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 2020

УДК 355.01:001.102:316.776.3(470)(075.8)
ББК 67.401.213
Р 56

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

Р 56 Романов А.А., Давлетов В.И. Противодействие органов внутренних дел деструктивным проявлениям социальной инженерии в сети Интернет как элемент обеспечения информационной безопасности [Текст] : учебно-практическое пособие. – Уфа : Уфимский ЮИ МВД России, 2020. – 39 с.

В учебно-практическом пособии раскрываются основные характеристики понятий «информационная война», «социальная инженерия», «социальный хакинг», приводится подтверждение опасности информационных войн, описание методов ведения информационных войн и общая характеристика социальной инженерии. На основании собранного эмпирического материала авторы выявляют признаки (индикаторы) ложных сообщений, являющихся орудием социальных хакеров. Основное значение работы заключается в формулировании конкретных предложений и направлений деятельности органов внутренних дел по противодействию информационному давлению посредством социальных сетей и мессенджеров. Кроме того, подготовлены конкретные инструменты для такого противодействия.

Учебно-практическое пособие предназначено для сотрудников органов внутренних дел и может применяться ими в профилактической деятельности в различных сферах (работе участкового уполномоченного полиции, инспектора по делам несовершеннолетних, сотрудников подразделений по связям с общественностью, в рамках работы лекторских групп образовательных организаций МВД России и т.д.). Также пособие могут применять все социально активные граждане и общественные организации, деятельность которых направлена на развитие информационной культуры и грамотности населения.

УДК 355.01:001.102:316.776.3(470)(075.8)
ББК 67.401.213

С О Д Е Р Ж А Н И Е

Введение

Стратегия национальной безопасности Российской Федерации, утвержденная указом Президента Российской Федерации от 31.12.2015 № 683, 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 стали 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. Активно злоумышленниками применяются методы социального хакинга, под которым понимается информационное воздействие на человека с целью спровоцировать его на определенные, выгодные первому 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.

Целью исследования является выработка предложений по противодействию проявлениям деструктивного социального хакинга в социальных сетях и мессенджерах.

Для достижения указанной цели необходимо решить следующие задачи:

– дать характеристику понятий «информационная война», «социальная инженерия», «социальный хакинг»;

– дать описание методов ведения информационных войн и общую характеристику социальной инженерии;

– на основе анализа примеров социального хакинга, обобщения и системной характеристики таких примеров, выявить характерные черты

(индикаторы) ложных информационных сообщений, позволяющие их идентифицировать;

– выработать предложения по противодействию распространения ложной информации, а также снижению эффективности социального хакинга как оружия (инструмента) информационной войны.

Научная новизна исследования определяется тем, что авторами произведен системный анализ примеров социального хакинга в российском сегменте социальных сетей и мессенджерах, который позволил 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.

Теоретическая значимость заключается в том, что расширены представления о методах ведения информационных войн посредством применения социального хакинга в социальных сетях и мессенджерах. Результаты исследования могут дать импульс для дальнейшего глубокого изучения данного явления.

Практическая значимость исследования заключается в формулировании конкретных предложений и направлений деятельности органов внутренних дел по противодействию информационному давлению посредством социальных сетей и мессенджеров. Кроме того, подготовлены конкретные инструменты для такого противодействия.

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 21 веке. К сожалению, многие люди используют этот термин, не зная его истинное значение**.** В целях установления общего определения, в данной статье будет дано понятие информационной войны, основанное на обсуждении оружия, стратегий и контрмер, связанных с «информационной войной».

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 стран участвующих в ней.

Что такое информационная война? 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 информационная война;

2) корпоративная информационная война;

3) глобальная информационная война.

А также классифицируется по следующим формам:

1) война в сфере командования и управления;

2) разведывательная война;

3) радиоэлектронная война;

4) психологическая война;

5) хакерская война;

6) экономико-информационная война;

7) кибервойна.

Простого определения информационной войны, возможно, не существует, так как информационная война – это многогранная система мер противоборства имеющая сложную систему. В своей работе «Информационные войны» Мартин Либицкий дает 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].

Понятие информационной войны имеет много измерений. В частности, мы говорим об информационной войне как о классе 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,

[1] Libicki, Martin C. What Is Information Warfare? / Martin C. Libicki. – Washington : Center for Advanced Concepts and Technology Institute for National Strategic Studies, 1995. – 104 p. – Текст : непосредственный.

безусловно, может применяться в любой конкурентной ситуации, государственной или частной, гражданской или военной.

Установив определение информационной войны, возникает следующий логический вопрос - что нам нужно для того, чтобы участвовать в информационной войне? В частности необходимо определить, что такое оружие информационной войны? Чтобы ответить на этот вопрос, мы рассмотрим каждый из методов и дадим краткий обзор наиболее распространенных видов оружия, используемых для их достижения.

Первым оружием информационной войны можем считать сбор информации. Сбор информации является частью информационной войны, потому что «информационная революция подразумевает возникновение способа ведения войны, в котором одна сторона, которая знает больше чем другая сторона, будет пользоваться решающими преимуществами в ходе войны». Идея состоит в том, что чем больше информации у человека, тем выше его ситуационная осведомленность, что приводит к лучшим планам боя и, надеюсь, 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, потому что 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. Инструменты, используемые в этой области, - это 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 и других технологий и протоколов передачи данных. Без этих технологий невозможно было бы обеспечить передачу информации в режиме реального времени, как этого требуют современные стандарты.

Теперь необходимо остановиться на вопросе защиты информации. Одним из наиболее важных аспектов информационной войны является необходимость сократить объем информации, к которой имеет доступ ваш противник. Важной частью этого вопроса заключается в защите имеющейся у вас информации от захвата другой стороной. Оружие, используемое для защиты информации, делится на два класса. Во-первых, это технологии, которые физически защищают наши жизненно важные объекты хранения данных, компьютеры и транспортные механизмы, включая бомбы и пуленепробиваемые оболочки, и механизмы предотвращения вторжений, такие как замки и сканирование отпечатков пальцев. Во-вторых, это технологии, которые предотвращают, возможность информации быть замеченной и перехваченной врагом. Это, безусловно, включает в себя основные технологии компьютерной безопасности, такие как пароли, а также более сложные технологии, такие как шифрование. Зашифровывая свои собственные сообщения и расшифровывая сообщения другой стороны, каждая сторона выполняет квинтэссенцию информационной войны, защищая свой собственный взгляд на реальность, одновременно занижая взгляд другой стороны.

Следующее оружие в контексте информационной войны это манипулирование информацией - это изменение информации с целью искажения реальной картины противника. Это можно сделать с помощью ряда технологий, в том числе компьютерных программ для редактирования текста, графики, видео, аудио и других форм передачи информации. Дизайн манипулируемых данных обычно выполняется вручную, поэтому те, кто командуют, имеют контроль над картиной, которая представляется врагу, но вышеупомянутые технологии обычно используются для ускорения процесса физического манипулирования после того, как контент был загружен.

Заключительными аспектами информационной войны, является изменение, совершенствование, и отрицание какой либо информации. Все три техники являются средством достижения одной и той же общей цели - предотвращения получения врагом полной, правильной информации. Из-за их сходства, многие из способов используются для достижения одной или нескольких целей. В связи с этим необходимо обсудить их совместно. Некоторые из наиболее популярных видов оружия, используемых для ведения этих видов информационной войны, - это спуфинг, введение шума, глушение и перегрузка.

