особенные слова. Так, например, при проверке

---

[1] См. : Non testatum, или от куда в медийный поток прилетают «утки» // Гродзенская правда. 11.04.2018. URL: grodnontws.by/category/zhizn/news42434.html (дата обращения: 11.02.2021).

[2] См. : URL: http://molbez.ru/anti-fakes/history24.html (дата обращения: 11.02.2021).

сообщения о конфетах с наркотиками, оказалось достаточным напечатать в поисковой строке название конфет «Поп-рок», чтобы убедиться в его ложности, так как в нашей стране подобное название реальных конфет не встречается.

Как правило, при проверке сообщений, в достоверности которых возникли сомнения, имеются индикаторы их подложности. По результатам поискового запроса можно убедиться в пересылке такого же сообщения в разных городах и в разное время или в наличии статьи, прямо указывающей на то, что данная рассылка является очередным «фейком».

В случае, если ложное сообщение новое и в результатах поискового запроса не определяется, следует понять его смысл и оценить реалистичность описываемых событий. Например, если в тексте упоминается какой-либо магазин, улица или иной объект, можно проверить по картам города, имеется ли таковой в вашем городе.

После трагедии в торговом центре «Зимняя Вишня» в городе Кемерово и распространения ложного сообщения о более трехстах погибших и сокрытии властями реального количества жертв, достаточно было задаться вопросом о том, какой смысл в подобных манипуляциях, если реальное и объявленное количество жертв и так было значительным. В действительности, если бы такое уменьшение количества жертв имело бы место быть, родственники погибших (пропавших) людей своевременно опровергнули бы официально озвученные данные.

Если поступившее сообщение, которое необходимо проверить, касается криминальных событий, то для ее достоверности необходимо обратиться в органы внутренних дел РФ. Именно так должны поступать в том числе и средства массовой информации, прежде чем опубликовать информацию на своих ресурсах.

Алгоритм проверки информации и идентификации ложных сообщений прост. Однако проблема заключается в низкой информационной культуре в обществе, отсутствии критического мышления. До сих пор отсутствует ответственное отношение к информации и понимание высокой общественной опасности, которую представляют социальные хакеры.

В связи с этим одним из действенных мер защиты от социального хакинга является повышение информационной культуры и грамотности населения, обучение граждан выявлению (идентификации) ложных сообщений, их проверке. Это позволит создать надежный барьер на пути их распространения.

Одним из способов повышения информационной культуры и грамотности населения является проведение выступлений в школах, вузах, трудовых коллективах. Так, перед школьниками старших классов одной из общеобразовательных школ было проведено информационное выступление сотрудниками органов внутренних дел, в результате чего выяснилось, что все дети сталкивались с подобными ложными

сообщениями и пересылали их. Однако около половины из них только на лекции узнали, что эти сообщения были ложными. Школьники удивлялись широкой распространенности «фейков» в социальных сетях и мессенджерах и тому, как простая пересылка сообщения из благих побуждений может причинить существенный вред, если это сообщение было ложным. Прямо на лекции школьники проверяли отдельные сообщения по ключевым словам в поисковых сервисах и выявляли в них индикаторы, удивляясь тому, как просто не дать обмануть себя. Проведенное мероприятие показало востребованность таких лекций. Их эффективность заключается в адресном и ёмком обучающем воздействии на подрастающее поколение – самых активных пользователей социальных сетей.

В то же время данный способ имеет существенный недостаток, заключающийся в ограниченности своего применения. В связи с этим обучающее воздействие должно проводиться также посредством распространения в СМИ и сети Интернет памяток по проверке и выявлению ложных информационных сообщений.

Следующим приемом повышения информационной культуры является включение в этот процесс тех людей, которые способны не поддаваться воздействиям социальных хакеров. То есть противодействие распространению ложных сообщений должно использовать те же сетевые алгоритмы, что и само распространение. Это станет возможным, когда более ответственные по отношению к информации граждане, научившись проверять достоверность сведений, не только сами не будут участвовать в распространении «фейков», но и будут объяснять участникам чатов, групп в сетях и мессенджерах, как отличить ложь от правды. Такое обучающее воздействие возможно различными способами, с разной степенью эффективности влияющими на различных людей. Так, одним нужно будет давать подробную инструкцию по идентификации ложных сообщений, другим будет достаточно отправить шуточную картинку-баннер или демотиватор, демонстрирующие недопустимость беспечного отношения к информации.

Зная, что сообщение имеет ложный характер, необходимо:

1) задать ее автору несколько вопросов, например: «Информация проверена?», «Вы проверили достоверность этих сведений?»;

2) разослать инструкцию по проверке пересылаемых сообщений;

3) найти и отправить опровержение сообщения и прикрепить ссылку на материал, подтверждающий ее недостоверность.

Для активного подключения сознательных и активных граждан к процессу повышения информационной культуры в обществе предлагаем «вооружить» их баннерами и демотиваторами, содержащими емкие высказывания, указывающие на необходимость ответственного отношения к информации и т. п. Такие баннеры и демотиваторы могут быть

размещены в социальных сетях и мессенджерах в ответ на очередное ложное сообщение социальных хакеров (рис. 18).

Рис. 18. Примеры простых баннеров и демотиваторов для ответов на ложные сообщения в социальных сетях и мессенджерах

Следующим способом развития у людей ответственного отношения к информации является установление юридической ответственности за публичное распространение ложных сообщений. Так, статья 274 Уголовного кодекса Республики Казахстан предусматривает уголовную ответственность для лиц, публично распространяющих заведомо ложные сведения[1].

Для устранения условий по возникновению социального хакинга сотрудникам органов внутренних дел предлагается (к примеру, участковым уполномоченным полиции) самим использовать социальные сети или мессенджеры для взаимодействия с населением. Это, с одной стороны, предоставит гражданам достоверный источник информации, который затруднит бесконтрольное распространение ложных сообщений, с другой – предоставит сотрудникам органов внутренних дел источник получения и распространения информации, что повысит эффективность и оперативность их работы.

Рассмотрим пример пересылаемого в нескольких городах России сообщения о банде педофилов (рис. 19). При наличии предложенной группы в мессенджерах под администрированием участкового уполномоченного полиции, гражданин, получивший такое ложное сообщение вместо его дальнейшего распространения сможет уточнить информацию у сотрудника полиции, получит опровержение, которое

[1] Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V ЗРК // Статья 274. Распространение заведомо ложно й информации. URL: https://kodeksy-kz.com/ka/ugolovnyj_kodeks/274.htm (дата обращения: 12.04.2021).

увидят все участники группы, а значит пересылка «фейка» тут же прекратится.

Рис. 19. Ложное сообщение о розыске банды педофилов

При этом в указанных группах со стороны органов внутренних дел должна распространяться информация, предназначенная только для открытого опубликования. Так, например, с целью взаимодействия с обществом Министерством внутренних дел Российской Федерации создана группа в социальной сети ВКонтакте. В плане противодействия социальному хакингу этот положительный опыт целесообразно развить. Это будет являться дополнительным преимуществом, способствующим установлению тесного взаимодействия между обществом и сотрудниками полиции и повышению доверия к органам внутренних дел. Указанные группы в мессенджерах будет удобно использовать для обнаружения реально разыскиваемых лиц.

