ISSN 2658-5014 (Print)
2024. Т. 6, № 1 (16). С. 59–66

СИИТ

ISSN 2686-7044 (Online)
http://siit.ugatu.su

СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
Научное сообщение

УДК 004.4 DOI 10.54708/2658-5014-SIIT-2024-no1-p59 EDN QGMIIO

Деструктивное и манипулятивное влияние социальных сетей

Ж. М. Даирбекова • А. Ю. Полуян

Аннотация. В статье рассматриваются виды деструктивного манипулятивного воздействия социальных сетей на общество. В частности, рассматриваются технологии поиска потенциального электората на выборах в США 2020 г., где с помощью таргетинга и ретаргетинга формировалось мнение о том или ином кандидате. Также рассматривались деструктивные влияния суицидальных групп в социальных сетях. Приводится статистика оценки ВЦИОМ использования по времени социальных сетей - большинство россиян ежедневно проводят время в социальных сетях и сервисах связи, особенно активно ими пользуется молодежь. Работа в социальных сетях может повлиять на центр удовольствия мозга, что приводит к зависимости от них из-за предоставления контента небольшими порциями в нужном тоне. В статье описывается, что социальные сети часто используются манипуляторами для провоцирования общественных протестов, вооруженных конфликтов, силового захвата власти. При этом информационная безопасность личности определяется защитой ее психики и сознания от опасных информационных воздействий, таких как манипуляция, дезинформация, доведение до самоубийства, участия в противоправных действиях. Указывается негативное влияние в виде распространения дезинформации, такой, как в частности была в отношении антипрививочного движения во время эпидемии COVID-19. Делается вывод, что необходимо провести юридическое регулирование по отношению к технологиям Deepfake по примеру опыта других государств. Затрагивается вопрос о юридическом регулировании информационных новостных групп в социальных сетях как средства массовой информации, так и в целом правового регулирования социальных сетей. Делается вывод, что необходимо провести юридическое регулирование по отношению к технологиям deepfake по примеру опыта других государств.

Ключевые слова: социальные сети; манипуляции общественным мнением; информационная безопасность; таргетинг; социальная инженерия.

Введение

В современном мире роль информационной отрасли постоянно растет. Информационная сфера оказывает значительное влияние на политический, экономический, оборонный и другие аспекты безопасности государства. Следовательно, национальная безопасность зависит от обеспечения информационной безопасности, особенно с учетом развития информационных технологий, что приводит к росту взаимозависимости и придает ей большее значение для государства и общества в целом. Так, согласно Указу Президента РФ от 05.12.2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации», информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации. Национальная безопасность тесно связана с деятельностью государства. Только она, имея в виду свой аппарат, властные органы, деятельность которых четко регулируется соответствующими правовыми актами, может обеспечить спокойствие граждан, создать благоприятные условия для их жизни и деятельности. Остальные социальные силы не способны выполнить эту миссию. Обеспечение своей безопасности и безопасности граждан является одной из основных задач любого государства. Успешное развитие Российской Федерации как суверенного государства невозможно без обеспечения национальной информационной безопасности.

В мире, где процессы информатизации и глобализации активно развиваются, роль информационной безопасности для личности, общества и государства растет, и ее обеспечение имеет важное значение в политике государства. Основные задачи обеспечения информационной безопасности как составляющей национальной безопасности государства требуют решения следующих вопросов:

• необходимость нормативно-правового регулирования для противодействия использованию информационных технологий, угрожающих интересам государства;

• создание экономических условий развития национальных информационных ресурсов и инфраструктуры, внедрение новейших технологий в сферу информации;

• совершенствование производства отечественных информационных технологий, внедрение отечественных разработок, повышение эффективности научных исследований и качества образования в области информационных технологий.

Информация стала одним из ключевых факторов, что может привести к серьезным авариям, военным конфликтам и дезорганизации государственного управления. Чем выше уровень интеллектуализации и информатизации общества, тем надежнее его информационная безопасность. Поэтому России важно уделять особое внимание национальной безопасности, поскольку она является основой определения важнейших направлений и принципов государственной политики страны, жизненно важных интересов личности, государства и общества.