Спуфинг - это метод, используемый для снижения качества информации, отправляемой противнику. Поток информации противника нарушается введением в этот поток «пародии» или фальшивого сообщения. Этот метод работает, так как он позволяет предоставлять «ложную информацию целым системам, чтобы побудить эту организацию принимать неправильные решения на основе этой ошибочной информации».

Другой способ нарушить информацию, получаемую оппонентом, - ввести шум в используемую частоту. Фоновый шум затрудняет для противника отделить фактическое сообщение от шума. Этот метод наиболее полезен тогда, когда противник использует формы беспроводной связи, так как эти частоты можно использовать без необходимости подключения к физической сети кабелей.

Заклинивание - это метод, используемый для достижения отрицания, который включает перехват сигналов, передаваемых между двумя каналами связи или между датчиком и каналом.

Считается, что современный мир приобрел беспрецедентную уникальную форму. Человечество стало свидетелем быстрых и радикальных изменений в формах и структурах, определивших его развитие за последние полвека. Геополитическое окружение мира безвозвратно изменилось в течение двадцати лет после распада СССР. Перераспределены мировые ресурсы, военно - политические инструменты, появились новые центры сил. В результате

национальные государства столкнулись с рядом фундаментальных проблем, которые требуют разработки новой стратегии и реакции.

Одна из таких проблем связана с так называемыми информационными войнами. Информационную войну следует понимать как серию нападений на гражданское или военное население государства - противника путем дезинформации и пропаганды с целью достижения определенных политических или военных целей. В то время как исследователи и военные эксперты различают несколько типов информационной войны, 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 их эмоции и рассуждения. Объединив эти два понятия, можно говорить об информационно-психологических войнах, которые становятся неотъемлемой частью постмодернистской геополитики, в дополнение к традиционным войнам.

Как только враг получает информацию, мало кто сможет помешать ему ею манипулировать. В связи с этим, действительно, существуют только две контрмеры, доступные для защиты от такого рода нападения. Во - первых, необходимо минимизировать возможность противника перехватить имеющуюся информацию. Методы защиты информации здесь наиболее эффективны, так как они не дают врагу ни получить доступ, ни понять информацию, как она была передана изначально.

Во - вторых, ключ к защите от манипулирования данными заключается в предотвращении повторного внедрения измененных данных в поток реальной информации. К счастью, для этого существует несколько методов, наиболее распространенных из которых является конечность. Собирая одну и ту же информацию из нескольких избыточных источников, вы повышаете вероятность получения правильной информации. Даже если противник успешно испортит эти данные на одной линии связи, вы легко обнаружите плохие данные, так как они отличаются от изображения, выполненного остальными вашими источниками.

Будущее достаточно непредсказуемо. Информационная война с каждым годом будет набирать свои обороты. На сегодняшний день неизвестно когда это произойдет и кто запустит первые крупные атаки. Угроза информационной войны подобна угрозе ядерной войны. Всегда будет надежда, что этого не произойдет, однако план и средства защиты должны быть подготовлены. В информационной войне мир не будет разрушен, как это было бы в ядерной войне. Но экономика может быть опустошена в информационной войне так же, как планета может превратится в пустошь после ядерной атаки.

«Кто владеет информацией, тот владеет миром», данное выражение точнее всего отражает картину современного мира. Вопрос защиты информации в настоящее время является одним из самых актуальных. В погоне за усовершенствованием технологий защиты информации мы забываем о самом слабом звене в защите информации – человеческом факторе, который является одним из самых уязвимых элементов системы защиты информации. Злоумышленники строят свои действия на методах, основанных на социальной инженерии, которая предполагает использование слабостей человека в ходе тергетированной атаки на него. В частности в процессе данной атаки методы социальной инженерии основываются на особенностях психологии человека, направленных на слабости и особенности личности (жадность, невнимательность, любопытство, наивность, безграмотность). Данные методы активно используются социальными инженерами как в сети Интернет, так и за её пределами.

Понятие «социальная инженерия», которое распространяется в настоящее время, появилось относительно недавно, но техники ведения существуютс давних пор. В Древней Греции и Риме имели уважение и почет люди, которые нередко 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 государства,

многие организации также подвергаются атакам в целях получения информации и усовершенствуют свою корпоративную безопасность.

В сфере информационной безопасности данный термин был разработан бывшим компьютерным преступником, ныне консультантом по 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, которое представляет собой метод получения информации путем обмана посредством использования человеческого фактора[1].

Социальная инженерия - это термин, используемый для широкого спектра вредоносных действий, осуществляемых через взаимодействие с людьми. Он использует психологические манипуляции, чтобы обмануть пользователей в совершении ошибок безопасности или раздавать конфиденциальную информацию. Атаки социальной инженерии происходят в один или несколько шагов. Преступник сначала собирает информацию о предполагаемой жертве, такую как потенциальные точки входа в сеть и слабые протоколы безопасности, необходимые для продолжения нападения. Затем злоумышленник переходит к завоеванию доверия жертвы и предоставляет стимулы для последующих действий, нарушающих правила безопасности, таких как раскрытие конфиденциальной информации или предоставление доступа к критически важным ресурсам.

Социальная инженерия существует в различных формах и может быть выполнена в любом месте, где задействовано человеческое общение. Ниже приведены наиболее распространенные формы цифровой социальной инженерии.

Травля

[1] Искусство обмана / Кевин Д. Митник, Вильям Л. Саймон [пер с англ.: А.А. Груздев, АВ. Семенов]. – М.: ДМК Пресс, 2006 – 124 с. – ISBN 5-98453-011-2. – Текст : непосредственный.

Данный метод заключается в даче ложного обещания, которое направлено на такие черты характера человека, как жадность или любопытство. Они заманивают пользователей в ловушку, которая крадет их личную информацию или наносит вред их системам.

Самой распространённой формой социальной инженерии является использование физических носителей для внедрения вредоносных программ. Например, злоумышленники оставляют приманку - как правило, зараженные вредоносными программами флэш-накопители—в заметных местах, где потенциальные жертвы наверняка их увидят (например, ванные комнаты, лифты, парковка целевой компании). Приманка имеет аутентичный вид, например, ярлык, представляющий его как список заработной платы компании. Жертвы берут приманку из любопытства и вставляют ее в рабочий или домашний компьютер, в результате чего 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.

Еще одним видом обмана в сети является подведение жертвы бомбардировке ложных тревог и фиктивных угроз. Жертвы обманываются, думая, что их система заражена вредоносными программами, тем самым решая установить программное обеспечение, которое не имеет реальной выгоды (кроме как для преступника) или является вредоносным ПО. Вскоре после установки данной программы преступник похищает интересующую информацию. Распространенным примером внушения для обывателя является всплывающие баннеры, появляющиеся в вашем браузере во время серфинга в сети Интернет, отображая такой текст, как «ваш компьютер может быть заражен вредоносными программами-шпионами». Он либо предлагает установить инструмент (часто зараженный вредоносными программами) для вас, либо направит вас на вредоносный сайт, где ваш компьютер заражается.

Следующим видом обмана является предлог. Здесь злоумышленник получает информацию с помощью хитрой лжи. Мошенничество часто инициируется преступником, притворяющимся, что ему нужна конфиденциальная информация от жертвы, чтобы выполнить критическую задачу. Обычно злоумышленник начинает с установления доверия к своей жертве, выдавая себя за коллег, сотрудников полиции, банковских и налоговых органов или других лиц, имеющих право на получение данной информации. Под предлогом задаются вопросы, якобы необходимые для подтверждения личности жертвы, с помощью которых они собирают важные личные данные. Все виды соответствующей информации и записей собирается с помощью этой аферы, такие как номера социального страхования, личные адреса и номера телефонов, телефонные записи, даты отпуска персонала, банковские записи и даже информацию о безопасности.

