Федеральное государственное образовательное бюджетное учреждение высшего образования

«Финансовый университет при Правительстве Российской Федерации»

(Финансовый университет)

Факультет информационных технологий и анализа больших данных

(наименование факультета)

Департамент «Информационная безопасность»

(наименование департамента/кафедры)

Выпускная квалификационная работа

на тему: «Информационная безопасность личности в условиях сетевой коммуникации(на примере соц.сетей Вконтакте,Facebook,Instagram)»

Направление подготовки 10.04.01 Информационная безопасность

(код и наименование направления подготовки)

Безопасность автоматизированных систем в финансово банковской сфере

(наименование направленности)

Выполнил студент учебной группы

ИБ17-2

(номер учебной группы)

Качура Никита Сергеевич

(фамилия, имя, отчество полностью) (подпись)

Руководитель д.ф.-м.н., проф.

(ученая степень и/или звание)

Крылов Григорий Олегович

(фамилия, имя, отчество полностью) (подпись)

Руководитель Департамента/ Заведующий кафедрой

к.ф.-м.н., профессор

(ученая степень и/или звание)

В.Г. Гисин

(подпись) (И.О. Фамилия)

« » 2020 г

Москва - 2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....2

Глава 1. Теоретические основы информационной безопасности личности в сетевой коммуникации.....4

1.1 Информационная безопасность: сущность и особенности феномена.....4

1.2 Сетевая форма коммуникации как фактор развития информационных угроз.....12

Глава 2. Информационные угрозы и способы защиты от них в контексте коммуникативных практик молодёжной аудитории социальных сетей.....18

2.1 Общая характеристика молодёжной аудитории социальных сетей.....18

2.2 Классификация информационных угроз в сетевой коммуникации.....24

2.3 Распространенные типы информационных угроз личности в сетевой коммуникации и способы защиты.....32

Глава 3. Комплексная защита личности от информационных угроз личности в сетевой коммуникации и способы защиты.....38

3.1 Определение сущности и характера информационных угроз.....38

3.2 Алгоритм действий по обеспечению безопасности.....40

3.3 Технические и социально-правовые способы защиты от информационных угроз в сетевой коммуникации.....44

ЗАКЛЮЧЕНИЕ.....49

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ.....53

ВВЕДЕНИЕ

Появление и внедрение новейших технических устройств, работающих на основе сетевой логики, принудительно инициировало эволюцию многих форм социальной активности. Особенно весомое влияние данные процессы повлияли на сферу сетевой коммуникации, способствуя появлению более простых инструментов взаимодействия между пользователями и сетевыми факторами.

Однако наряду с огромным количеством выгодных и продуктивных решений, основанных на свободном доступе и обмене информацией с участниками любых возрастных, гендерных, социальных, национальных групп, своё развитие получили также различного рода деструктивные процессы, как информационные атаки, информационный терроризм, хищение данных, сокрытие и искажение информации. Эти феномены стали объектом активных дискуссий и исследований в научных кругах, задавая курс на актуальную проблематику, связанную с минимизацией и ликвидацией информационных угроз, защитой информационной безопасности личности и особенностями сетевой коммуникации.

Широкое обсуждение в научном дискурсе получили такие темы, как информационная безопасность общества, информационные войны, манипуляции и скрытое принуждение, психологическая безопасность личности в интернет-пространстве. Современные научные исследования, как правило, охватывают большую сферу вопросов, позволяя изучать особенности современных информационных угроз со всех сторон.

Информатизация общества навязала современному миру свои правила. С одной стороны люди получили доступ к нескончаемому потоку информации, который открывает двери на совершенно новые уровни познания и усваивания новейших данных, с другой же, человечество просто неспособно фильтровать полезную информацию от «токсичной» и «неправильной» в таком объёме, в котором она поступает. Таким образом можно сделать несложный вывод, что с

наступлением цифровой эры, человечество получило как огромный прирост в функциональном и информационном плане, так и огромный ворох проблем, связанных с непрерывным развитием информационной среды.

К положительным факторам можно отнести массовое отторжение унификации и стандартизации – каждый член общества стал волен проявлять себя в тех областях в каких он непосредственно был заинтересован, стерлись границы и появилась возможность легко найти единомышленников, где каждый индивидуум мог легко выражать свое субъективное мнение по любому вопросу.

Благодаря огромному информационному потоку, человечество получило инструментарий для быстрого принятия решений – если раньше требовалось как минимум быть подкованным в конкретной теме, сейчас же достаточно пары интернет- запросов, для принятия решения в важных вопросах.

К неоспоримым плюсам информатизации можно так же отнести и развитие, и рост всех видов интернет потребностей у населения, за счет доступности и многообразия видов интернет- досуга.

В информационном обществе неостановимо изменился приоритет ценностей, а с ними и обычный уклад жизни. Как пример если раньше люди с ограниченными возможностями могли только положиться на близких людей, теперь они могут зарабатывать деньги и обеспечивать себя сами. Благодаря тому насколько информационное пространство стало комфортным для конечных пользователей, оно несет собой прогрессивное развитие общества и в большей степени способствует его развитию, однако в некоторых ситуациях оно способно влиять негативным образом.

Как пример с развитием технологий остро встала проблема манипулирования сознанием людей, современные масс медиа способны влиять на взгляды людей, выставляя любые события под тем светом, каким им или тем, кто стоит за ними более выгодно.

Так же не стоит забывать и о преступлениях, с ростом информционного пространства выросло и количество так называемых киберпреступлений, которые несут собой очень негативный осадок как для обычный пользователей так и для государства, общества в целом. Помимо этого, с развитием информационных технологий стала актуальна проблема адаптации определенных категорий людей к новой среде. Так, в частности, огромное количество преподавателей и учителей, которые в силу своего возраста не были способны к такой радикальной перестройке существующего уклада и были вынуждены покинуть свои должности. Эта проблема так же не обошла стороной и пожилое поколение. Неспособные в полной мере освоить информационные технологии, данная категория людей стала наиболее подвержена негативному влиянию киберпреступлений, кибермошенничеству и шантажу со стороны преступников.

Объектом исследования является феномен информационной безопасности личности в сетевой коммуникации

Предметом исследования выступает информационная безопасность личности в рамках коммуникативных практик, реализуемых молодёжной аудиторией интернет-площадок международных социальных сетей.

Цель исследования: изучить способы обеспечения информационной безопасности в условиях сетевой коммуникации в социальных сетях

Для достижения цели исследования необходимо решить следующие задачи:

1. Изучить молодёжную аудиторию социальных сетей и дать им общую характеристику
2. Проанализировать угрозы и способы защиты от них контексте коммуникативных практик молодёжной аудитории социальных сетей

3. Предложить план по обеспечению комплексной защиты личности от информационных угроз, а также выявить основные способы защиты от информационных угроз в сетевой коммуникации.

Выпускная квалификационная работа состоит из 60 страниц машинописного текста, содержит рисунков - 4, список использованных источников составляет 40 наименований.

Глава 1. Теоретические основы информационной безопасности личности в сетевой коммуникации

1.1 Информационная безопасность: сущность и особенности феномена

Появление информационных технологий кардинальным образом воздействовало на представление о коммуникационных способностях человека. С каждым годом появляется все более и более новых возможностей, которые в настоящее время еще не до конца изучены. Ход глобализации непосредственно объединён с информационным пространства, какое на сегодняшний день все глубже уходит в виртуальную сферу и тесно связано с современными информационными технологиями. Любой пользователь глобальной сети попадает в огромную и нескончаемую «реку» информации. Начинает погружаться все глубже, впитывая в себя информацию. Однако, в любой реке есть камни и камни и камнями информационной реки являются системы массово контроля и цензура в глобальной сети. Именно появление глобальной информационной сети с открытым доступом определило новую проблему безопасности личности в целом – информационную безопасность. [19]

На сегодняшний день мы люди пытаемся получить доступ к большему объёму информации и экстраполировать её в своих интересах. На фоне этого вполне очевидно свою нишу заняли социальные сети, как нескончаемые источники информации и удобнейший ресурс для навязывания своего мнения. Конечному пользователю необходимо научится прокладывать себе путь через нескончаемые потоки информации, чтобы в конечном итоге получить интересующие его знания.

Глобальные информационные технологии заметным образом изменили привычные всем методы изучения и изменения информации. Человечество получило в свои руки инструменты и системы для межсетевого общения который облегчили коммуникацию и перевернули привычное общение как таковое. Раньше требовалось купить условную газету, чтобы получить сводку последней информации о происходящем в мире, сейчас же достаточно просто

зайти на главную любого браузера. Чтобы встретится и пообщаться с другим человеком раньше требовалось заранее договорится о встрече или позвонить по телефону, сейчас достаточно обычного сообщения в любой социальной сети, или видеозвонка. Исходя из этого один из самых популярных сервисов глобальной сети, который широко представлен в современных сетях являются популярные ныне социальные сети.

Впервые понятие социальных сетей в реальном мире ввел Дж. Барнс в 1954 г. Он определял их как социальное поле, в рамках которого люди являются друзьями или просто знакомы друг с другом. [5] Похожее определение было дано в 1987 г. психологами М.С. Денофф и П.А. Пилконис, которые определили социальную сеть как набор межличностных отношений, связывающих людей. [17]

В социальных сетях правдивость и реальность информации устанавливаются за счет реальных знакомств между людьми, которые входят в это самое сообщество и знакомы друг с другом за пределами социальных сетей. В таких сообществах все участники следуют правилам установленными админами и руководителями данной сети.

Социальные сети — это своего рода отголосок виртуального мира, он подчиняется тем же правилам и имеет ту же конструкцию. Если говорить проще, то социальные сети можно описать набором конкретных свойств, формирующих настроение и поведение всех участников сети, а именно неочевидность, безответственность и безнаказанность любых источников информации.

Как и любая популярная вещь социальные сети были обречены на огромный успех, что в конечном итоге закрепила их на пьедестале лидеров в интернет-среде. Однако они все так же имеют ворох проблем, которые используют определенные лица и владельцы сетей себе на благо.

Социальные сети по своей конструкции делятся на 3 категории, а именно:

-открытые;

-закрытые(корпоративные);

-условно открытые;

По направленности социальные сети могут быть: узкотематические, полемические, информационные и т.п. Одна из самых важных составляющих, непосредственно влияющих на жизнеспособность сети является её экономическая составляющая. То есть кто получает выгоду от её эксплуатации:

-владелец виртуального пространства;

-владелец сайта;

-участники сети (опосредственную, в случае открытой и условно открытой сети и непосредственно участники закрытой сети);

-группы людей, заинтересованных в реализации информационного воздействия:

Однако, кроме людей в социальных сетях можно найти и много различных сообществ, представляющих конкретные фирмы и организации из реального мира. Это продиктовано тем, что в современном обществе проще всего воздействовать на многомиллионную аудиторию через лидеров мнений, которые в большом достатке обитают в социальных сетях. Они помогают сформировать положительное мнение о продукте, навязывать молодой аудитории свою точку зрения, и просто вынудить приобрести продукцию рекламодателя.

Одним из самых эффективных способов воздействия на целевую аудиторию в социальных сетях является предоставление информации, восхваляющей или порочащей какой-либо товар, услугу или даже человека. Данный прецедент принято называть инфо-поводом. Иногда такие средства становятся откровенной информационной ложью, которая в свою очередь наносит сильный ущерб имиджу человеку, товара или услуги. Однако, такие действия попадают под нарушение 7 статьи 152 ФЗ «О персональных данных»: Операторы и иные лица, получившие доступ к персональным данным, обязаны

не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом [1].