Безусловно, в настоящее время информационные потоки проникают во все сферы нашей жизни: так, например, фитнес-треккеры отслеживают наши биологические сигналы и перемещения и транслируют эти данные в такие социальные сети, как Garmin connect, или отслеживается потребление пищи в приложении с социальными сообществами Strava и т. д. Соответственно тот, кто получает доступ ко всей этой информации, может составить представление как о социальном статусе индивидуума, так и о его физическом, финансовом состоянии, политических взглядах. Все эти данных могут быть использованы против самого владельца этих данных.

Деструктивные социальные группы

Информационная безопасность личности определяется защищенностью ее психики и сознания от опасных информационных воздействий, таких как манипуляции, дезинформация, побуждение к самоубийству. Примером могут служить деструктивные группы в социальных сетях Синий кит [1] или социальные группы «школьных стрелков» [2], направленные на суицид и причинение вреда другим. Сейчас активно борются с этим явлением как силами блокировки таких каналов, так и путем разъяснения родителям детей, как распознать ту или иную группу, в которой состоит их ребенок. В ближайшее время появится перспектива, что за счет технологий машинного обучения такие группы будут блокироваться на начальном этапе их создания, так как везде они создаются по шаблону, – имеют в названии ключевые слова: «Синяки», «камень», «могила»…, и имеют типовую целевую аудиторию. И если на администрацию сетевого ресурса возложить перлюстрацию незаконно, то на искусственный интеллект вполне возможно возложить эти функции. Причем по такой схеме на текущий момент выявляется рассылка спам-контента в Интернете.

Фейковый контент

Важно заметить, что информационные воздействия опасны (или полезны) не столько сами по себе, сколько из-за их способности вызывать мощные процессы и управлять ими.

Кроме межличностной коммуникации, современные социальные сети часто используются манипуляторами для провокации общественных протестов, вооруженных конфликтов и захвата власти насильственным путем. Для управления и воздействия на человека используются специальные манипулятивные технологии, такие как фейковые фотографии, которые обычно используются для придания эмоционального оттенка или драматизации описываемого события. Существуют несколько типов фотоманипуляций:

1) настоящее изображение лица или места с подписью другого места или лица;

2) фотографии, отредактированные в графических редакторах для изменения определенных объектов (добавления или удаления элементов);

3) обрезанные фотографии, которые показывают только часть изображения, создавая впечатление вырывания из контекста необходимого материала. Можно выделить ряд признаков манипулятивного воздействия в социальных сетях, таких как скрытность, умелое оперирование информацией, латентное влияние на выбор, акцент на «массовых людях», побуждение к определенному поведению, создание иллюзии приспособления к новому, мастерство влияния и другие. Работа в социальных сетях может влиять на центр удовольствия в мозге, что приводит к зависимости от них из-за предоставления контента мелкими порциями в нужной тональности.

Рассылка фейкового контента стала большой проблемой во время эпидемии COVID-19. Массовая дезинформация оказала влияние на темпы вакцинации и самолечения. В научной работе «Social media and the COVID-19 pandemic: Observations from Nigeria» [3] был изучен вопрос в целом: есть ли зависимость между религиозными взглядами/политическими предпочтениями/этническими группами и внушаемостью дезинформации.

Дофаминовая петля

Согласно данным ВЦИОМ за 2023 г. [4], большинство россиян (86%) ежедневно проводят время в социальных сетях и сервисах для общения. Особенно активно их используют молодые люди: 92% в возрасте 18–24 лет и 94% в возрасте 25–34 лет.

Эти сервисы значительно превосходят другие виды досуга по частоте использования: просмотр телевизора (50%), прогулки (48%), чтение книг (27%) и спорт (15%).

В среднем россияне тратят 4.5 часа в день на социальные сети и сервисы для общения, а молодежь (18–24 лет) – более 8 часов в день.

Бывший вице-президент по росту пользователей Facebook (соцсеть, принадлежащая запрещённой в России организации) Чамат Палихапития в интервью The Sydney Morning Herald [5] выразил глубокое сожаление о своей роли в развитии этой платформы. Он считает, что социальные сети наносят вред обществу во всем мире, разрушая социальные связи и распространяя дезинформацию: «Движимые дофамином краткосрочные петли обратной связи, которые мы создали, уничтожают то, как работает общество. Никакого цивилизованного диалога, никакого взаимодействия, дезинформация, ложь. Это глобальная проблема.