Как один из самых популярных видов атак в социальной инженерии является, фишинг-мошенничество – который заключается в создании у человека чувства срочности, любопытства или страха у жертв с помощью электронной почты и текстовых сообщений. Затем он побуждает жертву раскрывать конфиденциальную информацию, щелкать ссылки 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, требующем немедленных действий с их стороны, например срочное изменение пароля. Он 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 отправляется 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.

Бывают более целенаправленные версии фишинга, когда злоумышленник выбирает конкретных лиц или предприятия. Затем они адаптируют свои сообщения на основе характеристик, должностей и контактов, принадлежащих их жертвам, чтобы сделать их нападение менее заметным. Фишинг требует гораздо больше усилий от преступника и может занять недели и месяцы, чтобы получить результат. Их гораздо труднее обнаружить и они имеют лучшие показатели успеха, если делать это умело.

Сценарий фишинга может включать самого злоумышленника, который, выдавая себя за консультанта организации, отправляет электронное письмо одному или нескольким сотрудникам. Он написан и подписан точно так же, как обычно делает консультант, тем самым обманывая получателей, думая, что это подлинное сообщение. Сообщение предлагает получателям изменить пароль и предоставляет им ссылку, которая перенаправляет их на вредоносную страницу, где злоумышленник теперь захватывает их учетные данные.

К вопросу о профилактике социальной инженерии можно сделать следующие выводы. Социальные инженеры манипулируют человеческими чувствами, такими как любопытство или страх, чтобы осуществить схемы и заманить жертв в свои ловушки. Поэтому будьте осторожны, когда вы сомневаетесь в подлинности сайтов, или когда вы находите цифровые накопители. Необходимо быть бдительным, так как это может помочь вам защитить себя от большинства социальных инженерных атак, происходящих в цифровой сфере. Кроме того, следующие советы помогут улучшить вашу бдительность по отношению к социальной инженерии.

Не открывайте сообщения электронной почты, и вложения из подозрительных источников, если вы не знаете отправителя, вам не нужно отвечать на сообщения электронной почты. Даже если вы знаете их и подозреваете, что в их сообщении может содержаться вредоносная программа, перепроверьте и подтвердите новости из других источников, например, по телефону или непосредственно с сайта поставщика услуг. Помните, что адреса электронной почты подделываются все время; даже письмо, предположительно

поступающее из надежного источника, может быть фактически инициировано злоумышленником.

Использовать многофакторную аутентификацию – одна из наиболее ценных частей информации, которую ищут злоумышленники, это учетные данные пользователя. Использование многофакторной аутентификации помогает обеспечить защиту вашей учетной записи в случае компрометации системы. Будьте осторожны с заманчивыми предложениями, подумайте дважды, прежде чем принять его как факт.

Обновляйте антивирусное программное обеспечение – убедитесь, что автоматические обновления включены, или развивайте привычку загружать последние обновления антивируса ежедневно. Периодически проверяйте, применены ли обновления, и проверяйте систему на наличие возможных заражений.

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

В данном разделе говоря об обнаружении, мы имеем ввиду идентификацию тех или иных постов в сети Интернет или сообщений в мессенджерах, как примеров социального хакинга. Речь не идет об их поиске, так как в большей своей части рассматриваемые примеры были получены авторами работы в процессе повседневной жизнедеятельности через «родительские группы» или «группы по интересам» в Сети, без выполнения целенаправленных поисковых действий. Основная задача при получении таких сообщений состояла в том, чтобы выявить подложность содержащейся в ней информации и, впоследствии, определить цель распространения данного сообщения.

Именно по цели распространения в отдельную группу можно выделить контент, направленный на мошенническое завладение материальными ценностями. Такие сообщения имеют ярко выраженную корыстную цель.

Примерами таких сообщений являются следующие:

– через взломанную личную страницу в социальной сети мошенники от имени жертвы рассылают сообщения ее друзьям с просьбой дать денег в долг (не смотря на то, что данный способ не является новым, к сожалению по прежнему встречаются люди, попадающие в данную ловушку);

– 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);

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

Таких примеров социального хакинга в корыстных целях огромное множество. В настоящее время этот вопрос достаточно широко описан в научной литературе, а в сети Интернет есть множество сайтов, где освещаются новые способы таких преступлений и даются рекомендации по противодействию им. Именно поэтому в данной работе мы не будем подробно останавливаться на данных примерах социального хакинга.

Отметим, что характерной чертой таких сообщений является либо прямая просьба о переводе денежных средств, либо попытка получить критические сведения о финансовых инструментах жертвы. Универсальной рекомендацией в такой ситуации будет проявлять бдительность при любых финансовых расчетах и не допускать утечки информации о средствах обеспечения безопасности финансовых инструментов.

В настоящей работе больший интерес для нас представляют примеры ложных информационных сообщений, которые не носят корыстного характера. Так, авторы исследования, сами являясь родителями, заметили периодическое появление массовых рассылок в родительских группах школ и детских садов в мессенджере WhatsApp ложных сообщений, якобы предупреждающих о какой-либо опасности для детей.