На сегодняшний день множество людей, не может даже представить своей жизни без социальных сетей. Утро такого человека будет начинаться не с какой-либо физической активности, а с просмотра новостных лент и общения с друзьями. Люди становятся зависимы от общественного мнения и социальных сетей, в частности. Социальные сети сопровождают человека на протяжении всего дня с момента пробуждения, до того момента как человек ляжет в кровать. В такой ситуации человек почти полностью теряет контроль над собственной жизнью. Им движет не желание к саморазвитию, а желание быть лучше остальных, показать, насколько он уникален и насколько его жизнь ярка и необычная, хотя зачастую это лишь грим и декорации. Человек теряет возможность трезво оценивать свою жизнь, ему необходимо что общество делало это за него посредством комментариев. В погоне за статусом человек теряет понимание о рамках приличия, дозволенности и безопасности.

С другой же стороны, социальные сети помогают человеку избавиться от одиночества. Здесь он может пообщаться с людьми, которых никогда не знал в жизни, он активно включается в коммуникацию между личностями. Однако, при это реально общение замещается виртуальным. Люди уходят в виртуальный мир, что приводит к трагическим последствиям, которые не решить без помощи специалиста, это превращается в реальное заболевание.

Социальные сети активно влияют на процесс коммуникации, в результате чего, отношение людей к окружающему миру изменяется, деформируется. Чувство нарциссизма противопоставляется семейным и национальными связям пользователя. Этот процесс, по мнению антрополога Ш. Теркл, включает в себя:

-исчезновение одиночества как части процесса социализации;

-зависимость от социальных сетей и гаджетов, обеспечивающих непрерывный процесс «виртуальной коммуникации» в ущерб «традиционны» социальным практикам общения;

-исчезновение причастности в региональной культуре;

-зависимость от гаджетов, часто западного производства;

-деформация процесса общения;

-отчуждения в семье;

-деформация языкового общения;

-формирование новой этики;

-потенциальное разрушение личного пространства;

Особенно подвержены влиянию социальных сетей дети и подростки. Они прикованы взглядами к своим кумирам и вторят их действиям и мышлению не задумываясь о том к чему может привести такого рода мышление, как пример мы можем увидеть влияние запрещенной на территории РФ организации «ФБК» на разум и сознание детей, они не пытаются и не хотят анализировать реальную ситуацию в стране, а просто по призыву, как марионетки выходят на улицы и скандируют опасные лозунги не задумываюсь что нарушают общественный порядок и спокойстве людей. Они не бояться ничего ни органов власти, ни своих родителей, они просто не понимают что то что они делают опасно и это лишь внедренная в их мысли идея, идея которую вложил в них интернет кумир.

На сегодняшний день в социальных сетях особенно активно проходят различные информационные кампании, которые нацелены на создание положительного образа на конкретные информационные события по актуальным экономическим, политическим, социальным и другим вопросам. Благодаря социальным сетям появились и продолжают появляются все новые инструменты воздействия на человеческое сознания и другие инструменты манипуляции над ним, коих в современном мире уже с избытком.

С точки зрения информационной безопасности пользователей социальных сетей, очень важно, в какой стране располагаются серверы, на которых хранятся данные о пользователях, и кто является непосредственным владельцем социальной сети. Например, серверы сетей Facebook, LinkedIn, MySpace, Instagram расположены в США; Одноклассники, Мой Круг, Вконтакте – В России. Существуют сети, которые принадлежат конкретным странам: Германии, Израилю и другим и в каждой располагаются сервера с конфиденциальной информацией пользователя, его личными переписками и т.д.

Социальные сети создаются физическими или юридическими лицами, и принадлежность к той или иной стране естественно условна. При регистрации в социальной сети от пользователя требуется лишь подписать пользовательское соглашение и ничего более. Нет необходимости верифицировать свою личность и вносить каки либо паспортные данные. Из этого вытекают как положительные, так и отрицательные тенденции. С одной стороны человек получает полную свободу слова, почти полную безнаказанность за публикацию тех или иных высказывания и точек зрения, с другой же открывает свободу для публикации экстремистских сообщений, призывов к террористическим актам и т.д. Помимо этого владельцы социальных сетей нередко в пользовательском соглашении оставляют для себя лазейки, позволяющие им свободно собирать и передавать личную информацию пользователей и передавать её рекламодателям. Наверняка каждый из вас сталкивался с таким феноменом : вы со своим другом обсуждали какой то продукт в котором вы заинтересованы и хотели бы приобрести, и вот во всех рекламных окнах начинает появляться именно этот продукт, знакомо, не правда ли?

Таким образом в руках у владельцев данных ресурсов содержится колоссальный инструмент для анализа социальной структуры общества или отдельной личности. Не редко случается и то, что личные данные пользователя

продаются третьим лицам, так как пользовательское соглашение не запрещает этого.

Можно понять точку зрения тех людей, что заходят в социальные сети чтобы найти группу единомышленников по интересующих их темам. Человек — это социальное существо, которому необходимо общественное общение в любых проявлениях. Социальные сети в свою очередь предоставляют возможность высказываться на интересующие нас вещи анонимно, что открывают двери людям, с опаской оглядывающихся на большие скопления людей(интровертов) и прочих типов личностей к свободному самовыражению.

Из предоставленного выше, мы можем сделать вывод, что социальные сети имеют уйму негативных черт, которые могут легко подорвать психическое здоровье человеку и даже вынудить его на поступки, которые в отсутствие социальных сетей он вряд ли бы осуществил. Угрозы, исходящие от сетевого коммуникативного пространства, принято называть информационными. Их обычно рассматривают в контексте проблемы обеспечения информационной безопасности, которая в российских нормативно-правовых актах определяется как состояние защищенности информационной среды и деятельность по предотвращению утечки защищаемой информации, по защите от несанкционированных и непреднамеренных воздействий на нее.[9,10] Соответственно, информационная безопасность личности определяется как состояние сохранности информационных ресурсов личности и защищенности законных прав в информационной сфере.

В нормативно правовых актах преобладает понимание информационной безопасности в ее техническом и правовом аспектах. Как правило, она трактуется как защита конфиденциальности (обеспечение доступа к информации только авторизированным пользователям), целостности (обеспечение достоверности и полноты информации и методов ее обработки) и доступности (обеспечение доступа к информации и связанным с ней активам авторизированных пользователей по мере необходимости) информации.[1] Но в юридических

документах в наибольшей степени находит отражение аспект, связанный с защитой программного обеспечения и обеспечением безопасности связи (коммуникации).

Однако существующая защищенность информационных ресурсов не гарантирует личности его информационной безопасности. Из-за недозволенности существует огромная прослойка людей разово или нет попадавшие под влияние киберпреступников посредством шантажа и т. п. Они не обладают базовой информации о защите своего личного информационного пространства и попадаются на различные уловки, как пример каждый год в полицию обращаются огромное количество девушек и парней, которым злоумышленники отправили угрозу опубликовать их личные данные/фото/видео если они не переведут условную сумму на подставной кошелек. И с ростом пользователей социальных сетей количество киберпреступников не идет на спад, а наоборот только растёт. Таким образом можно сделать вывод что отражение возникающих информационных угроз напрямую зависит об осведомленности пользователей о способах их отражения.

1.2 Сетевая форма коммуникации как фактор развития информационных угроз

Как уже говорилось ранее, наиболее опасными источниками угроз можно считать манипулирование сознанием человека посредством формирования вокруг него среды с измененным «более правильным» мнением, что приводит его к неизбежному следованию за новыми идеалами. Так же к отрицательным остаткам можно отнести информационную перегрузку личности. Если вкратце это происходит из-за возникновения у человека интернет-зависимости, вследствие чего человек начинает ощущать дефицит новой информации, межличностного общения и прочих видов потребностей, которые он никак не может утолить. В свою очередь это приводит к обесцениванию устоявшихся норм и правил привычной жизни.

Одним из наиболее опасных источников угроз для людей является использование его же персональных данных против него. Инструментарий социальных сетей позволяет с легкостью надавить на нужные рычаги и выставить любое лицо в необходимом свете.

К таким угрозам можно отнести публичную клевету, процедуру «удаления» очень популярную в США и странах западной Европы, когда какую-либо медийную личность, знаменитость, актера или любого мало-мальски знаменитого человека начинают массово травить в социальных сетях за какие-либо высказывания, которые он мог опубликовать несколько лет назад, ещё до становления той медиа личностью, которой он является сейчас. Помимо этого, к угрозам можно так же отнести прямые угрозы или распространение ложной информации о личности.

Сетевые коммуникации и сейчас обладают огромным инструментарием и предоставляют большие возможности для СМИ. В современном обществе большинство СМИ начало работать «на два фронта». Они комбинируют традиционные и современные медиа с целью привлечения большей аудитории. Посему в интернет-среде появляется такое огромное количество «Веб порталов» и Интернет-магазинов. Современное сетевое информационное пространство характеризуется медиа глобализацией. Их называют «новыми электронными медиа», для того чтобы отрезать их от привычных всем традиционным медиа: печати, радио, телевидения. [10]

Новые электронные медиа обладают почти безграничными возможностями передачи любой информации любым ее отправителем в различных направлениях, но медийные информационные потоки формируются в интересах владельцев транснациональных информационных агентств. Процесс монополизации на медиарынке приводит к угрозам манипулирования общественным мнением по отношению к тем или другим значимым событиям и, что еще более серьезно, к деформации моральных устоев общества, его национальной культуры путем навязывания ему чужих ценностей. Разумеется, сетевые коммуникации сами по себе являются просто эффективной технологией

для успешного развития бизнеса владельцев транснациональных информационных агентств. Западный бизнес не ставит своей целью разрушение нормативно-ценностной системы общества, но стремится распространить свои "правила игры", свою логику экономического, социального действия с тем, чтобы реализовывать коммерческие проекты в адаптивной для себя среде. Попутно глобальный медиарынок выполняет заказы, продиктованные ведущими геополитическими игроками. Ярким тому примером является мощная подача в информационных международных агентствах заведомо ложной информации о нападении России на Грузию в августе 2008 г.

Одной из самых распространенных групп угроз в современном обществе, можно без зазрения совести назвать киберпреступления. Они нацелены в основе своей на мошеннические махинации с использованием современных сетевых систем. Так же они служат для отмывания денег, полученных преступным путем, неправомерного использования финансовой, банковской информации и т.п.

Нет никаких сомнений, что социальные сети — это единственное место, хозяева которого если не напрямую нарушают установленные законом предписания, то занимают нейтральную позицию в правовом секторе. Это наглядно можно увидеть если обратить свое внимание на проблему авторских прав. На сегодняшний день в социальных сетях находится огромное количество пиратского и не нелицензионного контента, из-за которого обладатели прав интеллектуальной собственности находятся в не уделе. Однако только на этом противоречия между правом и сетевыми коммуникациями никак не останавливаются.

По данным аналитиков, число опасных Интернет-ресурсов за последнее время увеличилось в три раза. Эксперты по Интернет-безопасности утверждают, что сегодня атаки на ресурсы Всемирной паутины происходят каждые четыре с половиной минуты. Во многих странах отмечается увеличение объемов утечки данных, при этом только около 20% происходит из-за хакерских атак. По данным МВД, в 1 квартале 2020 года Количество IT-преступлений выросло на 83,9%, а

удельный вес таких деяний достиг 19,9% от общего числа. В основном из-за этого фактора уровень преступности в стране в целом вырос на 4%. [8]

Во Всемирной паутине сегодня существуют различного рода закрытые сети. Сетевые структуры эффективно используются организациями в условиях конспирации. Их главным козырем становится молниеносность распространения информации и новые возможности дистанционного управления террористическими актами. Террористические группы и мафиозные структуры используют нелегальные, полулегальные и криминальные методы политической борьбы, игнорируя правовые нормы и традиции, нарушая законы, расшатывая политический строй обществ.