Мы строим наши жизни вокруг чувства совершенства, потому что мы получаем награду в виде этих краткосрочных сигналов – «сердец», лайков, «больших пальцев» – и мы приравниваем их к ценностям, к правде. Но на самом деле, это краткосрочная, фальшивая, хрупкая популярность, которая, признайте это, оставляет вас еще более пустым, чем до ее получения». Палихапития не первый бывший сотрудник этой компании, который критикует ее негативное влияние. Он привел в пример трагедию в Индии, где фейковое сообщение о похищении детей, распространившееся через WhatsApp (мессенджер, принадлежащий запрещённой в России организации), привело к убийству двадцати трех невинных людей, которых приняли за преступников и линчевали [6].

Работа в социальных сетях оказывает влияние на центр удовольствия в мозге. Желание повторного ощущения этих эмоций заставляет человека проводить там все больше времени. Человек получает разную информацию порциями за короткий промежуток времени. Мозг быстро адаптируется к такому режиму работы из-за удобства, быстроты и доступности социальных сетей, что способствует формированию зависимости. Предоставление контента в небольших дозах в нужной форме способствует нейролингвистическому программированию, позволяющему распространять слухи, поданные манипуляторами в виде «вырванных» фрагментов информации, и вызвать необходимую эмоциональную реакцию у пользователей.

Манипуляции общественным мнением

Социальные сети часто используются для манипулятивного влияния на общественное сознание населения страны и для информационного противостояния на международном

уровне. В условиях гибридной войны опасное деструктивное информационно-психологическое влияние, направленное на разжигание национальных, религиозных и других конфликтов, ненависти и неповиновения, реализуется в популярных социальных сетях, таких как ВКонтакте, Одноклассники, Facebook (соцсеть, принадлежащая запрещённой в России организации) и другие.

Факторами этого опасного воздействия являются:

• неспособность посетителей социальных сетей анализировать большие объемы информации и проверять ее на достоверность;

• недостаточная техническая подготовка пользователей массовой коммуникации для получения качественной информации из социальных сетей.

Это может привести к тому, что пользователи социальных сетей становятся жертвами деструктивных манипулятивных технологий, враждебной пропаганды, специальных информационных операций и других влиятельных действий, активно проводимых в глобальном информационном пространстве.

Примером может служить деструктивная вербовка наших граждан и провоцирование их за деньги проводить противоправные действия. Так, количество поджогов электроавтоматики на московской железной дороге в 2023 г. возросло втрое [7]. Как правило, опасные информационные воздействия делятся на виды.

Первый связан с утратой ценной информации, это могут быть методы социальной инженерии, когда путем изучения информации, выложенной зачастую в открытом доступе, злоумышленники получают данные жертвы. В дальнейшем эти данные могут нанести уже экономический урон, когда злоумышленники путем социальной инженерии получают доступ к банковскому аккаунту жертвы и переводят средства на свой счет. Однако такие действия могут нанести урон не только физическому лицу, но и организации/предприятию, и даже государству в целом. Если говорить об организациях, то тут утечка информации может быть организована через сотрудников предприятий. Если же говорить о государстве в целом, то утечка информации может быть через людей, которые обладают доступом к государственной тайне, и могут иметь место методы OSINT, когда данные собираются из открытых источников и анализируются. На основании этой аналитики делаются выводы о тех или иных процессах в отрасли. В свою очередь, согласно отчету экспертов компании F.A.C.C.T. [8], Россия лидирует на рынке скомпрометированных данных в странах СНГ. Так, в 2023 г. значение UCL (облака логов) составили 7886, что почти в 4 раза больше, чем у страны, находящейся на втором месте рейтинга. Второй вид информационного влияния связан с распространением негативной информации, что может привести не только к опасным ошибочным решениям, но и заставить нанести вред, даже привести общество к катастрофе. Информационная безопасность этого вида должна обеспечивать специальные структуры информационно-технической борьбы. Их задача состоит в нейтрализации дезинформации, предотвращении манипулирования общественным мнением и ликвидации последствий компьютерных атак. Как пример можно представить революцию в Египте в 2011 г., которая в целом координировалась через социальную сеть Facebook (соцсеть, принадлежащая запрещённой в России организации) [9]. Соответственно деструктивные действия в обществе могут координироваться через социальные сети. Вторым примером может выступать история с девочкой Баной из Алеппо, когда фейковый аккаунт [10] девочки был создан с целью дискредитации Российской Федерации и ее вооруженных сил. Соответственно фейковые аккаунты могут создавать определенный нарратив, направленный на формирование отношения к тому или иному событию в нужном ключе.