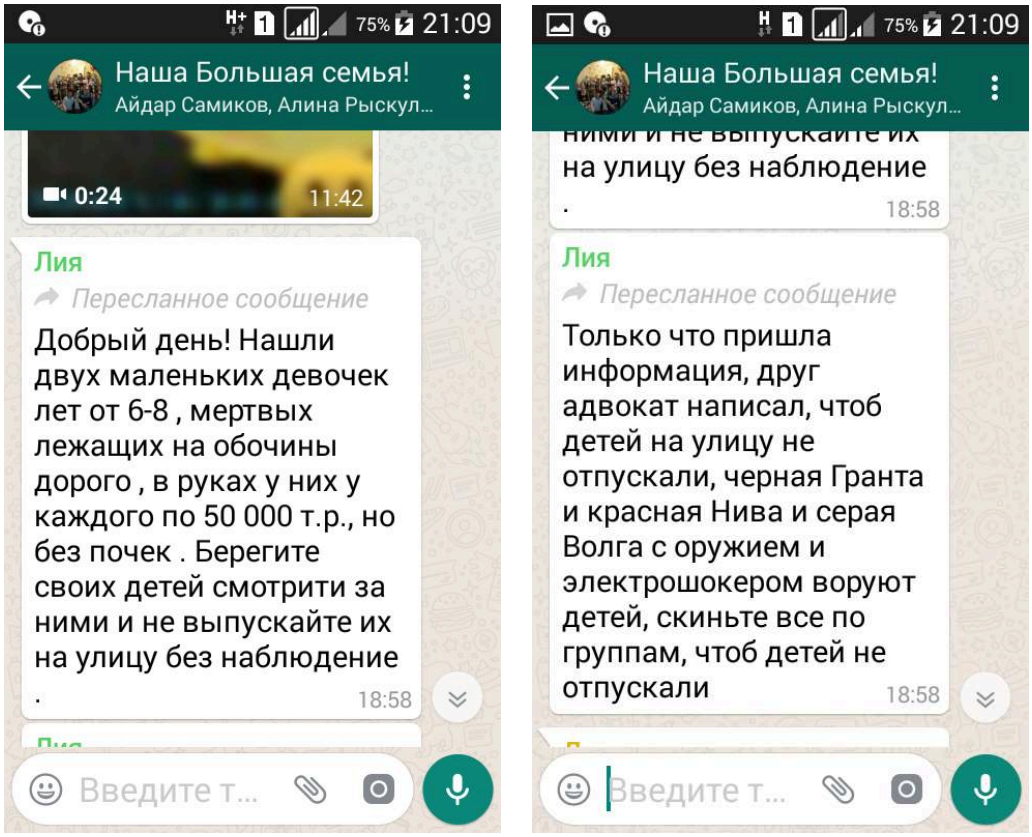

Рис. 1. Примеры ложных сообщений из «родительских групп» в мессенджере WhatsApp

Получая подобные сообщения родители, желая добра другим людям, тут же стараются максимально распространить их, помогая тем самым злоумышленникам. Можно было бы предположить, что создатели этих ложных сообщений преследуют таким образом благую цель научить детей и их родителей бдительности, осторожности. Но это не подтверждают другие ложные сообщения, описывающие либо совершенно нереальные угрозы (как, например, сообщение о жуке-убийце. См.: рис. 2), либо о якобы оказании помощи нуждающимся путем пересылки сообщения (см.: рис. 3), о якобы предоставлении определенных бонусов сделавшим «репост» (см.: рис 4) и т.д. и

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

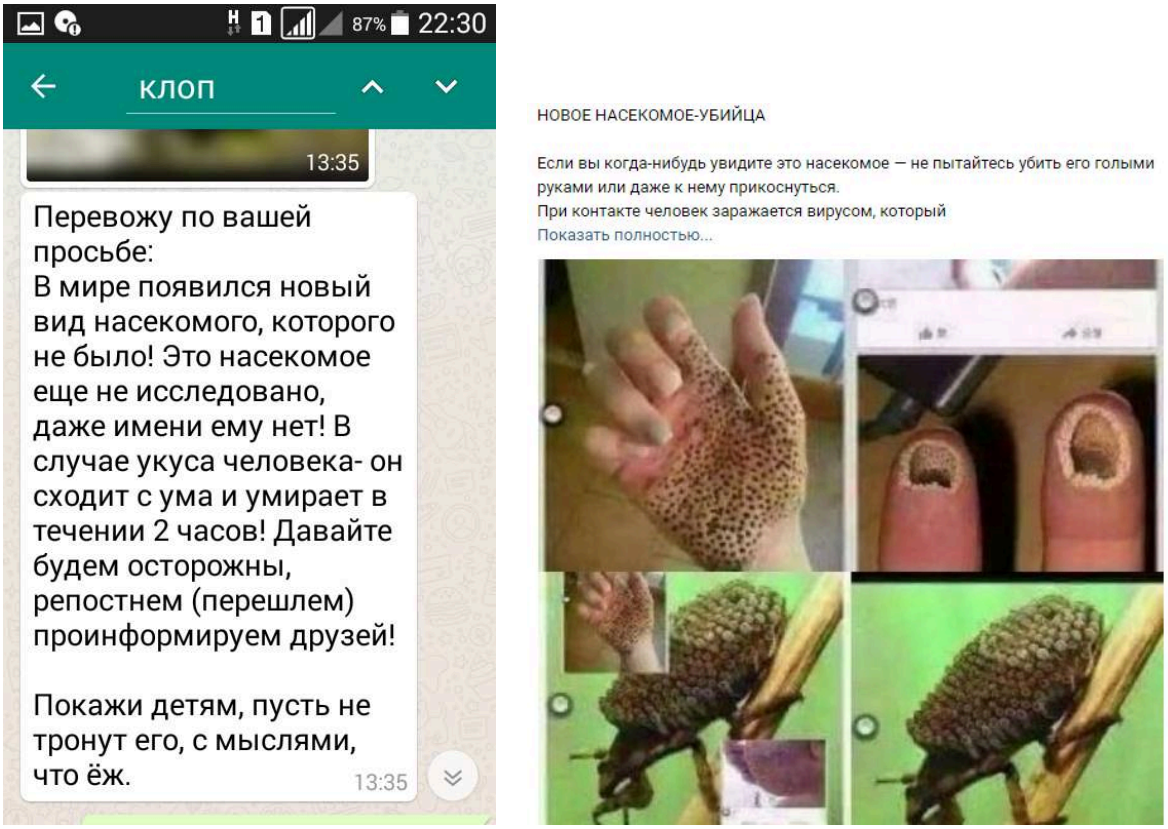

Рис. 2. Ложное сообщение о жуке-убийце, сопровождающееся подборкой ложных фото

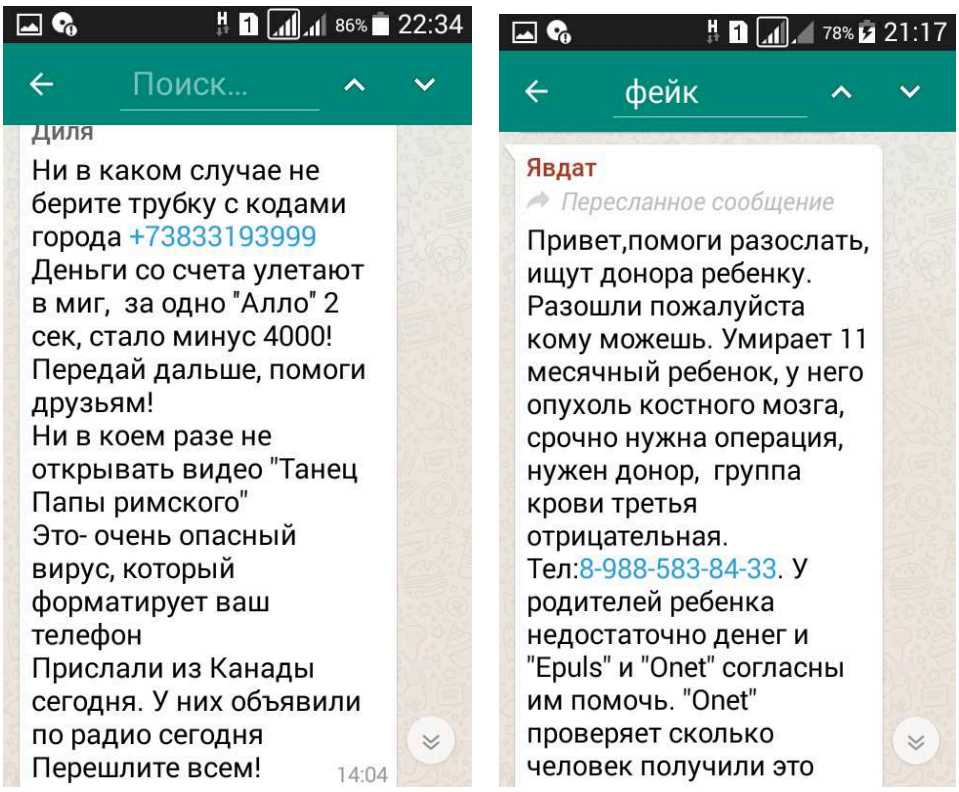

Рис. 3. Примеры ложных сообщений, манипулирующих чувствами людей

В то же время следует подчеркнуть, что в основном эти сообщения не являются подростковой шалостью, как может показаться на первый взгляд (хотя, вероятно, можно встретить и такие). На это указывает несколько особенностей. Во-первых, ряд из этих сообщений помимо текста сопровождается фотографиями, аудио или видео материалами, смонтированными или скомпилированными таким образом, чтобы создавалось ощущение подтверждения распространяемой лжи. Такие сообщения сделаны не «на скорую руку», а 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 якобы раздающейся детям возле школ жевательной резинке или конфетах с наркотиками периодически появляется в сетях и группах уже на протяжении около десяти лет. Почти каждый раз текст сообщения и прилагаемые к нему фотографии незначительно изменяются. Это

свидетельствует о том, что сообщение не случайно «облетев всю Россию» вновь возвращается по второму кругу в города, где уже появлялось ранее, а редактируется и запускается заново. При этом, как правило, запускаются сразу несколько ложных сообщений одновременно или с незначительным промежутком времени. Бывало, что авторам настоящего исследования в течение одного дня приходило три ложных сообщения на разную тему. Данный факт также указывает на скоординированность действий злоумышленников.