Бесспорно опасный источник угроз в условиях сетевой коммуникации — это непрерывно разрастающееся влияние информационных войн и распространение информации, напрямую влияющее на сознание и мировоззрение людей. Информационные войны идут на всех уровнях и механизмы их работы практически всегда идентичны. У тех людей кто её ведут, остаются одни и те же рычаги давления на общественное мнение. Кто-то недосказывает часть информации и намеренно вызывает её дефицит, чем и подогревает внимание общественности. Кто-то в свою очередь наоборот давит на неудовлетворённость людей конкретной ситуацией или продуктом и заставляет активно противостоять и оппонировать ей. Существуют также методы ведения информационной войны на территории информационной среды противника с целью полной дезинформации и создания хаоса и паники посредством методов и технологий дающих воздействовать на информационную среду. И. Л. Морозов различает три вида информационно-психологического оружия относительно стратегии нападения:

1. Системы дистанционного искажения или уничтожения информации: компьютерные вирусы общего и специализированного назначения (программы, проникающие извне и разрушающие систему); логические бомбы, тайно внедряемые в компьютер на этапе заводской сборки, которые при активизации парализуют работу компьютера;

2. Системы хищения информации: электронные шпионы (программы, проникающие извне и производящие незаметный для пользователя сбор служебной и непосредственно личной информации);

3. Системы комплексного воздействия на психику пользователя: мультимедийные сайты в виде информационно развлекательных или аналитических страниц с "горячей", "сенсационной" информацией.

Существует мнение, что повышение уровня "прозрачности" и доступности информации для всех участников политического процесса (например, в случае проведения президентских и парламентских выборов) облегчает общественный контроль за ним со стороны общественности. Однако И. Л. Морозов выделяет два блока угроз, ведущих к подрыву политических режимов: системные и периферийные угрозы.

Первый тип угроз направлен на дестабилизацию конкретных политических систем или их сегментов со стороны враждующего государства и затрагивает в основе своей атаки на информационное поле оппонента с использованием информационно-психологических атак властных и околовластных структур

Не менее серьезную опасность представляют угрозы второго типа, которые связаны с деятельностью широкого спектра внесистемных сил - от международных террористических организаций до всевозможных хакерских групп. Неструктурируемость и непрогнозируемое возникновение периферийных информационных угроз крайне затрудняют выработку действенной защиты от них .

И. А. Василенко, анализируя состав политических факторов, различает их на носителей власти и внесистемную оппозицию . Сетевые пользователи, составляющие внесистемную оппозицию, делятся им на две группы - легальное "самобытное сопротивление", которое находит себе опору в традиционных и нетрадиционных ценностях сообщества, и на нелегальные криминально-мафиозные сети. Основной силой легального и нелегального сопротивления является исключительно сетевая, децентрализованная форма организации и

политических действий. Характерным примером такого сопротивления становится стремительно нарастающее движение антиглобалистов, которое строится на основе национальных и международных сетей, активно используется Интернет, и при этом сети не только обеспечивают организацию их деятельности, но и совместное использование информации.

Децентрализованный, неуловимый характер сетевых структур сопротивления антиглобалистов и других самобытных движений (экологисты, "зеленые", женские движения, различные молодежные субкультуры, представленные, в частности, в блогосфере) во многом затрудняет их восприятие и идентификацию со стороны государственного управления. "Новые гибкие сетевые структуры внесистемной оппозиции становятся сегодня главным козырем в борьбе с неповоротливыми институтами политической власти, которая в большинстве случаев имеет старую иерархическую организацию и только отдельные силовые подразделения в ней перестроены по сетевому принципу».

В конечном итоге я могу выделить основные категории информационных угроз, оказывающих свое влияние на общество, государство личность посредством сетевых коммуникаций.

- Угрозы безопасности личности, связанные с манипуляцией над сознанием и информационной перегрузкой человека, с непосредственным увеличением в информационную зависимость. Сюда же можно отнести и использования личных данных во вред личности, как пример сбор личных данных с целью внедрения таргетированной рекламы конкретному человеку.

-Угрозы, связанные с управлением и манипуляцией над общественным мнением, появлением особых механизмом управления массы людей с целью организации процессов направленных на разрушение привычных ценностей общества.

-Угрозы безопасности всех структур, на которые пытаются повлиять посредством международной преступности и терроризма.

-Угрозы стабильности существующих режимов власти, обусловленные неконтролируемыми всплесками высказывания и активизации опасной оппозиции в социальной и сетевой коммуникации.

Глава 2. Информационные угрозы и способы защиты от них в контексте коммуникативных практик молодёжной аудитории социальных сетей.

2.1 Общая характеристика молодёжной аудитории социальных сетей

Для анализа молодёжной аудитории в социальных сетях, необходимо определить понятие молодёжи и разграничить хронологический интервал представителей, которые относятся к данной группе. В науке существует множество подходов и мнений о понятии «молодёжь». Так, например, такие учёные, как В. Т. Лисовский, И.С. Кон, Р.В. Сергеев, Л.Я. Аверьянов затрагивал данный термин. Однако, подходы у учёных разные, они отличаются олицетворением и не олицетворение молодёжи с социализацией, особенной восприимчивостью сознания и мировоззрением. Помимо этого, многие учёные ограничивают возраст молодёжи 30 годами [13].

До конца 2020 года в законодательном плане хронологический интервал молодёжи (16-30 лет) сохранялся и был таким же, как и в науке. Однако 30 декабря 2020 Президент Российской Федерации Владимир Путин подписал новый федеральный закон, который вступил в силу 10 января 2021 года, «О молодёжной политике в Российской Федерации» №489. Помимо того, что Федеральный закон был создан для того, чтобы регулировать все возникающие взаимоотношения между субъектами молодёжной политики, в статье 2 Федерального закона закреплены расширенные рамки хронологического интервала. Так, нижняя хронологическая грань молодёжи стала равняться 14 годам, а верхняя повысила на пять лет и стала равной 35 годам [2].

В рамках государство такая мера важна так, как расширяется перечень лиц, которые могут претендовать на различные меры поддержки для молодых людей и семей. Однако, в рамках настоящей выпускной квалификационной работы это также важно так, как позволяет определить, каких пользователей считать молодёжной аудиторией и учитывать при сравнении социальных сетей между друг другом, а каких пользователей считать возрастной аудиторией.

Для проведения анализа молодёжной аудитории в три социальных сетях: ВКонтакте, Facebook и Instagram были использованы ежегодные материалы авторитетной компании Brand Analytics, а именно их исследование, которое посвящено анализу социальный сетей в России за 2020 год.

В результатах отражены 7 социальных сетей: Facebook, ВКонтакте, Instagram, Youtube, Twitter, Одноклассники и Tiktok. Однако, в рамках выпускной квалификационной работы акцент сделан на трёх основных, которые перечислены первыми в списке.

Поскольку социальные сети воспринимаются как медиа-ресурс и многие обращаются к социальным сетям, как к источнику актуальной новостной информации, пользователей социальный сетей можно рассматривать, как публичных авторов. Согласно данным компании Brand Analytics, в 2020 году каждый месяц на территории России вели свою деятельность в среднем 64 млн публичных авторов в социальных сетях. В среднем за один месяц 2020 года, аудитория социальный сетей получила доступ к 1,2+ млрд постов и комментариев, что является большим массивом неверифицированной информации [31].

Конечно, количество авторов и постов в социальных сетях разное – это связано с общем интересом к социальной сети и с распределенностью аудитории. Молодёжь, более активно воспринимает технологические изменения и, соответственно, в сети она более активна.

Однако, стоит также заметить и оценить корреляцию между количество авторов и публикуемым контентом. В 2020 года контента было опубликовано примерно столько же, сколько и годом раннее, а общее количество пользователей возросло более, чем на 25% - с 49 млн публичных авторов в 2019 года до 64 млн публичных авторов в 2020 году. Подробная история о количестве ежемесячных сообщений на всех площадках и количество ежемесячных авторов

представлена на рисунке 2.1, который отражает краткую выжимку результатов за 2020 год.



Рисунок 2.1. Исследование Brand Analytics по количество пользователей-авторов социальных сетей и количеству опубликованного контента [31].

Из анализа рисунка 1 можно сделать вывод о том, что ВКонтакте является самой популярной социальной сетью для авторов контента, хотя проигрывает социальной сети Instagram по количеству пользователей примерно в 1,5 раза. Сама же социальная сеть Instagram является самой популярной социальной сетью в России. Третья социальная сеть, которая будет проанализирована в рамках выпускной квалификационной работы, - Facebook, занимает 4 место, уступая Одноклассникам по количеству создаваемого пользователями контента и предпоследнее место по количеству пользователей, опережая только Twitter. Направленность социальных сетей на молодёжь является ключевой причиной того, почему одни социальные сети популярнее других. Так, например, социальная сеть ВКонтакте, является исторически «молодой», в которой основное количество пользователи представители до 35 лет. Перейдём к более детальному анализу трёх социальных сетей от самой крупной по количеству

пользователей-авторов, которые находятся на территории Российской Федерации, до более мелких.

В первом анализе были представлены данные по социальной сети Instagram, которые отражены на рисунке 2.2.

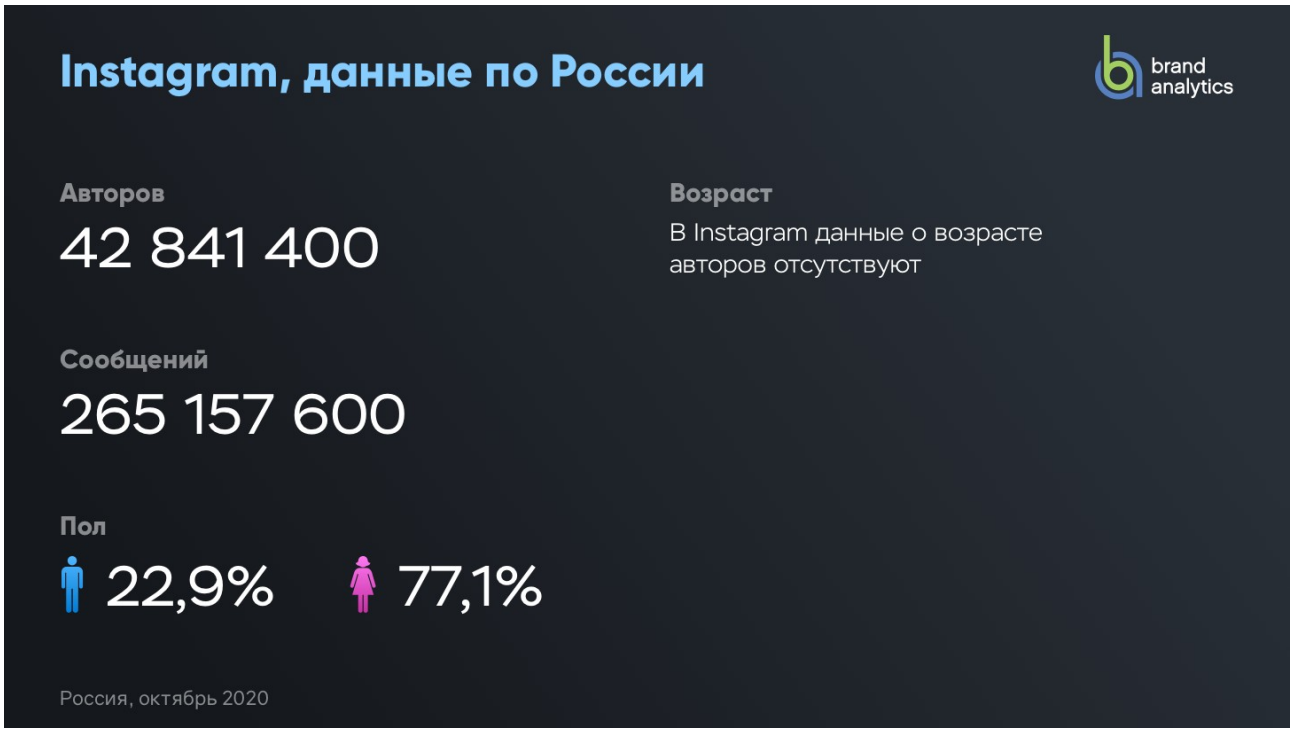


Рисунок 2.2. Аналитика аудитории социальной сети Instagram [31]

Социальная сеть Instagram набирает популярность на территории Российской Федерации, постоянно расширяя количество аудитории. Так, например, в 2019 году социальная сеть насчитывала 27,7 млн пользователей, а за год возросла более, чем на 50% до 42,8 млн публичных авторов на территории РФ. Сравнивая её с социальной сетью ВКонтакте, Instagram ещё пока проигрывает ВКонтакте по количеству контента, который производит аудитория. В Инстаграме показатель публикации на одного автора равен 6,2 публикациям в месяц. В социальной сети ВКонтакте данный показатель превышает в три раза. В общем, за один месяц в социальной сети Instagram производят 265,2 млн публикаций. Однако, социальная сеть не разглашает данные о возрасте аудиторий, что усложняет анализ. Однако, социальная сеть

считается молодёжной, и её главная аудитория является представителю молодёжи.