Развитие и внедрение новых информационных технологий в разные сферы жизни общества, как и любых других научно-технических достижений, не только обеспечивают комфортность, но часто несут и определенную опасность.

Современные социальные сети являются одними из наиболее посещаемых ресурсов, предоставляющих возможность мгновенно передавать информацию на любое расстояние в реальном времени значительной аудитории по всему миру. Однако эта возможность может

быть использована для целенаправленных деструктивных влияний на национальное информационное пространство. Это создает угрозу социальной опасности, связанной с использованием технологий искусственного изменения поведенческих реакций человека и влияния на его свободу волеизъявления. Давно уже используются таргетинговые технологии в социальных сетях для проведения маркетинговых акций. По сути дела, делается выборка целевой аудитории, на которую рассчитана реклама, – это может быть целевой регион, возраст, пол или ищутся люди с конкретными интересами (которые люди указывают в анкете). Однако не только для маркетинга используется составление таких выборок. Новые угрозы включают в себя неосознанные информационные влияния, формирование искусственной психической зависимости и манипулирование общественным сознанием, что может привести к скрытому возбуждению у пользователей социальных сетей намерений, не отвечающих их реальным желаниям.

В качестве примера выступает скандал с компанией Cambridge Analytica [11], которая была обвинена в незаконном сборе данных о профилях пользователей соцсетей без их согласия. Согласно статьям в The Guardian и The New York Times, компания использовала психологический тест, разработанный профессором психологии Алексом Коганом, для сбора информации о пользователях и их друзьях на Facebook. Эти данные затем использовались в предвыборной кампании Дональда Трампа, где персонализированная политическая реклама показывалась пользователям на основе их профилей.

Компания Cambridge Analytica собрала данные о профилях 50 миллионов людей, используя тест, который не только запрашивал информацию о пользователях, но и анализировал их лайки. Эти данные позволяли строить модели поведения людей и предсказывать их политические предпочтения.

Хотя Коган утверждал, что тест собирал данные в академических целях, в действительности он продавал их компании Cambridge Analytica. Этот скандал выявил проблемы с защитой данных пользователей в социальных сетях и вызвал широкий общественный резонанс.

В свою очередь Джо Байден на тех же выборах использовал следующую схему таргетинга и ретаргетинга [12]. Рекламные расходы были направлены на ключевые штаты, такие как Айова и Невада, где проходили ранние праймеризы, а также на такие крупные штаты, как Калифорния, Техас, Нью-Йорк и Флорида перед "супервторником" и для укрепления позиций на будущее. Реклама на Facebook была ориентирована в основном на избирателей в возрасте 55 лет и старше (67%) и на женщин (64%), в свою очередь у Трампа таргетинг и ретаргетинг были нацелены больше на мужскую аудиторию (52%) [13]. Такие технологии, как Pre-roll и mid-roll (видео-реклама длительностью 30 секунд, которую демонтировали перед или в середине целевого контента), больше использовались на выборах 2010 г. [14].

При этом сам контент социальных сетей содержит огромные объемы информации, которая не всегда является качественной, достоверной и объективной. А с появлением в широком доступе ChatGPT 4 объем контента будет только увеличиваться. И использование технологии Deepfake с помощью нейросетей создает большую проблему в идентификации и отделения реальной информации от сфабрикованной. Пользователи также представляют правдивые данные о себе и публикуют свои фотографии с целью лучшего познания жизни других. Это приводит к двум ключевым проблемам: защита пользователей от воздействия недостоверной информации и защита самой информации пользователей.