Какова же цель распространения таких «фейков», если это не простая забава хулиганов или корыстные действия мошенников? Еще одна закономерность появления ложных сообщений позволяет нам выдвинуть гипотезу о том, что они являются орудием, инструментом информационной войны. По сути это является информационным терроризмом.

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

Таким образом, можно констатировать, что распространяемые в социальных сетях и мессенджерах ложные сообщения, независимо от конкретного их содержания, являются инструментами информационного давления, создание нестабильности и благоприятной почвы для иных воздействий. Эти сообщения манипулируют ощущениями и эмоциями людей и имеют своей целью вызвать определенные чувства и подтолкнуть к совершению определенных действий.

Распространение ложных сообщений может решать несколько задач:

– 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 ощущение страха, собственной незащищенности;

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

Как было ранее отмечено, ложные сообщения, как правило, готовятся по определенным алгоритмам, в связи с чем, имеют некоторые схожие признаки. По наличию этих признаков возможно идентифицировать ложные сообщения, отличить их от достоверной информации. Такими признаками – индикаторами, являются:

1) сообщение не содержит указания на время и место описываемого события. Это делается для того, чтобы ложное сообщение могло получить максимальное распространение в разных городах и чтобы распространение длилось максимально долго. Например, если человек получит сообщение о том, что на автовокзале нашли девочку и ищут ее родителей (см.: рис. 4), но с момента события прошло уже недели две, он с большой долей вероятности не станет

пересылать это сообщение, так как оно уже не актуальное, а за прошедшее время родители наверняка нашлись. Тем более не станут пересылать сообщение о событии, произошедшем в другом городе. Если в ложном сообщении и имеется указание на какое-либо место события, то лишь такое, которое не добавляет конкретики: возле Ашана, на улице Ленина, на автовокзале, недалеко от музыкальной школы и т.п. Все перечисленные места и объекты имеются почти во всех крупных городах России. В указанном правиле бывают и исключения. Так, например, в сообщении о том, что группа «Кит» планирует организовать массовое самоубийство подростков (5 тысяч человек), была указана конкретная дата (см. рис. 5). Возможно, конкретная дата в этом сообщении была внесена одним из родителей перед тем, как он дальше стал его распространять. Однако благодаря именно этому обстоятельству по прошествии указанной даты дальнейшее распространение ложного сообщения в первоначальной редакции прекратилось.

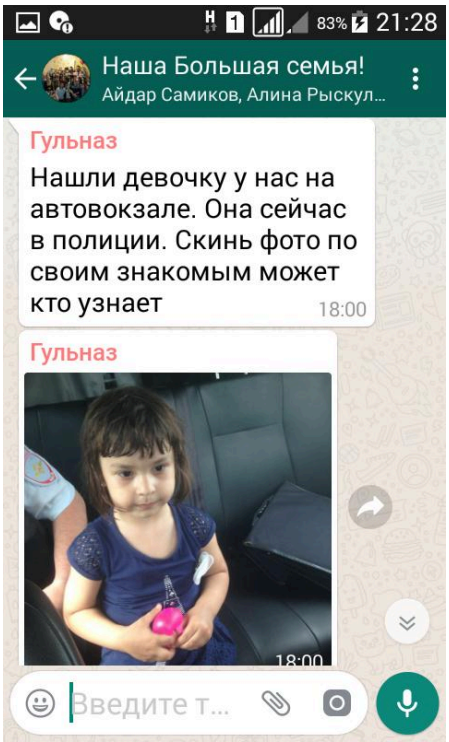

Рис. 4. Сообщение о девочке, которую в течение нескольких лет «находили» в разных городах России

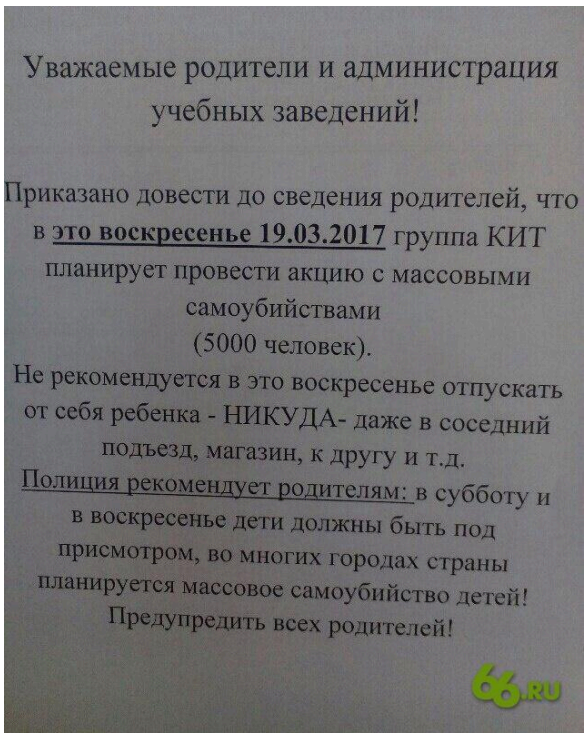

Рис. 5. Объявление о якобы массовом самоубийстве подростков

2) Ложные сообщения для придания вида достоверности наиболее часто ссылаются на мнимые авторитетные источники информации: «брат в полиции работает», «друг адвокат сообщил», «из управы позвонили» или просто «из достоверных источников» (см. рис. 6). Редко злоумышленники указывают данные людей, от которых якобы получена информация. Так, на рисунке 7 представлен пример сообщения, в котором указывается конкретное лицо. При этом, однако, место работы скорректировано таким образом, чтобы не было привязки к конкретному городу (в данном случае выполняется правило под пунктом 1), а Кировские районы, опять-таки, имеются во многих крупных городах России. В данном случае социальные хакеры указали данные настоящего сотрудника Кировского территориального управления департамента по образованию администрации города Волгограда. Видимо, расчет был на то, что люди не станут самостоятельно искать контакты данного человека и перепроверять информацию «из первых уст». А ссылка на настоящего человека, и ее настоящая должность должны были придать достоверности дезинформации. Однако представители СМИ и более ответственные в плане информационной культуры родители все же связались с данной сотрудницей, благодаря чему масштабы распространения «фейка» удалось снизить.