Далее была проанализирована социальная сеть ВКонтакте, результаты анализа которой представлены на рисунке 2.3.



Рисунок 2.3. Аналитика аудитории социальной сети ВКонтакте [31]

Социальная сеть ВКонтакте исторически считалась «молодёжной» социальной сетью, которая создаёт больше всего контента – почти 500 млн сообщений, постов, комментариев производят авторы платформы в месяц. В отличие от Instagram, ВКонтакте раскрывает информацию о возрастах пользователей, что позволяет проанализировать долю пользователей, которая относится к молодёжи. Поскольку в соответствии с новым Федеральным законом молодёжью считаются граждане до 35 лет, можно сделать вывод, что на платформе ВКонакте более 66,6% молодёжи. То есть из трёх людей, два точно будут представителями молодого поколения. Также стоит отметить, что из почти 29 млн пользователей аудитория разделились пополам между мужчинами и женщинами. Мужчин чуть более 45%, а женщин почти 55%. А сами молодые

авторы публикуют каждый почти по 17 единиц контента (посты, комментарии и т.д.) в месяц.

Последней проанализированной социальной сетью стал Facebook. Результаты анализа которого представлены на рисунке 2.4.

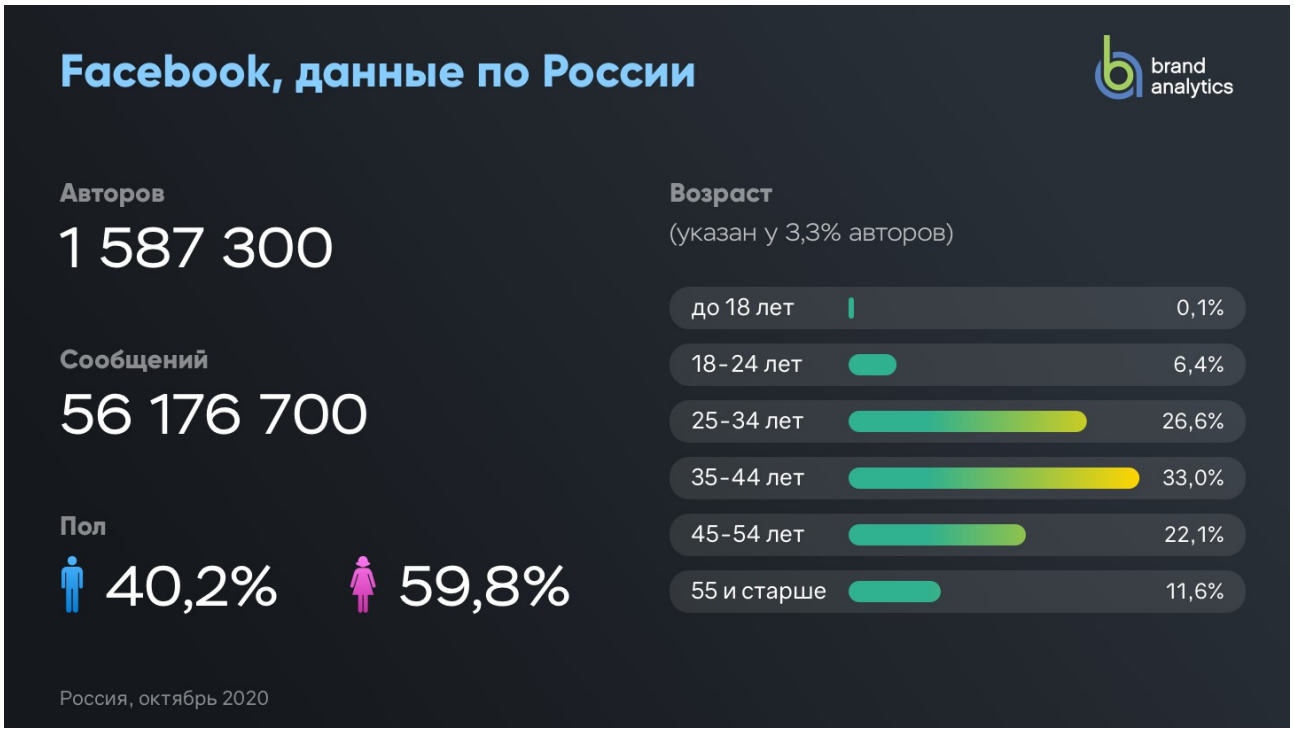


Рисунок 2.4. Аналитика аудитории социальной сети Facebook [31]

Социальная сеть Facebook не так популярна на территории Российской Федерации, как её аналог, ВКонтакте. Однако, возраст пользователей также является публичной информацией, что позволяет сделать некоторые выводы. В отличие от молодёжной сети ВКонтакте, Facebook является более возрастной социальной сетью. Всего лишь 33% аудитории являются молодёжью, то есть из трёх человек всего один. Здесь свою роль играет позиционирование социальной сети, как место «для профессионалов», что является непривлекательным для молодой аудитории. По соотношению мужчин и женщин, здесь также выигрывают женщин, опережая мужчин почти на 20%.

2.2 Классификация информационных угроз в сетевой коммуникации

Для создания классификации информационных угроз в сетевой коммуникации необходимо определиться в терминологии. Понятие

«информационная угроза» встречается в трудах многих авторов-теоретиков. Ученые используют различные подходы, которые описывают сложность термина и те деструктивные характеристики, которые в нём содержаться. По мнению А.А. Акмасова, информационная угроза – это некая возможность информационного воздействия, которая прерывает адекватное постепенное развитие личности с помощью того, что вносит изменения в собственных интересы и потребности личность для того, чтобы получить некоторую выгоду субъекту, который оказывает воздействие на личность [5].

В трудах учёного С.В. Вихорева также встречается определение информационной угрозы. К ней автор относится любую потенциальную или реально возможную опасность того, что произойдёт некоторое действие, которое способно причинить вред пользователю, который будет выражен для него в том, что информация, с которой он взаимодействует и к которой обращается, будет искажена, вовсе удалена или станет достоянием иных пользователей, которые изначально не имеют право на обращение к такой информации. С.В. Вихорев олицетворяет два понятия и связывает их: «информационная угроза» и «ущерб». По мнению ученого, любая информационная угроза несёт ущерб и доказать это можно через правовой аспект. Деятельность злоумышленника, который реализует информационную угрозу трактуется как преступление и доказываться через законы и уголовный кодекс [7].

Можно сделать локальный вывод о том, что информационная угроза неразрывна с некоторым ущербом и негативным воздействием на определенный субъект. Поскольку в рамках выпускной квалификационной работы рассматриваются сетевые коммуникации и информационные угрозы в сетевой коммуникации, то под субъектом негативного влияния понимается некоторая группа лица или отдельное лицо, которое действует злонамерено и заинтересовано в том, чтобы нанести вред объекту негативного влияния для того, чтобы стать обладателем некоторой материальной или нематериальной выгоды.

В свою очередь под объектом понимается участник сетевой коммуникации, который оказывается жертвой действия субъекта.

Информационные угрозы в сетевой коммуникации возможно классифицировать разными способами. Классификация всегда будет зависеть от базового критерия классификации, который ложится в основу для определения групп и выделения одних информационных угроз в сетевой коммуникации. Первая классификация в рамках выпускной квалификационной работы проведена по двум базовым критериям: психологические и технические аспекты информационных угроз для личности в сетевой коммуникации [16].

Под техническими угрозами будут пониматься вредоносные атаки, нацеленные на хищение, блокировку, искажение личной информации пользователя при помощи технических средств. К таким угрозам можно отнести все виды вредоносных программ: компьютерные вирусы, сетевые черви, троянские программы, логические бомбы, программы шпионы, кейлоггеры, рекламное обеспечение. Распространению таких угроз способствует незащищенное соединение, отсутствие защитных программ на персональных компьютерах, неполадки в системе, доступность для взлома, отсутствие способов защиты от нежелательных собеседников и другое [13].

Следует отметить, что в настоящее время популярные социальные сети оснащены надежными защитными механизмами, позволяющими блокировать вредоносные программы и предотвращать заражение пользовательских компьютеров. По этой причине технические угрозы в социальных сетях ограничиваются недостаточным функционалом: отсутствием возможности скрыть персональные данные на страницах, заблокировать пользователя по IP-адресу. Также к техническим опасностям можно отнести распространение на публичных страницах зашифрованных ссылок с недостоверной информацией, а также файлов сомнительного содержания.

Психологические угрозы личности представляют собой более обширную группу, связанную с негативными воздействиями мошенников на психику пользователя, а также использованием персональной информации во вред ее владельцу. Психологические угрозы представляют наибольшую опасность, так как доказать вред нанесенного ущерба не всегда возможно. В большинстве случаев пользователь совершает указанные действия самостоятельно и несет полную ответственность за них. Еще одной проблемой является то, что предоставленной информации может оказаться недостаточно для комплексной оценки ситуации и осуществлении мер по поиску преступника [12].

Что касается данной группы информационных угроз, представляющих собой полноценные диалоги злоумышленника и жертвы, то она является наиболее трудной для анализа и идентификации исследователями. Это связано с отсутствием каких-либо четких критериев для оценки сообщений как противоправных и деструктивных, ведь в данном случае зачастую используются тонкие манипулятивные приемы, методы воздействия на сознание и подсознание.

Прежде чем перейти к описанию сущности и особенностей психологических угроз необходимо рассказать о таком важном феномене, как социальная инженерия. Автор книги «Социальная инженерия и социальные хакеры» М.В. Кузнецов, описывает его как взлом компьютера посредством психологической атаки на пользователя. Социальные инженеры или социальные хакеры добывают конфиденциальную информацию не посредством технического взлома, а путем психологического воздействия на пользователя. В арсенале инженеров существует множество различных методов от шпионажа, сбора персональных данных в виртуальном пространстве и в реальной жизни, до шантажа, эмоционального воздействия, манипуляций, подкупа, обмана и использования в своих целях неблагополучное состояние индивида [10].