Сегодня манипулятивное влияние на психику человека в социальных сетях возможно не только при непосредственном контакте, но и через интернет-ресурсы. Одной из главных задач манипуляторов является введение «сенсационной» информации среди пользователей социальных сетей с целью дальнейшей трансляции этой информации широкой аудитории, представляя ее как общее мнение и настроение определенной части общества. Современные информационные технологии в социальных сетях используют различные методы манипулятивного воздействия, включая прием социального доказательства, направленный на использование группового инстинкта «массового человека», принимающего навязанное ему иллюзорное поведение большинства. Это вызывает «эффект толпы» – «как большинство, так и я» –

и не требует дополнительных усилий для проверки информации на достоверность. Кроме того, за счет использования фильтров персональных подборок может проявиться явление «Пузырь фильтров», или идеологический фрейм – это когда Персонализированный поиск, системы рекомендаций и алгоритмическое кураторство могут привести к состоянию интеллектуальной изоляции, известному как «информационный пузырь».

Пользуясь социальными сетями для поиска информации, люди сами решают, каким источникам доверять, и потом ориентируются на них. Одним из способов манипулирования общественным мнением является влияние высказываний или позиций популярных блогеров, считаемых лидерами мнений. Однако иногда лидеры мнений оказываются вовлеченными либо в экономические манипуляции, либо в политические. Условно говоря, канал блогера, который никогда не занимался политическими темами, набрав аудиторию несколько миллионов пользователей вдруг начинает высказываться на политические события, тем самым навязывая свое мнение. Либо, что более часто происходит, манипулирует и скрыто рекламирует участвовать, допустим, в криптовалютных проектах.

В информационном пузыре результаты поиска и рекомендации основаны на информации о пользователе, такой как его местоположение, история поиска и поведение при кликах. Это приводит к тому, что пользователи в основном видят информацию, которая соответствует их существующим взглядам, и изолируются от информации, которая им противоречит.

В результате пользователи оказываются в культурных или идеологических пузырях, что приводит к ограниченному и индивидуальному взгляду на мир. Выбор, сделанный этими алгоритмами, часто непрозрачен, что затрудняет пользователям понимание того, почему они видят определенный контент.

Юридическая сторона вопроса

Многие телеграмм-каналы имеют большое количество подписчиков и распространяют новости. Соответственно они являются средством массовой информации. Более того, Невский районный суд города Санкт-Петербурга признал анонимный Telegram канал «Занавеска Закса» средством массовой информации, однако сетевое средство массовой информации, согласно Закону РФ от 27.12.1991 N 2124-1 (ред. от 13.06.2023) «О средствах массовой информации», необходимо регистрировать в Роскомнадзоре.

Доступные дипфейки позволяют обходить системы идентификации лиц, осуществлять мошеннические действия и получать доступ к конфиденциальной информации о компаниях. Уже на сегодняшний день защититься от этого предлагается верификацией через биометрические данные[15]. Так, например, по данным отчета Onfido [16], в 2023 г. количество попыток мошенничества с использованием дипфейков увеличилось в 31 раз по сравнению с предыдущим годом.

IT-компании больше не способны самостоятельно регулировать публикуемый контент, и большинство стран занимается изменением законодательства с целью недопущения негативного влияния на общество в целом. Так, Австралия принялась регулировать свое законодательство в сфере информационной безопасности только после терактов в мечети [17]. Соответственно важно заранее разработать юридические положения, которые предотвратят такие события. Если рассматривать возможности частичного решения проблемы, то можно было бы решить их путем применения нейросетей, обученных на модели системы поддержки принятия решений [18–19]. Власти штатов Флорида, Огайо, Арканзас, Техас, Юта в США вообще пошли на кардинальные меры и запретили молодым людям до достижения 16 лет создавать аккаунты в социальных сетях и видеохостингах без разрешения родителей.

Обсуждение результатов

Исходя из рассмотренных проблем и опираясь на опыт их решения в других государствах можно сделать вывод, что необходимо, чтобы правовое регулирование СМИ распространялось и на мессенджеры, и на социальные сети. Сейчас все чаще можно столкнуться со сборами денежных средств в месенджерах и социальных сетях, однако в то же самое время из-за анонимности люди даже не в курсе, кому они конкретно отдают свои деньги.