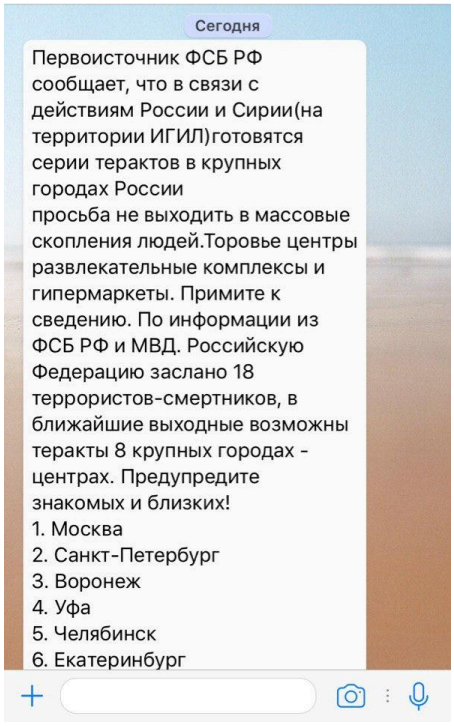

Рис. 6. Ложное сообщение со ссылкой на «достоверный» источник

Рис. 7. Сообщение с ложной ссылкой на настоящего человека

3) Поскольку задачей социальных хакеров является воздействие на чувства, ощущения человека, то распространяемые ими сообщения отличаются повышенной эмоциональностью (что подчеркивается использованием эмоционально окрашенных терминов: «ужасно», «страшно подумать», а также «срочно», «внимание» и т.п.; использованием заглавных букв, особых шрифтов, смайликов и стикеров), воззванию к благородным чувствам («от нас не убудет…») или страху («ни в коем случае не открывайте…») и т.п. (см. рис. 8).

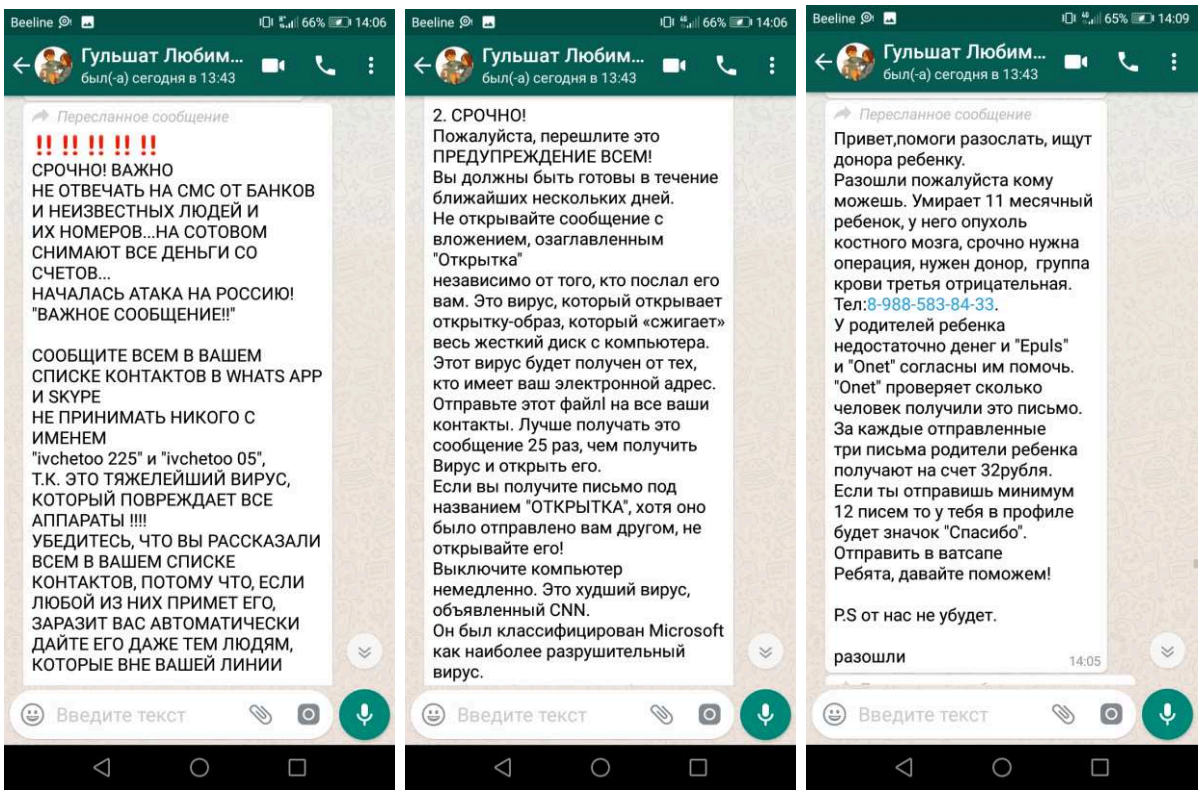

Рис. 8. Примеры эмоциональной окраски ложных сообщений

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 этом заключается слабое место социального хакинга – при ответственном отношении людей к получаемой информации и проверке ее достоверности распространение ложных сообщений потеряет свою эффективность как инструмент информационной войны.

5) При спокойном и внимательном прочтении можно обнаружить и некоторые другие признаки подложности сообщения: явная нереалистичность описываемых событий (например, так было с дезинформацией о якобы бегстве Эльвиры Набиуллиной за границу вместе с золотовалютным резервом страны. Достаточно представить, что такое золотовалютный резерв, чтобы идентифицировать лож), или несогласованность текста (так, на рисунке 9 представлен пример

сообщения, которое написано не обычным литературным или разговорным языком, а имеет признаки не очень качественного перевода на русский язык. В связи с этим можно предположить, что автор такого сообщения находится за границей, а описываемое событие не имело место в действительности).

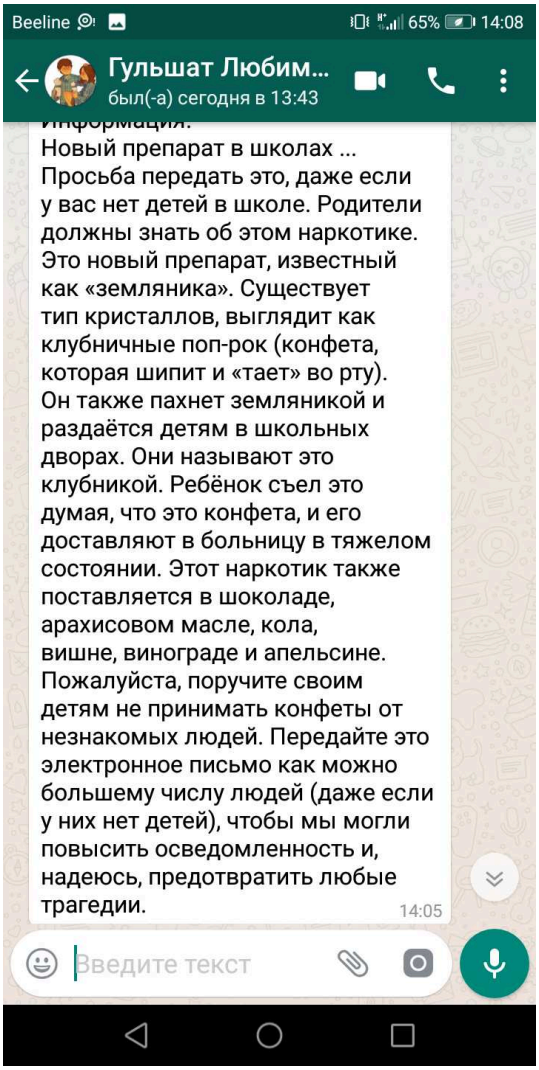

Рис. 9. Пример ложного сообщения, имеющего признаки перевода с иностранного языка

Таким образом, знание характерных особенностей распространения ложных сообщений и их индикаторов предоставляет возможность создания надежного заслона на их пути, выработки конкретных мер противодействия им и устранения условий, благоприятствующих их широкому тиражированию.