Как правило, социальных инженеров не интересуют обычные пользователи, ведь наиболее крупную выгоду они получают от доступа к данным

успешных компаний: банков, концернов, иных финансовых учреждений. Но вполне возможно, что известная и богатая персона или имитированный под нее профиль может стать их мишенью. В этом случае для достижения своих целей хакеры могут установить дружескую коммуникацию с ближайшим окружением пользователя, а после намеренно создавать ситуации, побуждая других из чувства ревности, мести делиться необходимыми данными. Также в ход могут пойти угрозы, предложение финансовой помощи, воздействие на эмоции коммуниканта.

Похожую, но немного отличную от представленной схемы используют представители террористических и экстремистских организаций. Отслеживая потенциальных жертв на различных социальных площадках, они устанавливают близкий контакт и доверительное общение, что в дальнейшем используется для вербовки сторонников. С целью привлечения новых членов, террористы используют различные манипулятивные техники, создавая впечатление внимательного, чуткого и доброго собеседника, а также обещая различные выгоды и блага за внесенный в деятельность организации вклад. Следует также иметь ввиду, что потенциальной жертвой террористов могут стать разочарованные, подавленные, угнетенные, недовольные своей жизнью люди, открыто выражающие негативные эмоции на социальных площадках, а также демонстрирующие потребность в поддержке и понимании.

Помимо представленных выше методов психологического воздействия, преследующих очевидную выгоду для ее субъектов, широкое распространение получили деструктивные коммуникативные акты, целью которых является унижение и подавление личности собеседника. Примерами таких явлений являются троллинг и кибербуллинг. Понятие кибербуллинга авторы Е.А. Еремина, Ю.В. Калинина, Е.А. Заплатина, Л.В. Лопатин определяют как нападения с целью нанесения психологического вреда, осуществляемые на различных информационно-коммуникационных площадках [17].

Существует несколько наиболее популярных методов кибербуллинга[35], к которым относятся: использование личной информации с целью воздействия на пользователя, компрометация взломанных профилей, шантаж интимными фотографиями и секретными данными; киберпреследование, которое заключается в систематическом отправлении пользователю оскорбительных и неприятных сообщений; флейминг, а именно, оскорбление и унижение пользователей в публичных места; клевета; хеппислепинг, что означает создание и размещение видео с избиением и унижением пользователя без его согласия. Отдельно необходимо отметить навязчивое преследование с сексуальным подтекстом, характерное для отдельной группы психически неуравновешенных людей - эротоманов, которые используют любые способы, чтобы привлечь внимание жертвы и вступить в контакт [17].

Такие информационные угрозы, как психологические воздействия и манипуляции социальных хакеров, представителей террористических группировок, наркодилеров, мошенников, эротоманов, а также кибербуллинг представляют наибольшую опасность в условии сетевой коммуникации, так как могут стать причиной серьезных психологических проблем, физических травм, а также привести к суициду[34].

Последняя группа информационных угроз представляет собой совокупность технических и психологических приемов. Мошеннические атаки осуществляются путем отправки единичного сообщения или небольшого стандартного диалога. Такие операции представляют меньшую степень опасности по сравнению с психологическими угрозами в связи с наличием универсальных приемов и отчетливого алгоритма действий хакеров.

Все виды информационных угроз, связанных с совокупностью информационнотехнических и информационно-технических способов атаки, можно обозначить таким понятием, как спам. По мнению О.В. Лутовиновой, спамом является анонимная рассылка сообщений пользователям, не дававшим на это согласие и не выражавшим желание ее получить. Автор предлагает

собственную классификацию спам-сообщений среди которых: коммерческий спам, целью которого является получение какой-либо коммерческой выгоды; спам для раскрутки ресурса, посредством которого владельцы сайта накручивают трафик и увеличивают посещаемость; мошеннический спам, направленный на кражу личных данных или денег, в том числе спам с рассылкой вредоносных программ; спам для сбора необходимых данных, который маскируется под видом опросников и анкет; религиозный спам; «письма счастья» или сообщения, которые с помощью тех или иных методов убеждают пользователя продолжать участвовать в рассылке сообщений [19].

Исследователь также отмечает, что наряду с укреплением информационной безопасности пользователей и увеличением осведомленности о различных формах спама и негативных последствиях, содержания нежелательных писем становятся все более персонифицированными, креативными и интригующими. Для того чтобы обеспечить посещаемость субъекта рассылки, способствовать продвижению определенного товара или услуги, а также из иных соображений, авторы спам-сообщений могут придумывать захватывающие заголовки, вызывающие немедленный эмоциональный отклик, а также использовать вопросы, просьбы поделиться интересной информации и взамен посмотреть содержание письма и многое другое [19].

Однако большая часть перечисленных методов используется в коммуникации посредством электронной почты. Что касается информационных угроз в контексте сетевой коммуникации, а в частности, коммуникации в социальных сетях, необходимо обратить более пристальное внимание на следующие явления: фишинг — это особый вид интернет-мошенничества, который основан на отсутствии у пользователя представлений о способах и приемах информационной защиты. [37]

Субъекты негативного воздействия отправляют коммуникантам сообщение с просьбой перейти на определенный сайт, который является

мошенническим (фишинговым), и зачастую может представлять точную копию официальных ресурсов крупных компаний. Подобные сайты предназначены для сбора персональной информации: паролей, логинов, данных банковских карт и др. Также создатели фишингового сайта могут предлагать пользователям воспользоваться услугой за символическую сумму денег, которая после совершения операции перечисляется на счет мошенников.

Другой распространенной угрозой является фарминг. Технология фарминга заключается в том, что на компьютер пользователя устанавливаются программы, так называемые «трояны», которые перенаправляют запросы на ложные ГР-адреса, тем самым инициируя кражу личных данных.

После того, как конфиденциальные данные пользователя стали доступны мошеннику, происходит массовая атака фишинговыми сообщениями дружеских профилей в социальных сетях. В содержании сообщения может быть указана любая информация, способная заинтересовать потенциальную жертву, как, например, просьба зайти и оценить видео или фотографии, адресованные лично пользователю, рекомендация полезного ресурса или эмоциональный отклик на содержимое страницы. Также со взломанного профиля возможна прямая рассылка с просьбой о помощи в трудной ситуации, просьба перечислить небольшую сумму денег на мобильный номер или банковский счет. В редких случаях после кражи персональных данных мошенник может полностью изменить содержание страницы, адаптируя ее для собственных коммерческих целей [6].

Обозначенные информационные угрозы редко наносят серьезный урон участнику сетевой коммуникации, так как после первого неудачного контакта с фишинговыми сайтами, пользователи становятся более бдительными и стараются игнорировать информацию о непроверенных ресурсах. Кроме того, технические специалисты сетевых площадок постоянно совершенствуют способы защиты от мошеннических рассылок, блокируя сомнительные профили и мгновенно реагируя на жалобы пользователей.

Однако, несмотря на наличие системы безопасности, объектами мошеннических операций с большой долей вероятности могут стать новые пользователи социальные сетей и виртуального пространства, а также дети и пожилые люди.

2.3 Распространенные типы информационных угроз личности в сетевой коммуникации и способы защиты

Специалисты информационной безопасности компаний, которые занимаются развитием онлайн-платформ и различных ресурсов, регулярно повышают уровень информационной безопасности, блокируют миллионы попыток вторжения. Однако, многие пользователи всё равно становятся жертвами хакеров. Этому есть несколько причин.

- Злоумышленники действуют на шаг впереди, а сторона защиты в многих случаях должна реагировать на новые вызовы, которые предлагают им хакеры
- Пользователи слабо информировано о том, какими возможностями обладают хакеры, также у них нет навыков, которые необходимы для надежной защиты своих собственных данных.
- Злоумышленникам проще действовать, видя те механизмы защиты, которые применены в системе. Хакеры подбирают нужные ключи и обладают преимуществом перед слабыми системами.

Так, например, несколько лет назад, в сеть утекла информация о продажи данных 100 миллионов аккаунтов, которые относятся к популярной в России социальной сети ВКонтакте.[36] СМИ подтвердили, что база данных продавалась на специализированных электронных ресурсах. В базе данных хранились данных для входа, которые необходимы для авторизации, а также номера телефоны, которые привязаны к аккаунту, и электронная адреса почты пользователей. Платформа слив данных не опровергла, но заявила, что слитая информация старая и не представляет ценности в текущем времени. Однако, сам факт слива информации подтвердился. Электронный ресурс также заявил, что

основная проблема в отсутствии цифровой грамотности у пользователей, которые пренебрегают классическими и фундаментальными правилами информационной безопасности, в частности создания паролей [24].

Другие случаи информационно-технических атак на пользователей были зафиксированы в социальной сети Instagram. Во-первых, оказалось, что Instagram-аккаунты пользователей можно было взломать с помощью картинки. Данный баг возникал из-за особенностей работы старой версии приложения и обработке картинок. Во-вторых, многие посетители социальной сети жаловались на подозрительную активность: добавление новых подписок, рассылку спама, искажение личных данных. В результате поиска возможных источников угроз опытные программисты обнаружили недочеты в настройках персонального аккаунта и приложений, позволяющих собирать личные сведения и управлять пользовательской страницей. Для решения данной проблемы, по их мнению, достаточно внимательно читать инструкции ресурса и требования установленных программ [31].

Еще один способ незаконного захвата страницы, которые актуален для таких социальных сетей, как Facebook и ВКонтакте, связан с особенностями авторизации. Для взлома аккаунта хакеру достаточно знать логин пользователя и ответ на секретный вопрос. В некоторых случаях указанную информацию посетители самостоятельно размещают в новостной ленте. Для защиты от подобных атак следует более внимательно относится к размещаемому контенту и не разрешать доступ к личным данным другим пользователям.

Однако не только технические ошибки и несовершенства виртуальных платформ открывают мошенникам доступ к информации. Зачастую сами пользователи проявляют невнимательность при вводе зашифрованных данных на сторонних ресурсах. Ради выгодного предложения, интригующих сведений, удовлетворения любопытства посетители социальных сетей игнорируют простые правила безопасности и становятся жертвами фишинговых атак.

Одной из таких мошеннических операций является кража данных с помощью приложения «Музыка ВКонтакте» (приложение не является официальным приложением платформы), свободно распространявшееся в онлайн магазине Google P1ay. Механизм работы программы достаточно прост: для доступа к архивам социальной сети Вконтакте пользователь добровольно вводит логин и пароль. Все собранные данные отправляются напрямую к злоумышленникам, которые используют их для собственных целей. Во избежание подобных ситуаций администрация ресурса настоятельно рекомендует не устанавливать сторонние приложения для социальных сетей и проявлять бдительность при вводе личных данных в незнакомых формах [14].

Фишинговые атаки участились и в популярной сети Instagram[38]. Хакеры под видом сотрудников компании EA Games предлагают пользователям приобрести новых игроков для компьютерной игры абсолютно бесплатно. Для совершения операции необходимо лишь перейти по указанной под фотографией ссылке и ввести персональные сведения. После того, как секретная информация попадает в руки нарушителей, пользователь теряет доступ к своему аккаунту и его настройкам. Подобный ход является универсальным для большинства хакерских атак. В связи с чем следует крайне осторожно реагировать на обещание бесплатных вознаграждений и преимуществ, особенно если в обмен на них нужно отправить какие-либо сведения.

Обобщая данные о фишинговых атаках пользователей, важно отметить, что несмотря на большое значение технической составляющей, успешность операции зависит от психологических факторов, а именно, ответной реакции участников сетей. Жажда легкой наживы, любопытство и беспечность посетителей эксплуатируются хакерами с целью взлома аккаунтов и кражи секретных сведений. Для предотвращения подобных действий следует тщательно анализировать входящую информацию, игнорировать подозрительные ссылки и файлы, внимательно изучать URL страницы, не вводить свои данные на посторонних ресурсах и в скачанных приложениях. При

поступлении сомнительных просьб от друзей, знакомых и представителей компаний, необходимо своевременно связываться с ними любыми другими доступными способами для уточнения деталей [14].