Следует отметить, что согласно прогнозу проекта «Время Вперед» в 2019 году против России будут применяться самые передовые информационные технологии – новые «фабрики троллей», «видеофейки»[1]. Так в опубликованном видео отмечается, что «главным трендом станет появление так называемых deep fakes, или глубоких фейков, созданных с помощью искусственного интеллекта. Такой контент будет невозможно оперативно разоблачить, что является серьезной опасностью. Прежде всего, речь о фейковых видео, созданных по технологии face to face. То есть по технологии, позволяющей создать фальшивое видео с речью любого человека, например видного политика».

Учитывая сказанное, а также имея информацию о том, что Госдепартамент США в 2019 году выделял гранты для «содействия укреплению принципов журналистской этики в России»[2] и о том, что на

[1] Готовится новый инфоудар по России – YouTube. URL: https://youtu.be/tC9pn0hCwMU/ (дата обращения: 23.01.2021).

[2] В США намерены содействовать «укреплению принципов журналистской этики» в России — РТ на русском. URL: https://russian.rt.com/world/news/579442-ssha-rossiya-zhurnalistika-grant/ (дата обращения: 23.01.2021).

территории Украины действует британское спецподразделение – 77 бригада, выполняющая военные задачи в Интернете, оказывающая психологическое воздействие и проводящая информационные операции[1], к вопросам противодействия социальному хакингу и другим информационным угрозам необходимо подойти комплексно и системно, активно привлекая к этому все слои населения и, в первую очередь, молодежь. Иначе ущерб от возможных информационных атак может дойти до критических показателей. Ведь по мнению активистов проекта «Время Вперед», сегодня мы еще так и не нашли противоядие даже против самых примитивных методов дезинформации[2].

Вопросы для проверки знаний

1. Что означает «non testatum»?
2. Назовите алгоритм проверки сообщения на его подлинность.

§ 2. Актуальные направления предупреждения мошенничеств в социальных сетях и мессенджерах

Стремление людей быстро заработать выступает сильным фактором совершения различного рода мошенничеств. С одной стороны, это стремление является характеристикой личности мошенника, готового пойти на обман ради получения материальной выгоды, с другой – виктимологическим фактором, облегчающим совершение преступления в связи с использованием желания жертвы извлечь выгоду. По данным ГИАЦ МВД России в 2019 году в Российской Федерации было совершено 257 187 преступлений, предусмотренных статьями 159–159.6 Уголовного кодекса Российской Федерации (далее – УК РФ), что почти на 20 % больше, чем в 2018 году. Доля мошенничества в общей структуре преступности составила 12,7 %. Часто мошенники для достижения своих корыстных целей используют компьютерную технику, различные средства и инструменты коммуникации. Так, в 2019 году из 294 409 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, 46,4 % (136 709 преступлений) приходится на долю различных видов мошенничества (ст. 159 УК РФ «Мошенничество» – 119 903 преступления; ст. 159.3 УК РФ «Мошенничество с использованием платежных карт» – 16 119

[1] Самая страшная беда, чем занимаются сотрудники Британской разведки в Украине. URL: https://ruafan.ru/1128331-publichnost-samaya-strashnaya-beda-chem-zanimayutsya-sotrudniki-britanskoi-fabriki-trollei-na-ukraine/ (дата обращения: 25.01.2021).

[2] Как не стать жертвой в эпоху инфомрака. URL: https://время-вперед.рус/post/как не стать жертвой в эпоху инфомрака (дата обращения: 17.02.2021).

преступлений; ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации» – 687 преступлений)[1].

В последние годы мошенники активно используют для совершения своих преступлений социальные сети и видеохостинги в сети Интернет, а также телефонные мессенджеры. Например, в настоящее время в новостных лентах таких социальных сетей как Instagram, ВКонтакте наблюдается всплеск рекламы, сообщающей о якобы имеющейся возможности получить различные виды компенсаций и выплат от государственных органов. Данные рекламные публикации содержат ссылки на сайты мошенников, оформленные в стиле, схожем с сайтами подразделений или фондов государственных органов, в базах которых можно проверить по своим персональным данным якобы положенную человеку компенсацию. После имитации проверки баз данных система выдает сообщение о том, что конкретному человеку действительно должны выплатить от десятков до нескольких сотен тысяч рублей, но для этого необходимо оплатить либо услуги юриста, заполнявшего анкету, либо госпошлину в размере нескольких сотен рублей. При этом жертва ставится перед выбором: рискнуть и заплатить 300–400 рублей для получения сотен тысяч рублей, или проявить осторожность и упустить возможность заработать сумму в несколько раз больше. К сожалению, часть людей поддается на такие уловки мошенников и теряет свои деньги.

Как видно, мошенники рассчитывают на предоставление ложного выбора. Кроме того, за предлагаемую возможность быстрого обогащения без вложения труда мошенники требуют незначительные суммы денег. Именно социальные сети и мессенджеры создают благоприятные условия для такого вида преступлений за счет массового распространения ссылок на мошеннические сайты. В результате этого каждая жертва теряет, казалось бы, незначительную сумму денег, но за счет большого охвата мошенники обогащаются крупными суммами.

Следует отметить, что уровень латентности в этой сфере очень высок и во многом виной этому – незначительные суммы ущерба. За редким исключением потерпевшие готовы обратиться в полицию. Таким образом, высокая латентность и безнаказанность мошенников объясняют столь широкую распространенность данного вида противоправных деяний.

Помимо предложений о полагающихся выплатах и компенсациях от государства, популярным является предлог о различного рода розыгрышах, проводимых деятелями культуры, искусства, шоу-бизнеса. Зачастую известные люди действительно участвуют в различных акциях для своих поклонников, в рамках которых раздают призы. Однако объявления и видеоролики реальных розыгрышей или благотворительных мероприятий в своих корыстных целях используют мошенники,

[1] Состояние преступности в России за 2019 год: статистический сборник. М. : ГИАЦ МВД России. 2020. С. 34.

перенаправляя жертву не на реальный сайт кумира, а на подставной. При этом для реализации своих противоправных деяний мошенники пользуются авторитетом известной личности. Дальнейшая схема совершения мошеннических действий аналогична рассмотренному выше примеру: для возможности получения приза сайт мошенника предлагает оплатить определенный комиссионный сбор либо совершить платеж небольшой суммы для подтверждения реквизитов карты, после производства такого платежа жертва не получает вознаграждения.

При этом жертве могут предложить подождать определенное время, пока, например, обрабатывается запрос / составляется платежное поручение в банк / осуществляется проверка данных службой безопасности и т. п. Это совершается с целью недопущения отмены произведенного платежа в своем банке до того, как мошенник успел распорядиться полученными денежными средствами (с целью скрыть реального получателя средств и лишить банк жертвы возможности отменить платеж мошенником может приобретаться криптовалюта).

В некоторых случаях мошенники действуют еще более бесстрашно, получая от жертвы еще больше средств. Например, под предлогом наличия другого кандидата на получение приза, вынуждают жертву подтвердить серьезность своих намерений, переведя определенную сумму на счет мошенников. Такое вытягивание все больших и больших средств может происходить до тех пор, пока жертва не осознает, что имеет дело с мошенниками. Зачастую диалоги посредством отправки сообщений ведут компьютерные программы по заранее составленному алгоритму.