3. Пути противодействия деструктивному социальному хакингу в социальных сетях и мессенджерах

Публичное распространение ложной информации явление далеко не новое. 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».

Как видим рассматриваемое деструктивное явление известно уже несколько столетий. И уже в тот период люди с большей или меньшей эффективностью, но 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.

Указанное емкое определение «non testatum» раскрывает как суть ложных сообщений, так и указывает на основной способ противодействия им. Чтобы не допустить распространения не проверенного, не подтвержденного сообщения, его нужно проверить. Первичная проверка полученного сообщения начинается с его восприятия, анализа, оценки по наличию имеющихся в нем индикаторов, приведенных нами в предыдущем параграфе. Следует подчеркнуть, что сам процесс вдумчивого, критичного

[1] См.: Non testatum, или откуда в медийный поток прилетают «утки» / Текст: электронный // Гродзенская правда. – 11.04.2018 – URL: grodnonews.by/category/zhizn/news42434.html (дата обращения: 11.02.2020).

прочтения полученного сообщения, а не его моментальная пересылка под воздействием эмоций, решает задачу выявления лжи едва ли не наполовину.

Наличие в сообщении приведенных нами индикаторов не указывает однозначно на его ложность, хоть и свидетельствует о высокой вероятности этого. Для более тщательной проверки сообщения есть простой способ, многократно описанный на сайтах гражданских активистов вроде «Лиги безопасного интернета» или «Молодежной службы безопасности»[1]. Необходимо в поисковой строке любого браузера напечатать какую-либо короткую фразу в точном соответствии с проверяемым сообщением. Лучше для этого выбирать фразу, где содержатся ключевые или особенные слова. Так, например, при проверке нами сообщения о конфетах с наркотиками, оказалось достаточно 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, в результатах поискового запроса можно будет увидеть либо, что такое же сообщение уже пересылалось в разных городах и в разное время, либо статьи прямо указывающие, что данное сообщение очередной «фейк».

В случае, если ложное сообщение новое и в результатах поискового запроса не определяется, следует вдуматься в его смысл и 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

[1] См.: Наркотик земляника меф клубника конфеты – Текст: электронный // Молодежная служба безопасности : [сайт]. – URL: http://molbez.ru/anti-fakes/history24.html (дата обращения: 10.02.2020).

манипуляциях, если реальное и объявленное количество жертв и так было значительным. Тем более, что если бы такое уменьшение количества жертв имело бы место, то родственники погибших (пропавших) людей могли бы быстро составить собственный список и опровергнуть официально озвученные данные.

Ну и наконец, если поступившее сообщение, которое необходимо проверить, касается каких-либо криминальных событий, то можно обратиться с вопросом в органы внутренних дел, например к участковому уполномоченному полиции. Именно так поступают добросовестные средства массовой информации, прежде чем публикуют новости на своих ресурсах.

Как видно, алгоритм проверки информации и идентификации ложных сообщений совсем не сложный. Однако проблема сегодня заключается в низкой информационной культуре в обществе, отсутствии критического мышления. Гораздо чаще тысячам, десяткам и сотням тысяч людей проще нажать несколько кнопок или сделать движений и разослать сообщение, сделать репост, чем утруждать себя проверкой его достоверности. 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 общества, обучение населения выявлению (идентификации) ложных сообщений, их проверке. Это позволит создать надежный заслон на пути их распространения, а значит, этот вид информационного воздействия потеряет свою эффективность.

Одним из способов повышения информационной культуры и грамотности населения представляется проведение выступлений в школах, вузах, трудовых коллективах с лекциями на данную тему. Так, авторы

настоящего исследования провели такое выступление перед школьниками старших классов одной из общеобразовательных школ города. В результате данного выступления 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 емком 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, опубликования в СМИ и сети Интернет памяток по проверке и выявлению ложных информационных сообщений.

Следующим шагом повышения информационной культуры должно стать включение в этот процесс тех людей, которые уже научились не поддаваться воздействиям социальных хакеров. То есть противодействие распространению ложных сообщений должно использовать те же сетевые алгоритмы, что и само распространение. Это будет происходить, 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-банеер или демотиватор, показывающие, что нельзя беспечно относиться к информации.

Когда мы видели в группах ложные сообщения, мы проверяли их достоверность, отправляли опровержение сообщения и прикрепляли ссылку на материал, подтверждающий ложность данного сообщения. Однако, как показал опыт, простого опровержения бывает не достаточно, чтобы научить людей самим анализировать сообщения, прежде чем переслать их. Из наших опровержений люди узнавали о ложности конкретных сообщений, но продолжали вновь и вновь пересылать новые «утки». Тогда мы разослали по группам инструкцию по проверке пересылаемых сообщений, а когда кто-либо присылал очередную «утку» задавали приславшему ее вопрос: «Информация проверена?», «Вы проверили достоверность этих сведений?». Как правило, люди отвечали в таких случаях: «Я просто переслал(а)», «Я только хотел(а) помочь» и т.п. После этого мы отправляли опровержение и ссылку на подтверждающие это материалы. Такой подход оказался гораздо эффективнее и количество пересылаемых «фейков» уменьшилось в разы. Участники групп стали более ответственно относиться к отправке пересылаемых сообщений хотя бы потому, что в случае отправки ложного сообщения им будет неудобно перед другими участниками группы.

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

размещаться ими в социальных сетях и мессенджерах в ответ на очередное ложное сообщение социальных хакеров (см.: рис. 10).

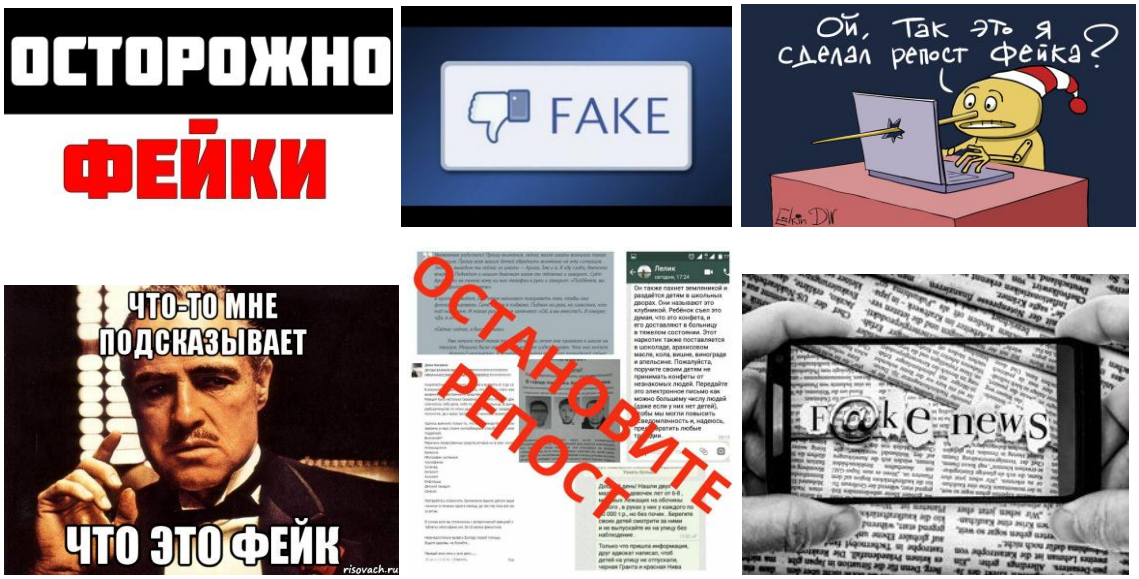

Рис. 10. Примеры простых баннеров и демотиваторов для ответов на ложные сообщения в социальных сетях и мессенджерах

Следующим направлением 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.