Действие обозначенных угроз основано на сложных программных алгоритмах и психологических уловках. Чаще всего мошенники используют простые и универсальные механизмы воздействия - интригующие заголовки, директивные послания, просьбы перевести деньги, обещания бесплатных подарков и другие. Для противодействия атакам достаточно быть осведомленным о возможной угрозе и внимательно фильтровать информацию.

В отличие от спама и фишинговых атак, информационно-психологические операции представляют собой комплекс более серьезных и деструктивных воздействий на психику пользователя с целью унижения достоинства личности, кражи секретной информации, провокации. Для совершения противоправных действий злоумышленники предпочитают виртуальные платформы с возможностью легкой и быстрой обратной связи, именно поэтому участники популярных сетей часто становятся мишенью негативных воздействий [8].

Одним из наиболее известных примеров информационно-психологической атаки является история Николы Брукс, одинокой англичанки, оставившей свой комментарий в поддержку выбывшего участника программы Х-фактор. Вслед за размещением нейтрального сообщения в социальной сети Facebook посетительница неожиданно стала мишенью для яростного троллинга. Больше, чем полгода британку оскорбляли и унижали на просторах Сети. Помимо этого, обидчики создали страницу от ее имени и распространяя непристойные сообщения. По данным СМИ, тролли также атаковали близких Николы, отправляя им грязную информацию якобы под ее авторством. Также они обнародовали данные о месте жительства Николь и начали преследовать женщину за пределами виртуального пространства [29].

Ответной реакцией британки стало обращение в полицию за просьбой возбудить уголовное дело против нарушителей. К сожалению, доступных способов поиска и привлечения к ответственности троллей слуги закона не обнаружили. Однако инициативная британка не сдалась и подала обращение в высокий суд Лондона, обязавший социальную сеть Facebook раскрыть IP-адреса обидчиков, с помощью которых можно установить личность нарушителя и привлечь его к ответственности.

Одним из положительных результатов дела Николы Брукс стало введение меры наказания британских пользователей, публикующих оскорбительную информацию и угрозы, сроком до шести месяцев заключения. Также подобный прецедент стал поводом для обсуждения способов защиты граждан страны от информационных атак, осуществляемых в Интернет-пространстве.

Что касается негативных последствий, то сама Никола Брукс призналась, что наряду с популяризацией данной темы количество негативных комментариев в ее адрес только увеличилось, тогда как поймать всех обидчиков не представлялось возможным и целесообразным. По данным полицейских, британка провоцировала троллей негативными репликами и яростными ответами на оскорбления в свой адрес, чем только усугубила свое положение [29].

Анализируя особенности данного случая, необходимо в первую очередь отметить важность способов самозащиты, включающих в себя как защиту психологическую, так и техническую. Отсутствие знаний о психологических угрозах, правилах поведения в сетевой коммуникации, способах реагирования на провокативные действия, методах технической защиты стало причиной разжигания конфликта до национального масштаба. С большой вероятностью можно предположить, что своевременные действия по защите личного аккаунта, ограничению нежелательных собеседников и спокойной адекватной реакции могли бы спасти женщину от трагичных последствий информационных атак.

Приведенные примеры являются уникальными прецедентами борьбы с информационными угрозами. Несмотря на то, что все обозначенные иски были удовлетворены, а пострадавшие лица получили моральную компенсацию и возможность наказания злоумышленников, результаты такого судебного вмешательства можно оценить неоднозначно.

Во-первых, необходимо отметить, что использование правовых механизмов целесообразно и оправдано только в случае единичных атак на пользователя. Это связано с возможностью установления личности и привлечения его к ответственности. Что касается массового троллинга, то, как показала история Николы Брукс, поиск виновных не только не помогает устранить всех субъектов психологического воздействия, но и становится катализирующим фактором информационной агрессии.

Во-вторых, полноценная информационная защита от пользовательских атак возможна только при соблюдении определенных правил поведения и рекомендаций, изучении способов технической, психологической и правовой защиты, формировании информационной культуры. Необходимо помнить, что сетевая коммуникация в силу своих особенностей является более свободной, демократичной, а значит менее доступной для единого контроля. Следовательно, особое внимание следует сосредоточить на способах защиты от информационных воздействий и манипуляций, развитию психологических навыков.

Глава 3. Комплексная защита личности от информационных угроз личности в сетевой коммуникации и способы защиты

3.1 Определение сущности и характера информационных угроз

Для успешной защиты от негативных воздействий в виртуальном пространстве необходимо, в первую очередь, правильно идентифицировать реальные и потенциальные угрозы. Определение сущности, особенностей и источников негативных воздействий может осуществляться на базе разработанной в ходе исследования классификации.

В соответствии с представленным в теоретической части описанием, все информационные угрозы в сети можно сгруппировать в 3 совокупности: информационно-технические опасности (хакерский взлом сети, распространение вирусного программного обеспечения на электронном ресурсе, кража данных с помощью специальных программ), информационно-психологические опасности (троллинг, преследование, унижение, оскорбление, шантаж, манипулятивные воздействия, методы социальной инженерии) и смешанные опасности, представляющие собой сочетание информационно технологических и простых информационно-психологических приемов (спам, фишинг, письма счастья и прочее). [9]

Идентификация информационно-технической опасности может представлять определенную сложность ввиду отсутствия видимых последствий. Однако для обеспечения собственной безопасности пользователю необходимо периодически проводить мониторинг компьютера на наличие вирусных программ, кейлоггеров, вредоносного ПО. [9]

Косвенными признаками заражения устройства является медленная и некорректная работа компьютера и отдельных программ, увеличение количества файлов, изменение их размера и даты модификации, искажение установленных программ, появление рекламных окон и баннеров, автоматическая загрузка нежелательных сайтов, а также иная подозрительная активность.

Что касается идентификации технической угрозы в социальных сетях, то пользователю следует внимательно проанализировать активность личного аккаунта: изучить содержимое персональной страницы, сообщений и диалогов, список групп, друзей и настройки страницы. Помимо этого, желательно воспользоваться сервисами анализа активности с возможностью отображения точного времени и способа активации аккаунта. При обнаружении подозрительной активности следует своевременно предпринять необходимые меры по защите информации.

Другой вид информационных угроз, основанных на психологических методах воздействия и манипуляции тяжело распознать лишь в редких случаях. Как правило, среди таких примеров - целенаправленные атаки экстремистов, шантажистов и социальных инженеров. Обнаружить опасность можно по некоторым характерным признакам: настойчивые просьбы незнакомых людей переслать личные сведения, интимные фотографии, поделиться секретами; невыполнимые обещания и предложения помощи в обмен на какую-либо активность; утаивание информации об имени, происхождении и деятельности собеседника, а также отсутствие основных данных на странице посетителя. [30]

В иных ситуациях информационные атаки осуществляются путем распространения оскорбительной информации, угроз, провокативных реплик, унизительных, грубых, пошлых выражений. Психологическая операция может осуществляться как одним пользователем, так и группой на основе договоренности. Местом атаки в большинстве случаев является публичная страница или группа с открытым доступом, реже злоумышленники обращаются к жертве напрямую в личные сообщения.

Последняя группа информационных атак, нацеленных на кражу данных аутентификации, установлении вирусного ПО на компьютеры пользователей, осуществление фиктивных денежных переводов представляет собой совокупность технических и психологических методов. К числу таких опасностей относится спам и такая его разновидности, как фишинговые атаки.

Идентификация данных угроз требует определенных знаний и навыков у пользователей социальных сетей. Фишинговые сайты могут быть абсолютны идентичны официальным ресурсам по содержанию и визуальному оформлению, однако при анализе адресной строки браузера разница станет очевидной. Мошенники зачастую используют рандомный набор букв при написании доменного имени и небезопасное соединение. Другой отличительной особенностью атаки злоумышленников является генерация похожих по содержанию сообщений, приглашающих пользователя ознакомиться с интересным, интригующим и необычным контентом и отсутствие обратной связи. Для распознавания хакерской операции достаточно задать собеседнику какой-либо сложный вопрос или попросить сообщить информацию, о которой может знать только он (при условии, что сообщение отправлено близким другом или знакомым) [32].

3.2 Алгоритм действий по обеспечению безопасности

Алгоритм представляет собой последовательность действий, необходимых для осуществления самозащиты в рамках коммуникативных практик. Разработка данного алгоритма базировалась на теоретических моделях представителей психологического направления. Также в основу легли данные аналитического исследования теоретического материала данной работы.

В соответствии с результатами научного поиска, для предотвращения негативных информационных воздействий на пользователя социальной сети необходимо осуществить последовательность следующих шагов: идентифицировать угрозу, описать и проанализировать особенности реальной или потенциальной опасности, выбрать подходящие методы защиты, определить план осуществления защитных действий, реализовать способы противодействия по обозначенной инструкции.

Под идентификацией угрозы понимается распознавание негативного воздействия в соответствии с обозначенными критериями. Способы идентификации информационных угроз были подробно изложены в

предыдущем разделе. Идентификация угрозы может осуществляться в рамках общего мониторинга технического устройства или целенаправленно при возникновении подозрительной активности установленных программ, аккаунта в социальных сетях, изменении адреса ресурса в поисковой строке, потери персональных данных или некорректной работы компьютера [31]

Обнаружить психологическую угрозу можно в результате анализа действий собеседника. Если пользователь настойчиво призывает совершать необходимые ему действия, будь то публикация или отправка персональных сведений, интимных фотографий, помощь в осуществлении определенных операций, и при этом скрывает данные о себе, то существует высокая вероятность информационной атаки для достижения собственных корыстных целей. Также психологические угрозы могут выражаться в публичных оскорблениях, унижениях, распространении ложной информации, порочащей честь и репутацию, дискриминации и возбуждении вражды и ненависти[38].

Описание и анализ реальной или потенциальной опасности заключается в соотнесении обнаруженной угрозы с определенной группой на основе классификации, обозначение основных характеристик, источников воздействия, цели атаки, используемые технические и/или психологические методы, установление количества нападающих злоумышленников и их личностные особенности. В первую очередь следует обозначить группу угрозы в зависимости от используемых методов: технические, психологические или их совокупность. Также важно обозначить источник угрозы: автоматизированная программа, реальный пользователь со своей настоящей или поддельной страницы, или группа пользователей и цели воздействий: кража данных с целью дальнейшей продажи, шантажа или иных преступных действий; кража денег путем обещания крупного выигрыша, накрутки рейтинга, быстрого решения какой-либо проблемы; получение секретной информации о персоне или организации, или иное. После этого следует более подробно изучить способы воздействия злоумышленников: распространение вредоносных программ,

поддельных сайтов, ложной информации, манипуляция данными и другие. Возможно, мошенник использует несколько перечисленных в предыдущих разделах способов. Идентификация и описание каждого из них поможет выбрать наиболее эффективных для защиты методы [31]

Выбор подходящих способов защиты осуществляется на основе полной характеристики угрозы и анализе существующих прецедентов. Прежде всего изучается эффективность применения правовых, психологических и технических способов защиты. После этого осуществляется выбор активной или пассивной стратегии поведения. Активная стратегия предполагает возбуждением судебного процесса против нарушителя, жалобы на подозрительную активность администрации сайта, а также психологическую оборону. Пассивная стратегия связана с игнорированием негативных воздействий или использованием метода решения конфликтных ситуаций. В рамках пассивной стратегии также возможны обращения к администрации ресурса, однако публичное дело против нарушителя не инициируется.