В описанных примерах обман жертвы совершается по единой схеме:

1) предоставление как можно более широкому кругу адресатов (это достигается посредством рассылки рекламных сообщений и ссылок на мошеннические сайты в социальных сетях и мессенджерах) информации о якобы имеющейся возможности быстрого заработка без материальных и трудовых затрат (например, на видеохостинге YouTube можно встретить видеоролики, «обучающие» как получить компенсацию от США за утечку персональных данных, или как обмануть казино и быстро заработать на этом и т. п.) (рис. 19);

2) направление по ссылке жертвы на сайт мошенника, где якобы проверяется и подтверждается возможность такого заработка по персональным или иным данным жертвы (в действительности введение абсолютно любых, в том числе несуществующих имен выдает один и тот же результат);

3) для получения выплаты в размере нескольких сотен тысяч рублей жертве предлагается оплатить комиссию, пошлину или иным образом названную сумму в размере от 100 до 1000 рублей (рис. 20);

4) после перевода средств мошенники перестают отвечать на сообщения жертвы, либо пытаются отсрочивать время осознания жертвой обмана, либо пытаются обогатиться на ее доверчивости еще больше.

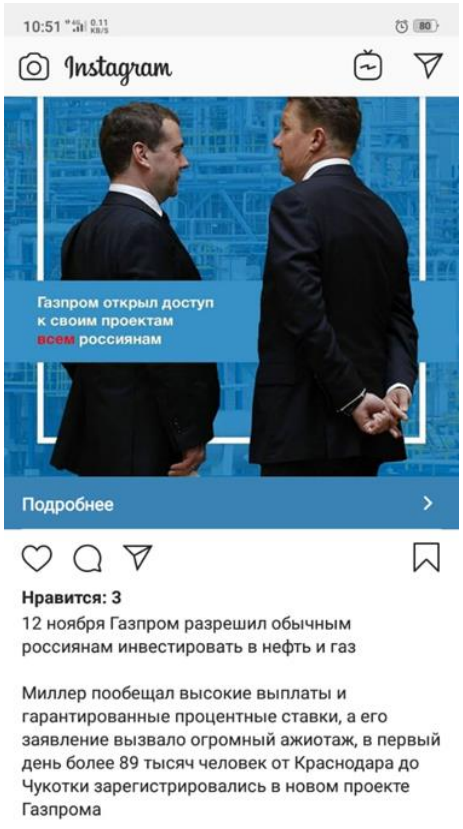

Рис. 19. Пример ложного рекламного сообщения

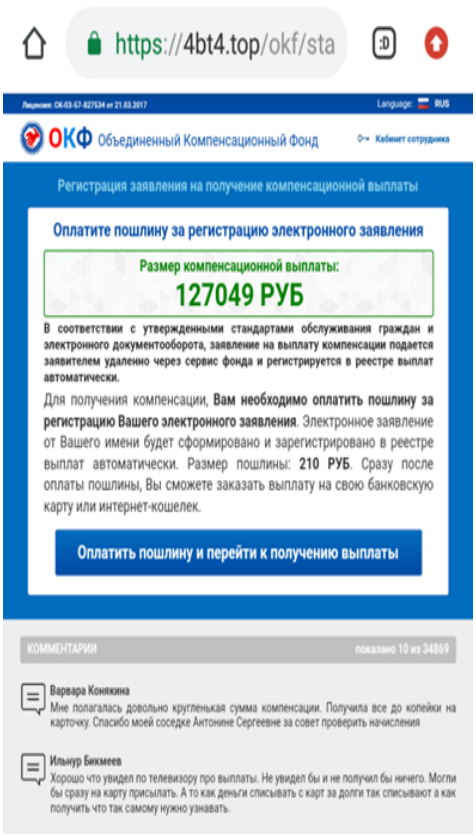

Рис. 20. Мошеннический сайт

Ключевым фактором в данной схеме является попытка мошенников сыграть на корыстных желаниях самой жертвы. Соответственно лучшей защитой от подобных противоправных действий является усвоение истины: «бесплатный сыр может быть только в мышеловке». В то же время следует указать, что иногда мошенники свой обман выдают за социальные обязательства государства в отношении своих граждан. Это повышает актуальность усиления противодействия подобным проявлениям.

Подводя итог вышесказанному, выделим следующие практические рекомендации.

1. Необходимо вести речь о социальной, а в некоторых случаях и юридической ответственности собственников социальных сетей и видеохостинговых ресурсов.

Так, например, руководство социальной сети ВКонтакте достаточно оперативно реагирует на создание мошеннических страниц и распространение вредной информации, удаляя ложные аккаунты и блокируя мошеннические страницы. В социальной сети Instagram также имеется возможность отправить жалобу на мошенников, однако рекламные сообщения на мошеннические страницы в данной сети приходят несколько чаще. В то же время видеохостинговый ресурс

YouTube, предоставляя возможность отправить жалобу, не предусматривает возможности указать на то, что это мошенничество.

Следует отметить, что блокирование страниц мошенников в социальных сетях, служащих для распространения информации о мошенническом сайте без блокирования собственно данного мошеннического сайта и привлечения его создателя к ответственности, является поллиативом. Однако даже такая отлаженная работа руководства данных интернет-ресурсов способна лишить преступников удобных инструментов и сделать их усилия нерентабельными.

2. Кроме того, при получении первых же сообщений от пользователей о мошеннической рекламе (как и любой другой запрещенной информации) администраторам соответствующих интернет-ресурсов следует доводить информацию о данных сайтах до органов внутренних дел для последующего выявления виновных лиц. Совместно с администрацией социальных сетей и видеохостингов органы внутренних дел могли бы проводить работу по отысканию всех жертв мошенников (при желании самих жертв раскрывать сведения о себе). Это требуется как для возмещения причиненного потерпевшим ущерба, так и для привлечения виновных к равной доле ответственности в соответствии с масштабом и уровнем общественной опасности деяния. Кроме того, при отсутствии заявления потерпевшей стороны виновных можно будет привлечь лишь за покушение на мошенничество.

Согласно ответу, поступившему на наше обращение из Управления контроля и надзора в сфере электронных коммуникаций Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), в соответствии с частью 1 статьи 15.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон № 149-ФЗ) в целях ограничения доступа к сайтам в сети Интернет, содержащим информацию, распространение которой в Российской Федерации запрещено, создана единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено» (далее – Единый реестр).

К основаниям внесудебного ограничения доступа, определенным статьей 15.1 Федерального закона № 149-ФЗ, относятся: распространение материалов с порнографическими изображениями несовершеннолетних, информации о способах изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств и культивирования наркосодержащих растений и информации о способах совершения самоубийств, призывов к совершению самоубийства, информации о незаконной деятельности по организации и

проведению азартных игр и лотерей, информации о незаконной розничной продаже дистанционным способом алкогольной продукции, информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц, а также информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействий), распространение которой запрещено федеральными законами.

В электронном виде создана форма для приема жалоб о наличии в сети Интернет данной запрещенной информации[1]. Сообщить о конкретных ссылках на сайты в сети Интернет, содержащие вышеуказанную информацию, можно заполнив вышеуказанную форму. В случае признания информации запрещенной к распространению, доступ к ней будет ограничен в установленном порядке.