Также для устранения благоприятных условий для социального хакинга, предлагается сотрудникам органов внутренних дел (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 стороны, предоставит сотрудникам органов внутренних дел источник получения и распространения информации, что повысит эффективность и оперативность их работы.

Так, например, можно вспомнить пересылаемое в нескольких городах России сообщение о банде педофилов (см.: рис 11). При наличие 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 увидят все участники группы, а значит пересылка «фейка» тут же прикратится.

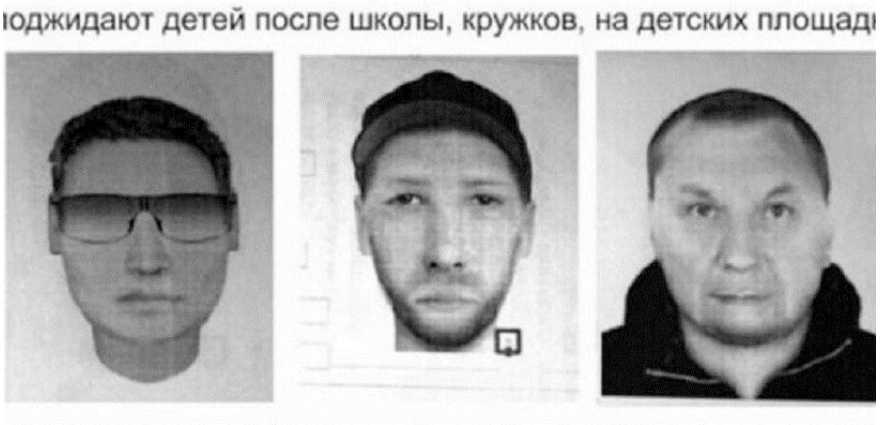

Рис. 11. Ложное сообщение о розыске банды педофилов

При этом следует подчеркнуть, что в указанных группах со стороны органов внутренних дел должна распространяться исключительно только та информация, которая предназначена для открытого опубликования. Так, например, с целью взаимодействия с обществом Министерством внутренних дел России создана группа в социальной сети «ВКонтакте». В плане противодействия социальному хакингу этот положительный опыт целесообразно расширять. Как дополнительное преимущество это будет способствовать 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.

Подводя итог 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 частности, 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 и это 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 будет выделять гранты для «содействия укреплению принципов журналистской этики в России»[2] и о том, что на территории Украины действует британское спецподразделение – 77 бригада, выполняющая военные задачи в Интернете, оказывающая психологическое воздействие и проводящая информационные операции[3], к вопросам противодействию социальному хакингу и другим информационным угрозам необходимо подойти комплексно, системно и широко, активно привлекая к этому широкие слои населения и в первую очередь молодежь. В противном случае ущерб от возможных информационных атак может оказаться огромным. Ведь, как справедливо отметили активисты проекта «Время Вперет», сегодня мы еще так и не нашли противоядие даже против самых примитивных методов дезинформации.

---

[1] Готовится новый инфоудар по России – Текст: электронный // Sonar2050 : [сайт]. – URL: https://youtu.be/tC9pn0hCwMU (дата обращения: 10.02.2020).

[2] В США намерены содействовать «укреплению принципов журналистской этики» в России – Текст: электронный // RT : [сайт]. – URL: https://russian.rt.com/world/news/579442-ssha-rossiya-zhurnalistika-grant (дата обращения: 10.02.2020).

[3] Публичность – самая страшная беда: чем занимаются сотрудники британской «фабрики троллей» на Украине – Текст: электронный // Федеральное агентство новостей : [сайт]. – URL: https://riafan.ru/1128331-publichnost-samaya-strashnaya-beda-chem-zanimayutsya-sotrudniki-britanskoi-fabriki-trollei-na-ukraine (дата обращения: 10.02.2020).

Заключение

Подводя итог настоящего исследования можно сделать следующие основные выводы:

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

2. Эффективным, опасным и часто применяемым в современном обществе инструментом информационной войны является социальный хакинг.

3. Проанализированные примеры социального хакинга позволили выявить индикаторы ложных сообщений на основании которых возможно их идентифицировать, а также выработать правила (порядок) проверки контента на достоверность.

4. Противодействие социальному хакингу возможно путем развития информационной культуры и грамотности населения, развития ответственного отношения к информации, а также путем использования органами внутренних дел таких средств коммуникации, как социальные сети и мессенджеры, в позитивных целях.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

I. Нормативные правовые акты

1. **Российская Федерация. Указы.** Об утверждении Стратегии национальной безопасности Российской Федерации : указ Президента Российской Федерации от 31.12.2015 № 683 // URL: http://pravo.gov.ru/ (дата обращения: 15.02.2020).

II. Литература и Интернет-ресурсы:

1. Non testatum, или откуда в медийный поток прилетают «утки» / Текст: электронный // Гродзенская правда. – 11.04.2018 – URL: grodnonews.by/category/zhizn/news42434.html (дата обращения: 11.02.2020).

2. В США намерены содействовать «укреплению принципов журналистской этики» в России – Текст: электронный // RT : [сайт]. – URL: https://russian.rt.com/world/news/579442-ssha-rossiya-zhurnalistika-grant (дата обращения: 10.02.2020).

3. Готовится новый инфоудар по России – Текст: электронный // Sonar2050 : [сайт]. – URL: https://youtu.be/tC9pn0hCwMU (дата обращения: 10.02.2020).

4. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие : в 2 ч. / [А. В. Аносов и др.]. – М. : Академия управления МВД России, 2019. – Ч. 1. – 208 с. – ISBN 978-5-906942-87-6. – Текст : непосредственный.

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

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

7. Наркотик земляника меф клубника конфеты – Текст: электронный // Молодежная служба безопасности : [сайт]. – URL: http://molbez.ru/anti-fakes/history24.html (дата обращения: 10.02.2020).

8. Публичность – самая страшная беда: чем занимаются сотрудники британской «фабрики троллей» на Украине – Текст: электронный // Федеральное агентство новостей : [сайт]. – URL: https://riafan.ru/1128331-publichnost-samaya-strashnaya-beda-chem-zanimayutsya-sotrudniki-britanskoi-fabriki-trollei-na-ukraine (дата обращения: 10.02.2020).

9. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. – СПб.: БХВ-Петербург, 2007. – 368 с. : ил. – ISBN 5-94157-929-2. – Текст : непосредственный.

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

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

12. Libicki, Martin C. What Is Information Warfare? / Martin C. Libicki. – Washington : Center for Advanced Concepts and Technology Institute for National Strategic Studies, 1995. – 104 p. – Текст : непосредственный.

13. Искусство обмана / Кевин Д. Митник, Вильям Л. Саймон [пер с англ.: А.А. Груздев, АВ. Семенов]. – М.: ДМК Пресс, 2006 – 124 с. – ISBN 5-98453-011-2. – Текст : непосредственный.