Перед использованием активной стратегии необходимо оценить возможный ущерб публичного обсуждения дела, вероятность массовой информационной атаки в будущем и наличие достаточного количества и качества доказательств для победы в ходе процесса обвинения. Пассивной стратегия поведения предпочтительнее при отсутствии полной информации о перспективе и характере будущих угроз, а также при недостатке документально оформленных доказательств своей правоты.

На основе анализа прецедентов можно утверждать, что пассивная стратегия защиты более эффективна в ситуации массового троллинга, когда любое публичное действие и ответная реакция жертвы возбуждают интерес злоумышленников. В результате настойчивого сопротивления конфликт разгорается сильнее, а число вовлеченных в него участников начинает увеличиваться в геометрической прогрессии. Если же посетитель стал мишенью информационной атаки со стороны одного зарегистрированного пользователя,

то выбор активной стратегии позволит не только оградить себя от негативных воздействий в коммуникативных ситуациях, но и потребовать от обидчика возмещения морального ущерба [31]

В случае негативного воздействия при помощи совокупности информационно-технических и информационно-психологических методов, следует обозначить несколько методов противодействия, среди которых может быть как техническая блокировка аккаунта, изменение настроек на странице социальной сети, так и психологические способы защиты, в том числе использование стратегий решения конфликтных ситуаций, постепенное прерывание беседы и игнорирование собеседника, разъяснение своей позиции, реакция с помощью шутки или нейтральный ответ на реплики пользователя.

Разработка плана защиты включает последовательность совершения выбранных способов для достижения большей эффективности в борьбе со злоумышленниками. В большинстве случаев более предпочтительной является следующий порядок действий: использование психологических, технических и затем правовых методов. Такая очередность применима к информационно-психологическим и смешанным воздействиям и обусловлена рядом некоторых факторов, которые выявляются на этапе анализа.

С учетом возможных негативных последствий предпочтительнее в первую очередь реализовать выбранную психологическую стратегию: игнорирование или решение конфликтной ситуации. При невозможности блокировать угрозу психологическими методами, следует применить технические средства для удаления нежелательного аккаунта, ограничения доступа к своей странице.

В последнюю очередь, при уверенности в отсутствии негативных последствий правовой защиты, следует собрать необходимые для судебного разбирательства документы и потребовать наказания злоумышленника. В случае предъявления обвинения по статье «Оскорбление» административного кодекса все документально заверенные доказательства угрозу пользователю необходимо

собрать самостоятельно. Если же в деле фигурирует обвинение по Уголовному кодексу РФ, профессиональная экспертиза и разбор дела проводятся правоохранительными органами [31]

После совершения всех указанных выше действий, а именно идентификации угрозы, ее анализа и описания, выбора защитных методов и составления плана необходимо осуществить описанные в инструкции шаги и не забывать корректировать план в зависимости от реакции собеседника и других обстоятельств.

3.3 Технические и социально-правовые способы защиты от информационных угроз в сетевой коммуникации

Лучшая защита от вредоносных атак – антивирусные программы, а также обновленные версии браузеров и специальные дополнения, которые уничтожают вредоносные ресурсы и файлы, мешая тем самым распространению негативных информационных воздействий. Наряду с этим следует проводит еженедельный мониторинг компьютера на наличие подозрительной активности от посторонних программ. При обнаружении признаков возможного заражения необходимо незамедлительно диагностировать и удалить возможную угрозу самостоятельно или обратиться к специалистам.

Для того чтобы избежать хакерского вторжения и кражи персональных данных в социальных сетях следует придумывать сложные пароли с сочетанием букв и цифр, в которых не указаны доступные публике данные, а также использовать дополнительные способы аутентификации, предлагаемые ресурсом. При наличии угрозы взлома следует периодически изменять пароли, используя как можно большее количество символов[40].

Желательно, чтобы пароль представлял собой рандомный набор букв и цифр, а не известные и часто используемые слова. Что касается такой информационной угрозы, как спам в виртуальном пространстве, то избавиться от нее полностью невозможно, однако с помощью настроек

конфиденциальности, инсталляции специальных приложений, блокирующих нежелательную информацию, специальных методов оповещения об опасности в социальных сетях можно сократить его количество до минимального уровня [11].

Также следует проявлять осторожность во время перехода по ссылкам на сторонние ресурсы. Делать это необходимо только после проверки источника ссылки и косвенной информации. Также рекомендуется не открывать файлы и вложения от незнакомых людей без предварительного диалога и согласия. То же самое касается и дружеской просьбы. Убедиться в истинности намерений собеседника достаточно легко с помощью наводящих вопросов.

Не стоит вводить личные данные, такие как логины, пароли, реквизиты банковских карт на сторонних ресурсах. Перед внесением конфиденциальной информации следует внимательно изучить сайт, а особенно его электронный адрес. В строке браузера не должны находится лишние элементы, знаки другой кодировки, случайные наборы букв и цифр. Также следует обратить внимание на наличие безопасного соединения. При возникновении подозрений лучше сразу покинуть данный ресурс, стараясь игнорировать возникающие ссылки и кнопки. При реальной необходимости посетить данный сайт, лучше всего воспользоваться ссылка из поисковых ресурсов, закладок браузера или ввести данные вручную [11].

Если же переход на ресурс с помощью описанных выше методов невозможен и вместо официальной страницы сети загружаются фишинговые (поддельные) сайты, значит пользователь стал жертвой так называемой фарминговой атакой или подмены домена в результате вирусного воздействия. Для решения данной проблемы существует несколько методов, однако все они требуют работы с системными файлами компьютера. Как правило, в результате вредоносного воздействия, вирус изменяет содержимое файла операционной системы, который содержит информацию, необходимую для связи имен серверов с их IP-адресами. После такой подмены браузер считывает ложную

информацию с системного файла и направляет пользователя по указанному вирусом пути. При наличии посторонних адресов следует самостоятельно очистить файл и перезапустить компьютер [32].

Что касается способов защиты от информационно-психологического воздействия на пользователя со стороны мошенников или провокаторов, то в первую очередь необходимо ограничить доступ к персональной информации, а также заблокировать сообщения от незнакомых лиц. Такую конфиденциальную информацию, как домашний и рабочий адреса, номера мобильного и домашнего телефонов, ссылки на личные блоги, интимные фотографии желательно не размещать на страницах социальных сетей.

Для предотвращения возможности вербовки со стороны представителей экстремистских и террористических организаций следует тщательно фильтровать публикуемую информацию, избегая слишком личных, откровенных, пессимистичных публикаций, жалоб на одиночество, апатию и покинутость. При отсутствии возможности ограничения просмотра записей, любая откровенная информация должна строго ограничиваться и фильтроваться [26].

Важно помнить, что большую опасность может представлять обмен личными данными, секретными материалами, провокационными фотографиями с малознакомыми пользователями.

Для нивелирования психологических угроз в сетевой коммуникации необходимо также изучать специальную литературу, освещающую схемы и методы работы преступников, способы психологической защиты личности. По мнению некоторых авторов научных статей, осведомленность о сущности и особенностях информационных угроз сама по себе является средством защиты от нежелательных атак [26].

В случае, когда пользователь стал объектом унижения, запугивания, троллинга, преследования следует вести себя спокойно, не провоцировать

конфликт, не вступать в дискуссии с обидчиками, не пытаться объяснить собственные действия и оправдываться. Лучшей стратегией будет игнорирование собеседников, укрепление защиты своих аккаунтов, удаление личной и конфиденциальной информации профиля, снижение уровня активности [26].

При условии нападения одного или нескольких провокаторов, для защиты собственной безопасности и блокирования возможных угроз в будущем можно обратиться в прокуратуру с заявлением. Если злоумышленники адресовали оскорбление пользователю ресурса и разместили его на публичной странице или в открытой группе, то после получения нотариально заверенного документа о факте нанесения оскорбления, пользователь имеет право начать судебное разбирательство и потребовать моральную компенсацию от провокатора.

При этом за простое оскорбление, выражающееся в нецензурной форме, истец может предъявить обвинение по статье 5.61 Кодекса Российской Федерации об административной ответственности, которая предусматривает штраф за публичной оскорбление личности для граждан от одной до трех тысяч рублей, для должностных лиц - от десяти тысяч до тридцати тысяч рублей, а для юридических лиц - от пятидесяти до ста тысяч рублей. В случае унижения по признаку расы, пола, вероисповедания, национальности, языка и принадлежности к какой-либо социальной группе, пользователь может потребовать наказание от ста до трех ста тысяч рублей или в размере заработной платы обвиняемого за один или два года. Также злоумышленник может быть осужден или направлен на принудительные работы сроком до двух лет в соответствии со статьей 282 Уголовного кодекса РФ [3]

Отдельное внимание можно уделить статье 148 Уголовного кодекса РФ, налагающей штраф до трех ста тысяч рублей или лишение заработной платы и иного дохода сроком до двух лет или принудительными работы, тюремным заключением за публичное оскорбление чувств верующих. Однако есть вероятность, что факт наличия оскорбительных высказываний придется

доказывать в суде самостоятельно, так как дополнительных пояснений к формулировке закона о том, что именно можно считать «оскорблением чувств верующих» не указано [3]

Еще одна статья Уголовного кодекса РФ о клевете может стать основой для правовой защиты в случае распространения ложных сведений, порочащих честь и репутацию пользователя. В случае одобрения заявки истца злоумышленнику может грозить штраф до пятидесяти тысяч рублей или обязательные работы до ста шестидесяти часов [3].

ЗАКЛЮЧЕНИЕ

Появление и популяризация инновационных технических устройств, функционирующих на основе сетевой логики, инициировали трансформацию многих форм социальной активности личности. Особенно сильное влияние обозначенные процессы оказали на коммуникативную сферу, способствуя формированию простого, доступного, моментального опосредованного взаимодействия с сетевыми факторами.

Однако наряду с поиском выгодных и продуктивных решений, основанных на свободном доступе и обмене информацией с представителем любой возрастной, гендерной, социальной группы, получили развитие такие разрушительные процессы, как информационные атаки, информационный терроризм, хищение данных, сокрытие и искажение информации. В этой связи изучение сущности и особенностей информационной безопасности в сетевых коммуникациях, описание реальных и потенциальных угроз в социальных сетях и способов защиты от них стало особенно актуальным.

Под информационной безопасностью в данном исследовании понимается состояние защищенности личности от деструктивных воздействий в информационной среде.

Объектами защиты являются: конституционные права, психика, физическая, духовная и интеллектуальная сферы.

Субъектами защиты могут выступать как государство, технические специалисты, так и сама личность. Система информационной безопасности обозначена как совокупность нескольких элементов: информационно-технической, информационно-правовой, информационно-психологической безопасности

Феномен сетевой коммуникации определяется в работе как коммуникационный процесс, организованный по принципу сетевой структуры и обладающий такими характеристиками, как динамичность, глобальность,

опосредованность, анонимность, гибкость, децентрализованность, интерактивность и хаотичность.

Принцип сетевой коммуникации наиболее наглядно представлен в интеракциях пользователей социальных сетей. Под социальной сетью понимается онлайн сервис, посредством которого люди могут группироваться по различным принципам, а также общаться и самовыражаться при помощи специальных инструментов. Основным отличием социальных сетей является возможность быстрого поиска единомышленников, установления контактов с пользователями, передачи различной информации, создания и наполнения собственных персональных страниц и другое.

На основе анализа сущности и особенностей сетевой коммуникации и социальной сети показано, что несмотря на преимущества новой формы взаимодействия, которая позволяет устанавливать контакт независимо от географического положения, национальности, культуры, часового пояса, способствует формированию коммуникационных сетей, играющих ключевую роль в решении экономических, политических и иных проблем, а также помогает найти знакомых, друзей, родственников, деловых партнеров, единомышленников, существуют негативные последствия данных новаций.