Ограничение доступа к сайтам в сети «Интернет» в соответствии со статьей 15.1 Федерального закона № 149-ФЗ осуществляется также на основании решения суда о признании информации, содержащейся на интернет-ресурсе, запрещенной к распространению на территории Российской Федерации. Блокирование сайтов, имеющих признаки мошеннических действий, осуществляется исключительно по решению суда. В свою очередь такое решение выносится судом на основании рассмотрения уголовных дел. В общей сложности в Единый реестр на основании соответствующих судебных решений о признании информации запрещенной (по тематике – экономические преступления) в настоящее время было внесено около 20 тыс. сайтов (указателей интернет-страниц).

На основании изложенного можно сделать вывод о том, что, не смотря на имеющуюся определенную практику в сфере выявления мошенничеств в информационно-телекоммуникационных сетях, в настоящее время имеется потребность в совершенствовании работы органов внутренних дел в данной сфере. Десятки мошеннических страниц и рекламных объявлений в социальных сетях и мессенджерах свидетельствуют о необходимости усиления работы по выявлению Интернет-мошенников. Направлением такого совершенствования может быть установление сотрудничества органов внутренних дел с администраторами и собственниками интернет-ресурсов в части выявления источников распространения запрещенной информации. Кроме того, значительную пользу могло бы оказать расширение сотрудничества с общественными объединениями, работающими в сфере выявления мошеннического контента (например, Лига безопасного интернета и т. п.).

[1] Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено. URL: http://eais.rkn.gov.ru/feedback/ (дата обращения: 12.02.2021).

Вместе с тем, работа органов внутренних дел по выявлению лиц, создающих мошеннические интернет-ресурсы, является лишь реакцией на противоправные действия. В целях организации работы и устранения факторов, способствующих совершению данных преступлений, необходимо проводить работу по усилению информационной грамотности среди всех возрастных групп населения.

Вопросы для проверки знаний

1. Приведите примеры мошеннических схем в сети Интернет.
2. Основываясь на практических рекомендациях, назовите свои способы противодействия мошенническим действиям в сети Интернет.

§ 3. Противодействие информационным угрозам в отношении сотрудников правоохранительных органов

В целях предупреждения методов и форм негативного воздействия в информационном пространстве на общественное сознание и на сотрудников правопорядка необходимо принятие комплекса мер. В частности, в рамках работы по морально-психологическому обеспечению в органах внутренних дел должна проводиться индивидуальная работа с сотрудниками полиции в случае выявления факта травли его или членов его семьи в социальных сетях, поступлению угроз, обнародования его персональных данных и т. п.

Отдельно следует обратить внимание на вопросы информационной сферы и безопасности. Так, целесообразно в рамках комплексной деятельности по противодействию дестабилизации общества организовывать специальные функциональные группы, которые будут осуществлять работу в социальных сетях и мессенджерах. Такие группы должны осуществлять мониторинг, сбор информации о планируемых мероприятиях, их характере, тенденциях и т. п. Отслеживать информационные потоки в режиме онлайн.

Кроме того, целесообразно способствовать созданию неформальных групп, которые будут осуществлять в социальных сетях разъяснительную работу, аргументированно отвечать деструктивным действиям протестующих с целью преодоления ложного негативного фона в сети Интернет. Для этой работы следует активно взаимодействовать с общественными формированиями и использовать их помощь в создании таких групп в социальных сетях.

Собственные штатные IT-специалисты в период проведения незаконных акций также должны быть переведены на интенсивный вариант несения службы, учитывая угрозу совершения хакерских атак на ресурсы органов внутренних дел в сети Интернет. Целесообразно рассмотреть возможность атак и блокировок ресурсов в сети Интернет, рассылающих вредоносную информацию, в том числе персональные

данные сотрудников и иную служебную информацию, специалистами в информационно-телекоммуникационной сфере.

Отдельного внимания заслуживает вопрос информационной культуры всех сотрудников органов внутренних дел. Информационной культурой называются правила поведения в виртуальном пространстве, размещение там фотографий, постов, комментариев и т. п. В период проведения незаконных акций целесообразно разъяснить личному составу об опасности наличия в социальных сетях не только на личных страницах, но и страницах родственников фотографий, на которых изображено лицо сотрудника, что именно эта страница будет найдена злоумышленниками и подвергнута атакам с помощью использования сервиса поиска совпадений по лицу. Кроме того, в период противостояния не целесообразно некоторое время посещать социальные сети, учитывая то, что на их аккаунт могут поступать угрозы и оскорбления. Спустя время, когда внешняя ситуация станет спокойнее, эти угрозы и оскорбления уже не смогут оказать угнетающее психологическое воздействие как на самого сотрудника, так и на членов его семьи.

В целом, работа по противодействию попыткам дестабилизации гражданского общества и захвату власти должна быть заблаговременной, плановой, нацеленной на опережение, комплексной и системной. Отдельного внимания заслуживают меры по недопущению злонамеренной дискредитации органов власти путем распространения ложных сообщений, а также попытки психологического воздействия на сотрудников правопорядка и членов их семей в информационном пространстве. Следует подчеркнуть, что в данном направлении в нашей стране уже сделано многое. Другие меры находятся в разработке.

Так, например, Федеральным законом от 11 июня 2021 г. № 206-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» была введена статья 17.13 КоАП РФ, частью 2 которой предусмотрена ответственность за сбор, передачу (распространение, предоставление, доступ) персональных данных судей и сотрудников правоохранительных органов в связи с осуществлением ими служебной деятельности или выполнением такими лицами общественного долга либо персональных данных близких таких лиц, совершенные с нарушением требований законодательства Российской Федерации в области персональных данных[1]. Введение указанной нормы представляется обоснованным и своевременным. Однако она по своему содержанию является бланкетной и отсылает к положениям законодательства о персональных данных.

[1] О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: федеральный закон от 11 июня 2021 г. № 206-ФЗ // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru (дата обращения: 11.06.2021).

Безусловно, информация о личном номере телефона, адресе места жительства, государственном регистрационном знаке автомобиля является персональными данными сотрудника полиции, распространение которых без его согласия будет являться нарушением законодательства Российской Федерации. Однако, Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» содержит понятие «персональных данных, разрешенные субъектом персональных данных для распространения»[1]. К таким данным могут быть отнесены данные о личной странице в социальных сетях сотрудника полиции или членов его семьи. При этом такая страница может быть обезличена, но, тем не менее, использоваться злоумышленниками для совершения провокаций, психологического давления или иных противоправных действий в отношении хозяина данной страницы. Признать такие действия нарушением законодательства о персональных данных будет довольно проблематично, а, значит, и привлечь нарушителя к административной ответственности не удастся.

Здесь следует разъяснить, что анализ случаев информационной травли сотрудников правопорядка свидетельствует о следующем способе противоправных действий. Злоумышленники используют изображение сотрудника правоохранительных органов либо любого другого человека, не поддерживающего их точку зрения (злоумышленник может как сам сфотографировать сотрудника правопорядка в момент выполнения им задач по обеспечению общественной безопасности, так и использовать фото или видеоматериалы из сети Интернет). Данная фотография с помощью приложений поиска похожих изображений находит в сети Интернет все страницы, на которых изображено лицо с исходной фотографии. Такими страницами могут быть как сайты официальных органов места службы сотрудника, так и персональные страницы социальных сетей или личные кабинеты иных ресурсов как самого сотрудника, так и членов его семьи, на которых от также запечатлен. Так, например, сотрудник полиции может не состоять в социальных сетях, однако его супруга (родители, дети, брат или сестра) на своих личных страницах разместили фотографии, на которых кроме них самих присутствует и сотрудник полиции. В этом случае злоумышленники найдут именно эту страницу родственника сотрудника полиции и смогут организовывать травлю этого человека и через него повлиять на самого сотрудника.