Также необходимо срочное правовое регулирование технологии Deepfake, так как с каждым годом будет только возрастать количество мошеннических схем с участием этой технологии.

Возможно, стоит обратить внимание на опыт других стран и ограничить доступ к социальным сетям молодым людям, не достигшим 16-летнего возраста.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

1. Алгави Л. О., Кадырова Ш. Н., Расторгуева Н. Е. «Синий кит»: пять аспектов новостного нарратива //Вестник Российского университета дружбы народов. Серия: Литературоведение, журналистика. 2017. Т. 22. № 4. С. 660-668. [[Algavi L. O., Kadyrova Sh. N., Rastorgueva N. E. “The Blue Whale: Five aspects of the news narrative” (In Russian) // Vestnik RUDN, vol. 22, no. 4, pp. 660-668, 2017.]]

2. Peshkovskaya A. Suicide-related groups and school shooting fan communities on social media: a network analysis // Computers. 2024. Vol. 3. No. 13. Pp. 61.

3. Obi-Ani N., Anikwenze C., Isiani M. Social media and the Covid-19 pandemic: observations from Nigeria// Cogent Arts & Humanities. 2020. Vol. 1. No. 7. Pp. 179-483.

4. Социальные сети и мессенджеры: вовлеченность и предпочтения [Электронный ресурс]. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/socialnye-seti-i-messendzhery-vovlechennost-i-predpochtenija (дата обращения: 02.03.2024). [[Social networks and instant messengers: involvement and preferences [Online], (in Russian) URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/socialnye-seti-i-messendzhery-vovlechennost-i-predpochtenija]]

5. Wang A. Social media destroying society with 'dopamine-driven feedback loops': ex-Facebook VP // The Sydney Morning Herald. Para. 12 Dec. 2007. [Online] Available: https://www.smh.com.au/world/social-media-destroying-society-with-dopaminedriven-feedback-loops-exfacebook-vp-20171213-h03jfo.html [March. 02, 2024].

6. Rajput R. Murderous mob – 9 states, 27 killings, one year: and a pattern to the lynchings // The Indian Express. Para. 15 July. 2018. [Online] Available: https://indianexpress.com/article/india/murderous-mob-lynching-incidents-in-india-dhule-whatsapp-rumour-5247741/ [March. 02, 2024].

7. Число поджогов электроавтоматики на МДЖ в 2023 году возросло втрое [Электронный ресурс]. URL: https://tass.ru/proisshestviya/18087733 (дата обращения: 02.03.2024). [[The number of arson attacks on electrical equipment at MRR has tripled in 2023 [Online], (in Russian). URL: https://tass.ru/proisshestviya/18087733]]

8. Киберпреступность в России и СНГ. Тренды, аналитика, прогнозы 2023–2024 [Электронный ресурс] URL: https://www.facct.ru/resources/research-hub/cybercrime-trends-annual-report-2023-2024/ (дата обращения: 02.03.2024). [[Cybercrime in Russia and the CIS. Trends, analytics, forecasts 2023–2024 [Online], (in Russian). URL: https://www.facct.ru/resources/research-hub/cybercrime-trends-annual-report-2023-2024/]]

9. Hamanaka S. The role of digital media in the 2011 Egyptian revolution // Democratization. 2020. Vol. 5. No. 27. Pp. 777-796.

10. Douglas K. Twitter, the child, and the war diary // Textual Practice. 2020. Vol. 34. No. 6. Pp. 1021-1039.

11. Afriat H. ’This is capitalism. It is not illegal’: Users’ attitudes toward institutional privacy following the Cambridge Analytica scandal // The Information Society. 2020. Vol. 37. No. 2. Pp. 115-127.

12. Alashri S., Alalola T. Functional analysis of the 2020 US elections on Twitter and Facebook using machine learning // Proc. ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)’02. 2020. Pp. 586-589.

13. Tasente T. Facebook discourse analysis of US president Donald Trump // Technium Soc. Sci. J. 2020. Vol. 5. No. 1. Pp. 26.