Наряду с активным распространением сетевых средств коммуникации увеличивается сложность социальной системы в целом и системы коммуникации в частности, что является фактором ослабления стабильности. Распространение горизонтальной коммуникации, ее открытость и демократичность инициируют развитие новых способов деструктивной деятельности в виртуальном пространстве.

В контексте обозначенных тенденций изучены особенности наиболее активной аудитории виртуальных платформ - молодежи. Сделан вывод о том, что представители молодежной аудитории, обладающие неустойчивой психикой, восприимчивым сознанием, отсутствием сформированной системой

ценностей, противоречивыми чертами личности и потребностью в идентификации и самопрезентации, являются уязвимой для информационных воздействий группой.

Помимо этого, в рамках исследования описаны и классифицированы способы информационных атак в условиях сетевой коммуникации. Негативные воздействия в виртуальной коммуникации сгруппированы в три совокупности: технические, психологические и смешанные информационные угрозы.

Под техническими угрозами личности автор работы обозначил опасные воздействия, связанные с несовершенством технических устройств, программ, способов обработки, передачи информации, такие как компьютерные вирусы, вредоносное программное обеспечение, кейлогеры, неполадки в системе безопасности виртуальной площадки, незащищенное соединение ресурса, некорректно указанные настройки и пр.

Психологические угрозы личности определены как негативные воздействия мошенников на психику пользователя путем обмана, манипулирования данными, шантажа, угроз, распространения оскорбительной информации и пр. Было выяснено, что психологические угрозы представляют наибольшую опасность, так как доказать ущерб и причастность к делу конкретного лица не всегда возможно. В большинстве случаев преступник регистрирует аккаунты на компьютерах общего пользования или отрицает свою вину, что препятствует расследованию преступлений. К психологическим угрозам отнесены такие феномены, как кибербуллинг, троллинг, хеппислепинг, методы социальной инженерии и другие.

Отдельную группу составляют виртуальные опасности, основанные на применении информационно-технических и информационно-психологических методов в совокупности. Особенностью атак данного типа является использование одиночных сообщений или примитивных диалогов, содержащих

подозрительные ссылки или вложения. Примерами таких информационных угроз являются спам, фишинг, фарминг.

В рамках исследования изучены реальные ситуации хакерских нападений на пользователей и связанные с ними судебные прецеденты. В результате анализа представленных кейсов сделаны значимые выводы о необходимости комплексной защиты личности, базирующейся на совокупности технических, психологических, правовых методов и определенном алгоритме действий. В ходе работы доказано, что разрозненные способы защиты могут не только не привести к необходимому результату, но и повлечь за собой более серьезные негативные последствия для пользователя.

На основании теоретических и практических данных описаны основные элементы комплексной модели защиты, обозначена последовательность действий для обеспечения личной безопасности: идентификация угрозы, описание и анализ особенностей реальной или потенциальной опасности, выбор подходящих методов защиты, разработка плана действий и его реализация.

Под идентификацией в рамках данной модели понимается распознавание негативного воздействия техническими и/или психологическими способами. Описание и анализ реальной или потенциальной опасности определены как совокупность процессов соотнесения обнаруженной угрозы с определенной группой на основе классификации, обозначения основных характеристик, источников воздействия, цели атаки, используемых методов, установления количества нападающих злоумышленников и их личностные особенности.

В работе также указаны критерии выбора подходящих методов защиты, основанных на анализе сущности и особенностей негативных воздействий, изучения существующих прецедентов и реальных кейсов. Автором обозначены основные стратегии поведения при угрозе негативного информационного воздействия в виртуальном пространстве, подробно описаны способы обеспечения личной безопасности.

Данная работа выполнена мною самостоятельно

«15» _Мая_____ 2021 г. _____ (подпись)

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

1. Федеральный закон от 27.07.2006 N 152-ФЗ // Статья 7. Конфиденциальность персональных данных (ред. от 24.04.2020) "О персональных данных"
2. Федеральный закон от 30 декабря 2020 г. N 489-ФЗ "О молодежной политике в Российской Федерации"
3. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 05.04.2021, с изм. от 08.04.2021)
4. ГОСТ Р 50922-96: «Защита информации. Основные термины и определения» (дата обращения 20.11.2020)
5. Акмасова А.А., Информационно-психологическая безопасность личности [Электронный ресурс] // URL: http://www.bla.by/public/conf_2/1_2003.pdf (дата обращения 05.03.2021)
6. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации : учеб. пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2018. — 336 с. — (Высшее образование) [Электронный ресурс] // URL: https://publications.hse.ru/mirror/pubs/share/direct/218576514 (дата обращения: 05.03.2021).
7. Вихорев С.В., Классификация угроз информационной безопасности [Электронный ресурс] // URL: https://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml (дата обращения 05.03.2021)
8. Информационно-психологическая и когнитивная безопасность. Коллективная монография / Под ред. И.Ф.Кефели, Р.М.Юсупова. ИД «Петрополис», Санкт-Петербург, 2017. —300 с. 32 рис., 8 табл.
9. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: Учебное пособие. Авторы: Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. – 198 с

10. Кузнецов, М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. — СПб.: БХВ-Петербург, 2017. — 368 с.
11. Макаренко С. И. Информационная безопасность: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил. [Электронный ресурс] // URL: https://sccs.intelgr.com/editors/Makarenko/Makarenko-ib.pdf (дата обращения: 25.04.2021).
12. Нестеров С. А. Основы информационной безопасности: учеб. пособие. - 5-е изд., стер. - Санкт-Петербург: Лань, 2019. - 324 с. [Электронный ресурс] // URL: https://e.lanbook.com/book/114688 (дата обращения 05.03.2021)
13. Таржанов Т.В., Кудряшов В.Е., Макарова Д.Г., Вредоносное программное обеспечение и методы борьбы с ним - Интерэкспо Гео-Сибирь, том 9, 2019, с. 15-18
14. Эрик Кулман, Безопасная сеть. Правила сохранения репутации в эпоху социальных медиа и тотальной публичности, Альпина Паблишер, Москва, 2017 – 214 с.
15. Бритвин Н.И. Социальные сети как прообраз общественного устройства Власть. 2008. №1. Стр. 45-49 [электронный ресурс] // URL: https://cyberleninka.ru/article/n/sotsialnye-seti-kak-proobraz-obschestvennogo-ustroystva/viewer (дата обращения 10.11.2020)
16. Владимирова Т.В. Сетевые коммуникации как источник информационных угроз [Электронный ресурс] // URL: http://ecsocman.hse.ru/data/2011/09/20/1267451215/Vladimirova.pdf (дата обращения 05.03.2021)
17. Горбатюк Я.С., Кибербуллинг как педагогическая проблема - Актуальные проблемы физической культуры и безопасности жизнедеятельности, Сборник научных трудов факультета физической культуры и безопасности жизнедеятельности. Под редакцией Л.В. Кашицыной. Саратов, 2019, с. 53-57

18. Елишев С.О. Молодёжная проблематика и подходы к определению понятия «Молодёжь» в социологии – Вестник Московского университета, серия 18, Социология и политология. 2017. №3 с. 200-223
19. Фенина Виктория Владимировна Особенности речевого манипулирования в электронных спам-письмах // Язык и культура. 2017. №37. [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/osobennosti-rechevogo-manipulirovaniya-v-elektronnyh-spam-pismah (дата обращения: 05.03.2021).
20. Черных А. И. Социология массовых коммуникаций: учебное пособие. М.: Изд. дом ГУ-ВШЭ, 2008 [электронный ресурс] // URL: https://publications.hse.ru/mirror/pubs/share/folder/ox5oymyz2c/direct/54927100.pdf (дата обращения 15.11.2020)
21. Bourdieu P. The forms of capital // Handbook of theory and research for the sociology of education / Ed. By J.G. Richardson. N.Y. : Greenwood, 1986
22. Muromtsev V.V., Muromtseva A.V. Human-Information Space in the Context of Contemporary Virtual Communications // Components of Scientific and Technological Progress, 2014. № 3(21). Стр. 38-46
23. Википедия [Электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Информационная_безопасность (дата обращения 23.11.2020)
24. «ВКонтакте» прокомментировала сообщения о краже данных 100 млн аккаунтов, Технологии и медиа, РБК, 2016 [Электронный ресурс] // URL: https://www.rbc.ru/technology_and_media/06/06/2016/575507249a7947351eb7bc0f (дата обращения: 05.03.2021).
25. Социальные сети в России: цифры и тренды, осень 2020. Brand Analytics [Электронный ресурс] // URL: https://br-analytics.ru/blog/social-media-russia-2020/ (дата обращения 05.03.2021)
26. Соцсети и общедоступные данные пользователей [Электронный ресурс] // URL: https://vc.ru/legal/64191-socseti-i-obshchedostupnye-dannye-polzovateley (дата обращения: 05.04.2021).

27. «Касперский» заявил о краже данных сотен тысяч пользователей «ВКонтакте», Технологии и медиа, РБК, 2015, [Электронный ресурс] // URL: https://www.rbc.ru/technology_and_media/09/10/2015/5617a9d19a79477d5a3458f1 (дата обращения: 05.03.2021).
28. МВДМедиа [интернет ресурс] // URL: https://mvdmedia.ru/news/official/o-sostoyanii-prestupnosti-v-rossiyskoy-federatsii-v-1-m-kvartale-2020-goda/ (дата обращения 25.11.2020)
29. Личности интернет-троллей можно будет установить, BBC [Электронный ресурс] // URL: https://www.bbc.com/russian/uk/2012/06/120612_identify_trolls (дата обращения: 05.03.2021).
30. Угрозы информационной безопасности [Электронный ресурс] // URL: https://www.anti-malware.ru/threats/information-security-threats (дата обращения: 05.04.2021).
31. Угрозы информационной безопасности [Электронный ресурс] // URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/ (дата обращения: 25.04.2021).
32. Фишинг [Электронный ресурс] // URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3_(phishing) (дата обращения: 05.04.2021).
33. Instagram-аккаунты пользователей можно было взломать с помощью картинки, Екатерина Быстрова, Anti-Malware, 2020, [Электронный ресурс] // URL: https://www.anti-malware.ru/news/2020-09-24-111332/33763 (дата обращения: 05.03.2021).
34. Ефимова Е.С. Кибербуллинг как проблема психопедагогики виртуальных сред // Успехи в химии и химической технологии. 2014. Т. 28. №7(156). С.65-66

35. Черкасенко О.С. Травля в социальных сетях // Наука и Мир. 2015. Т. 2. № 8 (24). С. 107-108
36. Хакер объявил о продаже базы со 100 млн аккаунтов «ВКонтакте» за 1 биткоин, VC.ru, 2016, [Электронный ресурс] // URL : https://vc.ru/social/16009-vk-hack-base (Дата обращения 14.02.2021)
37. Что такое фишинг ? , CISCO , [Электронный ресурс] // URL : https://www.cisco.com/c/ru_ru/products/security/email-security/what-is-phishing.html
38. Фомина Н. А. Использование методов социальной инженерии при мошенничестве в социальных сетях. // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодёжи. 2015. С 443-453
39. Instagram фишинг использует 2FA в качестве приманкки. [Электронный ресурс] // URL : https://bezmaly.wordpress.com/2019/08/24/instagram-phishing-2fa/ (дата обращения 10.02.2021)
40. Советы по созданию уникальных надёжных паролей. [Электронный ресурс] // URL : https://www.kaspersky.ru/resource-center/threats/how-to-create-a-strong-password (15.02.2021)