Применение в таких случаях положений об охране изображения (ст. 152.1 Гражданского кодекса Российской Федерации; далее – ГК РФ) или частной жизни гражданина (ст. 152.2 ГК РФ) также не представляется возможным, поскольку указанными нормами не охватываются случаи, когда сбор, хранение, распространение и использование информации о

[1] О персональных данных: федеральный закон от 27 июля 2006 г. № 152-ФЗ // Доступ из справочно-правовой системы «КонсультантПлюс».

частной жизни гражданина или использование его изображения осуществляется в государственных, общественных или иных публичных интересах, а также в случаях, если информация о частной жизни гражданина ранее стала общедоступной либо была раскрыта самим гражданином или по его воле. Так, Постановление Пленума Верховного Суда РФ от 23 июня 2015 г. № 25 «О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации» разъясняет, что без согласия гражданина обнародование и использование его изображения допустимо в силу подпункта 1 пункта 1 статьи 152.1 ГК РФ, то есть когда имеет место публичный интерес, если такой гражданин является публичной фигурой (занимает государственную или муниципальную должность, играет существенную роль в общественной жизни в сфере политики, экономики, искусства, спорта или любой иной области), а обнародование и использование изображения осуществляется в связи с политической или общественной дискуссией или интерес к данному лицу является общественно значимым[1].

Следует отметить, что в отношении сотрудников Росгвардии выявленный законодательный пробел отсутствует. Часть 3 статьи 23 Федерального закона от 03 июля 2016 г. № 226-ФЗ «О войсках национальной гвардии Российской Федерации»[2] предусматривает обеспечение конфиденциальности сведений о военнослужащих (сотрудниках) войск национальной гвардии и членах их семей в качестве гарантии их личной безопасности. Названная норма позволяет полноценно использовать потенциал ст. 17.13 КоАП РФ[3] для привлечения виновных лиц к ответственности и указывает на необходимость предусмотреть аналогичные положения для сотрудников органов внутренних дел. Однако следует отметить, что для сотрудников полиции она должна быть сформулирована несколько иначе. Поскольку сотрудники Росгвардии часто являются сотрудниками подразделений специального назначения, обеспечение конфиденциальности любых сведений о них представляется обоснованным. В отношении же сотрудников полиции такая формулировка будет противоречить принципу гласности и открытости. В связи с этим необходимо разграничить информацию о служебной деятельности сотрудника полиции (за исключением случаев, когда это является государственной или служебной тайной), которая может быть

[1] О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации: постановление Пленума Верховного Суда РФ от 23 июня 2015 г. № 25 // Российская газета. № 140. 2015.

[2] О войсках национальной гвардии Российской Федерации: федеральный закон от 3 июля 2016 г. №226-ФЗ // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru (дата обращения: 11.06.2021).

[3] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. №195-ФЗ // Доступ из справочно-правовой системы «КонсультантПлюс».

общедоступной, и информацию, относящуюся к частной жизни сотрудника полиции, включая его персональные социальные сети или сведения о его родственниках, сбор, обобщение и распространение которой не допускаются.

Таким образом, в настоящее время имеется необходимость правового закрепления в ч. 3 ст. 24 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции» гарантии обеспечения личной информационной безопасности сотрудников полиции и членов их семей в следующей редакции: «3. В интересах личной безопасности сотрудников полиции и членов их семей не допускается распространение без согласия сотрудника полиции в публичных выступлениях, в средствах массовой информации, в сети Интернет и информационно-коммуникационных сетях сведений о частной жизни сотрудника полиции и членов его семьи» [1].

[1] О полиции: федеральный закон от 7 февраля 2011 г. №3-ФЗ // Доступ из справочно-правовой системы «КонсультантПлюс».

ЗАКЛЮЧЕНИЕ

Информационные войны являются реальностью нашей современной жизни и ведутся не только одними странами против других, но и внутри стран (в частности, в Российской Федерации) отдельными объединениями, политическими, криминальными силами, в отношении населения данной страны для достижения своих целей.

Эффективным, опасным и часто применяемым в современном обществе инструментом информационной войны является социальный хакинг. Примеры социального хакинга позволяют выявить индикаторы ложных сообщений, на основании которых возможно их идентифицировать, а также выработать правила (порядок) проверки контента на достоверность (см. с. 38–39).

Противодействие социальному хакингу возможно путем развития информационной культуры и грамотности населения, развития ответственного отношения к информации, а также путем использования органами внутренних дел средств коммуникации (социальных сетей и мессенджеров) в позитивных целях.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

I. Нормативные правовые акты

1. Об утверждении Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 // Официальный интернет-портал правовой информации URL: http://pravo.gov.ru/ (дата обращения: 15.02.2021). – Текст : электронный.

2. **Российская Федерация. Законы.** О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ // Доступ из справочно-правовой системы «КонсультантПлюс» (дата обращения: 15.02.2021). – Текст : электронный.

3. **Российская Федерация. Законы.** О внесении изменений в Кодекс Российской Федерации об административных правонарушениях Федеральный закон от 11 июня 2021 г. № 206-ФЗ // Официальный интернет-портал правовой информации URL: http://pravo.gov.ru, (дата обращения: 11.06.2021). – Текст : электронный.

4. О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации: постановление Пленума Верховного Суда РФ от 23 июня 2015 г. № 25 // Российская газета. – 30 июня 2015 г. – № 140.

II. Литература и Интернет-ресурсы:

1. **Манойло, А. В.** Роль СМИ в разжигании политических конфликтов – теория и практика информационных войн / А. В. Манойло // Геополитический журнал. – 2016. – № 3 (15). – С. 3–8 – Текст : непосредственный.

2. **Манойло, А. В.** Технологии современных информационных войн / А. В. Манойло // Политическая наука. – 2017. – Спецвыпуск. – С. 306–325 – Текст : непосредственный.

3. **Страхов, А. А., Анисимова, Т. В.** Оценка подлинности и достоверности информации в интернет-публикациях / А. А. Манойло, Т. В. Анисимова // Вестник экономической безопасности. – 2016. – № 6. – С. 129–146 – Текст : непосредственный.

4. **Трофимов, В. М., Видовский, Л. А., Дьяченко Р. А.** Модель информационного воздействия в социальных сетях / В. М. Трофимов [и др.] // Научный журнал КубГАУ. – 2015. – № 110 (06). – С. 236–239 – Текст : непосредственный.

5. Non testatum, или откуда в медийный поток прилетают «утки» // Гродзенская правда. – 11 апреля 2018 г. – URL: grodnonews.by/category/zhizn/news42434.html (дата обращения: 11.02.2021) – Текст : электронный.

6. Наркотик, земляника, меф, клубника, конфеты // Молодежная служба безопасности. – URL: http://molbez.ru/anti-fakes/history24.html (дата обращения: 10.02.2021) – Текст : электронный.

7. Готовится новый инфоудар по России // Sonar2050. – URL: https://youtu.be/tC9pn0hCwMU (дата обращения: 10.02.2021) – Текст : электронный.

8. В США намерены содействовать «укреплению принципов журналистской этики» в России // RT. – URL: https://russian.rt.com/world/news/579442-ssha-rossiya-zhurnalistika-grant (дата обращения: 10.02.2021) – Текст : электронный.

9. Публичность – самая страшная беда : чем занимаются сотрудники британской «фабрики троллей» на Украине // Федеральное агентство новостей. – URL: https://riafan.ru/1128331-publichnost-samaya-strashnaya-beda-chem-zanimayutsya-sotrudniki-britanskoi-fabriki-trollei-na-ukraine (дата обращения: 10.02.2021) – Текст : электронный.

10. **Емельянов, В. П.** Терроризм и преступления с признаками терроризирования – СПб, 2010. С. 17 – Текст : непосредственный.

11. **Моисеенко, А. И.** Уголовно-правовая и криминологическая характеристика терроризма (по материалам Южного федерального округа России) : дис. канд. юрид. наук – Ставрополь, 2006. С. 9 – Текст : непосредственный.

12. Digital 2019 : Глобальное использование интернета – URL: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates (дата обращения: 20.03.2021) – Текст : электронный.

13. Шифровка для террориста : одобренные приложения для защищенной связи и новый раунд дебатов о безопасности – URL: https://www.wsj.com/ (дата обращения: 19.03.2021) – Текст : электронный.

14. **Муртазин, А. И., Давлетов, В. И.,** Интернет- пространство как среда для распространения идей экстремизма и терроризма // Актуальные проблемы государства и общества в области обеспечения прав и свобод человека и гражданина. Уфа, 2020. С. 73 – Текст : непосредственный.

15. Как не стать жертвой в эпоху инфомрака – URL : https://время-вперед.рус/post/ как не стать жертвой в эпоху инфомрака (дата обращения: 17.02.2021). – Текст : электронный.

ПРИЛОЖЕНИЕ

Памятка сотрудникам органов внутренних дел по защите от угроз в информационном пространстве

Анализ контента в сети Интернет и мессенджерах позволяет выделить наиболее вероятные угрозы.

1. Распространение вредоносных программ, порча компьютерной техники. Вредоносные программы (компьютерные вирусы) могут похищать информацию, хранящуюся на компьютере, похищать трафик абонента зараженного компьютера, либо приводить к сбою работы программного обеспечения, приводить к потере хранящейся на нем информации. Стандартными и наиболее эффективными правилами безопасности в отношении данной угрозы является использование надежных антивирусных приложений, ответственное отношение к используемым на компьютере носителям информации, непосещение подозрительных сайтов и неустановка пиратских компьютерных программ. Для заражения компьютера жертвы злоумышленники могут применять следующие приемы: например, оставить зараженные вредоносными программами флэш-накопители в заметных местах, где потенциальные жертвы наверняка их увидят. Если жертва вставит эту приманку в рабочий или домашний компьютер, то происходит автоматическая установка вредоносного ПО в систему. Приманка мошенников не обязательно может иметь физическую форму. Онлайн-формы обмана состоят из заманчивых объявлений, которые приводят к вредоносным сайтам или побуждают пользователей загружать вредоносное приложение. Зачастую воздействие на жертву происходит путем атаки ложными сообщениями об угрозах заражения компьютера вирусам. Жертвы обманываются, полагая, что их система заражена вредоносными программами, тем самым решая установить ПО, которое не имеет реальной выгоды (кроме как для преступника) или является вредоносным ПО. Вскоре после установки данной программы преступник похищает интересующую информацию. Распространенным примером этого являются всплывающие баннеры, появляющиеся в браузере во время работы в Интернете, сообщающие под видом работы антивируса о том, что компьютер может быть заражен вредоносными программами-шпионами.

2. Похищение персональных данных и личной информации. Похищение личной информации может осуществляться либо путем применения компьютерных вирусов, либо путем удаленного взлома по сети Интернет, завладения техникой или носителями информации (например, при потере человеком телефона, флеш-накопителя и т. д.), а также путем взлома персональных страниц в социальных сетях, облачных хранилищах. Целью похищения информации может быть последующий шантаж человека под угрозой публичного ее обнародования; дискредитация человека или его близких, в том числе с возможным внесением изменений в личную

информацию, ее искажением; сбор информации о человеке для получения возможности завоевать доверие и последующего совершения мошенничества, вербовки в опасные группы, воздействия на его сознание и манипуляции.

Стандартными правилами безопасности в отношении данной угрозы являются: использовать надежные пароли на своих устройствах, а также в личных кабинетах и персональных страницах различных ресурсов, периодически изменять эти пароли; использовать разные пароли для разных устройств и ресурсов в интернете; не размещать информацию, утечка которой способна причинить вред, в социальных сетях (в том числе на закрытых аккаунтах), облачных хранилищах; при завершении работы в социальных сетях выходить со своих персональных страниц (нажимать на кнопку «выйти»); быть внимательным к внешнему виду и адресу в Интернете страниц того ресурса, на котором вы вводите пароль. Так, один из самых популярных видов атак в социальной инженерии является создание так называемых фишинговых сайтов – это поддельный веб-сайт почти идентичный по внешнему виду его законной версии, на котором имеется форма для входа в якобы личный кабинет жертвы. Если человек не замечает подмены и вводит свои персональные данные (логин и пароль), то они отправляются злоумышленнику, который в последующем сможет воспользоваться ими для взлома личного кабинета жертвы.

3. Травля в сети (кибербуллинг). Этот вид угрозы представляет собой массированное воздействие на жертву путем оскорблений, угроз, унижения, пожеланий несчастий и т. п. Такой вид угрозы особенно опасен для детей и молодежи с еще не окрепшей психикой и более подверженных внешнему влиянию. Для защиты от этого явления в первую очередь родителям необходимо: во-первых, знать о его существовании, чтобы быстрее обнаружить при проявлении подобных фактов в отношении их ребенка; во-вторых, внимательно относиться к изменениям в настроении ребенка, стараться ненавязчиво выяснить причину подавленного состояния; в-третьих, разъяснить ребенку как следует правильно реагировать на подобные проявления; в-четвертых, если источник таких нападок известен персонально, принять необходимые меры для их прекращения. Внимание на проявления таких угроз должны обращать и предпринимать меры к их нейтрализации также и педагогические работники образовательных организаций.

Что же касается правильной реакции ребенка (молодежи) на такие нападки, то ее можно охарактеризовать следующим образом. Следует помнить, что человек, занимающийся кибербуллингом, может быть даже лично не знаком со своей жертвой, а подобное поведение является для него всего лишь развлечением, хулиганством. Поэтому ни в коем случае не стоит принимать все высказывания и оскорбления на свой счет. Озвучиваемые им угрозы являются лишь попыткой вывести из психологического равновесия и не будут реализованы, а значит, из-за них также не стоит переживать. О

любых проявлениях травли необходимо немедленно сообщать родителям, классным руководителям, друзьям. При проявлении фактов оскорбительного общения направлять соответствующие жалобы администраторам социальных сетей, а при таких фактах в мессенджерах включать таких абонентов в «черный список», чтобы сообщения от них не поступали. Кроме того, в таких случаях действует правило: чем острее жертва реагирует на приемы травли, тем злоумышленник больше активизирует свои противоправные действия.

4. Склонение к суициду и опасным действиям. Печально известные «группы смерти» вызвали большой резонанс в свое время, в связи с чем этому направлению было уделено внимание органов власти, были внесены определенные изменения в законодательство. К сожалению, данная проблема полностью не решена в настоящее время. Группы смерти дополнили группы, склоняющие подростков совершать опасные для их жизни и здоровья действия. В таких группах на подростков воздействуют путем представления опасных заданий под видом интересной игры, в которой нужно проявить смелость. Кроме того, за отказ выполнения заданий участника могут обвинить в трусости либо за их выполнение обещать какое-либо вознаграждение. Следует отметить, что молодежи свойственно определенное стремление к экстремальным действиям, желание ощутить всплеск адреналина. Учитывая это, профилактическая работа в отношении подобных угроз должна строиться, с одной стороны, на разъяснении всего спектра возможных неблагоприятных последствий от участия в таких «играх», с другой – на предоставлении возможности молодым людям реализовать энергию в спортивных соревнованиях, конкурсах и иных мероприятиях, на которых организованы условия безопасности.

5. Распространение, изготовление порнографического контента, развратные действия в отношении молодежи. К сожалению, следует отметить, что сексуальная тематика сегодня является достаточно распространенной в молодежном общении. При этом она в значительной степени потеряла признаки интимности, а стала нормальной для публичного обсуждения. С одной стороны на законодательном уровне приняты меры по защите детей от информации, причиняющей вред их здоровью и развитию, в соответствии с которыми, в частности, публично распространяемые информационные материалы должны иметь маркировку возрастных ограничений, однако с другой – тема свободных сексуальных отношений свободно обсуждается в телепередачах, театрализованных и музыкальных проектах и т. п. В сети Интернет фактически в открытом доступе находится контент порнографического содержания. Все это создает благоприятные условия для дальнейшего вовлечения молодых людей в эту сферу. Яркой иллюстрацией того, что принимаемые в этом отношении меры не достаточно эффективны, являются показатели распространения ВИЧ / СПИД. Так, не смотря на ежегодно выделяемые на противодействие

распространению данного заболевания значительные средства, не смотря на поистине напряженную работу задействованных в этом направлении специалистов, статистические данные указывают на то, что в нашей стране по-прежнему не удалось взять под контроль это опасное заболевание. При этом если раньше большинство заразившихся ВИЧ / СПИДом были людьми из групп риска (наркоманы, люди, имеющие нетрадиционные сексуальные отношения), то сегодня более половины вновь заболевших являются гетеросексуальными людьми, не употребляющими наркотиков. То есть основной причиной заражения становятся свободные сексуальные отношения.

Исправление сложившейся ситуации видится в следующих мерах:

– усиление контроля за соблюдением Федерального закона от 29 октября 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»[1];

– стимулирование социальной ответственности СМИ за содержание распространяемого контента;

– проведение разъяснительной работы с родителями с целью расширения практики использования ресурсов «родительского контроля» на устройствах их детей;

– выявление и оперативное реагирование на обнаруженные ресурсы, содержащие детскую порнографию, их блокирование, а также выявление и привлечение к ответственности лиц, причастных к данному противоправному деянию;

– развитие института семьи, акцентирование внимания на высокой значимости семьи, материнства и детства. Как справедливо однажды заметил президент Российской Федерации, традиционная многодетная семья должна вновь стать символом России. На это указывает обновленная Конституция Российской Федерации, а значит, наша задача сегодня заключается в том, чтобы воплотить в жизнь положения, за которые проголосовало абсолютное большинство наших сограждан.

6. Пропаганда наркотиков, алкоголя, потребительства и деградации. Такая пропаганда в сети Интернет приобретает массовый характер через распространение произведений отдельных музыкальных групп, а также демонстрацию молодежными «лидерами мнений» распущенного образа жизни, формирование привлекательного образа, при котором они имеют любые материальные блага, не вкладывая в их получение значительного труда. Ответом на данную угрозу может стать, с одной стороны, наглядная демонстрация истинной картины реальных достижений указанных «молодежных кумиров», результатов подобного образа жизни с целью развенчания мифа об их успешности. С другой стороны, гораздо более

[1] О защите детей от информации, причиняющей вред их здоровью и развитию: федеральный закон от 29 декабря 2010 г. №436-ФЗ // Доступ из справочно-правовой системы «КонсультантПлюс».

сложная, но в то же время более эффективная работа должна быть направлена на формирование жизненных принципов и понятий о достоинстве, чести, совести. В этом отношении целесообразно говорить о необходимости усиления воспитания, в том числе воспитательного потенциала образовательного процесса.

7. Вовлечение в незаконную деятельность. В первую очередь здесь мы говорим о преступных формах незаконной деятельности, распространенными среди которых являются различные формы хищений (кражи, грабежи), хулиганство, участие в незаконном обороте наркотиков. Так, например, в социальных сетях можно найти объявления о возможности легкого заработка. Предлагаемая «работа» представляет собой осуществление так называемых «закладок» наркотических средств и психотропных веществ. Рассказы молодых людей, занимавшихся данным видом незаконной деятельности, опубликованные в сети Интернет, демонстрируют с какой относительной легкостью они согласились на это преступление и как легко нашли соответствующую «работу» (фактически можно сказать, что искать и не пришлось, распространители наркотиков сами находят потенциальных работников)[1]. При этом в отношении опасности быть пойманными у молодых людей часто превалирует ощущение, что с ними этого не произойдет, они ловчее, хитрее, смогут вовремя остановиться. Часто нет четкого представления о высокой опасности совершаемых действий, их вредности для других людей. В связи с этим, среди широкого перечня общесоциальных и специально-криминологических мер профилактики преступного поведения, к которым, в частности, относятся меры воспитательного воздействия, мероприятия по правовой пропаганде и информированию, должно быть предусмотрено доведение информации о неотвратимости наступления ответственности, а также визуальное представление информации о разрушительных последствиях преступной деятельности для других людей.

8. Распространение ложной информации, манипуляция сознанием. Сегодня мы можем говорить о пандемии не только в отношении вируса COVID-19, но и о настоящей киберпандемии ложной информации в социальных сетях и мессенджерах. Можно встретить ложные сообщения, касающиеся практически любой сферы общественных отношений. По характеру такие сообщения могут различаться от самых безобидных (например, о том, что мессенджер WhatsApp скоро станет платным), до тех, что затрагивают важные стороны общественной жизни и искажают представления о правильном поведении (в частности, это относится к

[1] Исповедь наркокурьера : «Думал, сами виноваты, где-то прокололись, но я же не такой, меня точно не поймают» // РИА Новости. 28.05.2019. https://ria.ru/20190528/1554639391.html; «Беда, нет денег? Есть предложение!» Исповедь 19-летней закладчицы из Екатеринбурга, которой грозит 20 лет колонии // Znak.com. 21.12.2020. URL: https://www.znak.com/2020-12-21/ispoved_19_letney_zakladchicy_iz_ekaterinburga_kotoroy_grozit_20_let_kolonii.

необходимости ношения масок в период пандемии, целесообразности вакцинирования, соблюдения иных противоэпидемиологических мер и т. д.). Широкий масштаб распространения ложной информации иногда приводит к тому, что у молодых людей формируется картина мира, полностью оторванная от реальности. Доходит до того, что отдельные люди начинают искренне верить в плоскую форму Земли, пытаются подвести под это мнение аргументы, создают целые группы в Интернете. Однако, если в отношении формы планеты человек демонстрирует лишь собственную безграмотность, то в случае распространения ложной информации, например, политического характера, это становится инструментом для дестабилизации гражданского общества.

Рассмотрим советы для развития информационной культуры молодежи.

Во-первых, необходимо разъяснить, что не стоит любую информацию немедленно воспринимать как достоверную, необходимо проверять ее. Особенно это важно делать в случае наличия в этом сообщении призывов к максимальному распространению. В отношении распространяемых в мессенджерах и социальных сетях сообщений это можно легко сделать, набрав в поисковой строке браузера какую-либо ключевую фразу из проверяемого сообщения. Часто в результатах поискового запроса можно будет увидеть, что распространяемое сообщение уже ранее публиковалось в других городах и было опровергнуто, а значит пересылать нет смысла. Для стимулирования у людей привычки проверять сообщения, прежде чем распространять их дальше, достаточно эффективно задать человеку, приславшему ложное сообщение, вопрос: «А вы проверили достоверность этого сообщения?». Как правило, на это человек отвечает, что лишь переслал пришедшее ему сообщение, либо не отвечает на вопрос. После этого можно отправить в группу ссылку на результаты поискового запроса, где сказано, что это сообщение ложное, а также призывать ответственно относиться к распространяемой информации. После 3–4 раз задавания таких вопросов в группе эпидемия бездумной пересылки ложных сообщений прекращается, так как людям не хочется отвечать на неудобный вопрос.

Во-вторых, нельзя основывать свое мнение на односторонней оценке каких-либо событий. Тематические группы в социальных сетях и мессенджерах имеют существенный недостаток в том, что вся размещаемая в них информация носит строго узконаправленный характер, то есть, если подросток является участником группы сторонников плоской земли, то весь размещаемый там контент будет касаться только различных аргументов в пользу этой теории, а совершенно очевидные нестыковки этих аргументов, указывающее на их ошибочность, а также аргументы противоположной стороны в этой группе освещаться не будут. По этой причине у подростка формируется ложное представление об абсолютной доказанности картины мира, не имеющей ничего общего с реальностью. В связи с этим следует

учить молодежь задавать вопросы, сомневаться, изучать информацию разных источников и подвергать ее анализу.

В-третьих, не стоит воспринимать информацию эмоционально. Здесь должно работать правило, согласно которому, если распространяемая информация или ее источник пытаются воздействовать на эмоции, а не на аргументы разума, высока вероятность того, что вами пытаются манипулировать. Решение по таким сообщениям необходимо принимать спустя определенное время, когда эмоции утихнут, и возобладают разумные аргументы.

9. Вербовка в террористические и экстремистские организации. В полной мере приведенные выше рекомендации относятся и к сфере противодействия вовлечению в террористические и экстремистские организации, так как вербовщики в этих организациях используют приемы распространения ложной информации, манипулирования сознанием, воздействия на эмоции. Не останавливаясь подробно на конкретных приемах вербовщиков, остановимся лишь на одном аспекте. Часто экстремистские организации для вовлечения в свои ряды новых сторонников апеллируют к чувству ложной справедливости. Потенциальной жертве демонстрируется комплекс проблемных аспектов общественной жизни, предлагается извращенное видение причин возникновения этих проблем и предлагаются радикальные пути их решения, как единственные возможные и эффективные. Молодежи свойственен определенный радикализм в суждениях и стремление сделать что-либо значимое, полезное. Однако под воздействием психологических приемов вербовщиков положительные желания и стремления к улучшению жизни трансформируются в разрушительную деятельность. В связи с этим органам государственной власти (в первую очередь органам в сфере реализации молодежной политики) необходимо открыто обсуждать с молодежью существующие в нашем обществе проблемы, обсуждать истинные причины возникновения этих проблем, разъяснять наличие законных способов решения указанных проблем, а также вовлекать молодежные организации в созидательную деятельность, осуществлять их поддержку, тесное взаимодействие, при этом делать это в инициативном порядке, то есть самостоятельно мониторить существующие молодежные объединения и предлагать им возможные варианты взаимодействия. Такая работа, с одной стороны, позволит молодым людям социализироваться, проявить свои творческие, управленческие и иные созидательные качества, почувствовать собственную востребованность и полезность. С другой стороны, это позволит сохранять активность таких молодежных групп в рамках законной деятельности и не даст возможности радикализоваться. Кроме того, это позволит существенно повысить эффективность работы самих государственных органов за счет использования ресурса молодежных и иных общественных организаций.

10. Мошенничество с использованием сети Интернет и иных коммуникационных сетей. Частыми способами мошеннических действий в сети Интернет и мессенджерах являются следующие:

1) взлом персональных страниц в социальных сетях и рассылка от имени хозяина данной страницы просьб об отправки денег взаймы. При этом для придания достоверности того, что деньги получит действительно хозяин страницы социальной сети мошенники отправляют жертве фотографию с изображением банковской карты, на которой написано действительное имя того, с чьей страницы обращается мошенник. Защититься от такого способа мошенничества достаточно просто, если взять за правило все важные вопросы, к которым относится и финансовый вопрос, решать с людьми лишь при личном контакте, либо получив подтверждение по аудио или видео звонку;

2) мошенничество при продаже товаров. Этот способ может использовать площадки продажи товаров, такие как Авито, Юла и т. п., при этом злоумышленник, представляясь хозяином товара, может просить предоплату как подтверждение серьезности намерений покупки. Либо мошенниками могут создаваться специальные подставные сайты магазина, в котором товар предлагается купить по невероятно выгодным условиям. После получения предоплаты мошенники перестают выходить на связь. Чтобы не стать жертвой такого вида мошенничества, оплату товаров необходимо производить только при надежности сделки (к примеру, при доставке товара наложенным платежом, курьером, либо при личной встрече), а также использовать для покупок только проверенные и надежные сайты. Для проверки можно обращать внимание на оформление сайта, наличие контактов, регистрационных данных, а также проверять достоверность данных по номеру ИНН на сайте ФНС России (услуга бесплатная и доступна всем);

3) использование фишинговых сайтов известных магазинов;

4) мошенничество при ложной благотворительности. Сверка реквизитов;

5) рассылка ложных писем о полученном наследстве либо предложения ведения совместного бизнеса, для реализации которого необходимо внести определенные инвестции;

6) обман на сайтах знакомств, где мошенником создается ложная страница человека, якобы желающего установить отношения, ведется переписка с потенциальной жертвой, в результате которой мошенник просит жертву одолжить деньги на решение каких-либо проблем, приобретения билета для встречи и т. п.;

7) вовлечение в финансовые пирамиды.

Учебное издание

Романов Антон Александрович
(кандидат юридических наук)
Давлетов Вадим Илдарович
(б/с, б/з)

ПРОТИВОДЕЙСТВИЕ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ДЕСТРУКТИВНЫМ ПРОЯВЛЕНИЯМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В СЕТИ ИНТЕРНЕТ КАК ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-практическое пособие

Редактор Э. Р. Ишемгулова

Подписано в печать 10.12.2021	Выход в свет 15.12.2021
Гарнитура Times	Формат 60x84 1/16
Уч.-изд. л. 3,8	Усл. печ. л. 4
Тираж 40 экз.	Заказ № 83

Редакционно-издательский отдел
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2

Отпечатано в группе полиграфической и оперативной печати
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2