14. Shaw D., Blunt C., Seaborn B. Testing overall and synergistic campaign effects in a partisan statewide election // Political Research Quarterly. 2018. Vol. 71. No. 2. Pp. 361-379.

15. Миронова Н. Г. Методы антиспуфинга в системах биометрической идентификации и верификации // Информационные технологии обеспечения комплексной безопасности в цифровом обществе. 2021. С. 43-51. [[Mironova N. G. “Anti-spoofing methods in biometric identification and verification systems” // Information Technologies for Ensuring Comprehensive Security in the Digital Society, pp. 43-51, 2021.]]

16. Identity Fraud Report 2024 // Onfido. Para. 10, Jan. 2024. [Online] Available: https://onfido.com/landing/identity-fraud-report/ [March 10, 2024].

17. Wellman M. Ethics of authenticity: Social media influencers and the production of sponsored content // Journal of Media Ethics. 2020. Vol. 35. No. 2. Pp. 68-82.

18. Сазонова Е. Ю., Сметанина О. Н., Журавлева К. И., Юлаев Р. С. Интеллектуальная СППР при управлении психофизическим состоянием человека // Системная инженерия и информационные технологии. 2023. Т. 5. № 6(15). С. 38-49. EDN JFLRCX.

[[E. Yu. Sazonova, O. N. Smetanina, K. I. ZHuravleva, R. S. Yulaev. “Intelligent DSS for managing the psychophysical state of a person“ // Systems Engineering and Information Technology, vol. 5, no. 6, pp. 38-49, 2023. EDN JFLRCX.]]

19. Закиева Е. Ш. Методология поддержки принятия решений при управлении социетальной системой на основе динамического моделирования и интеллектуальных технологий // Системная инженерия и информационные технологии. 2023. Т. 5. № 3(12). С. 69-92. EDN UWIPDO. [[Zakieva E. Sh. “Methodology for decision support in managing a societal system based on dynamic modeling and intelligent technologies“ // Systems Engineering and Information Technology, vol. 5, no. 3, pp. 69-92, 2023, DOI 10.54708/2658-5014-SIIT-2023-no3-p69. EDN UWIPDO]]

20. Singer N. Florida passes sweeping bill to keep young people off social media // The New-York Times. Para. 12, Feb. 2024. [Online] Available: https://www.nytimes.com/2024/02/23/business/florida-social-media-youths.html [March 10, 2024].

Поступила в редакцию 7 марта 2024 г.

МЕТАДАННЫЕ / METADATA

Title: Destructive and manipulative influence of social networks.

Abstract: The article examines the types of destructive manipulative effects of social networks on society. Technologies for searching for potential electorates in the 2020 US elections are considered, where an opinion about a particular candidate was formed using targeting and re-targeting. The destructive influences of suicidal groups on social networks were also considered. The statistics of the All-Russian Center for the Study of Public Opinion on the use of social networks by time are presented – most Russians spend time on social networks and communication services every day, young people are especially active in using them. Social media use can affect the pleasure center of the brain, leading to addiction due to the provision of content in small portions in the right tone. The article describes that social networks are often used by manipulators to provoke public protests, armed conflicts, and violent seizure of power. At the same time, the information security of an individual is determined by the protection of his psyche and consciousness from dangerous information influences, such as manipulation, disinformation, incitement to suicide, and participation in illegal actions. A negative impact is indicated in the form of the spread of misinformation, such as in particular regarding the anti-vaccination movement during the COVID-19 epidemic. It is concluded that it is necessary to carry out legal regulation in relation to deepfake technologies following the example of the experience of other states. The issue of legal regulation of information news groups in social networks as a mass media and in general legal regulation of social networks is raised. It is concluded that it is necessary to carry out legal regulation in relation to deepfake technologies following the example of the experience of other states.

Key words: information, social, networks, users, data, security, technologies, manipulation.

Язык статьи / Language: русский / Russian.

Об авторе / About the author:

ДАИРБЕКОВА Жулдуз Муратхановна
Донской государственный технический университет, Россия.
Магистрант кафедры вычислительных систем и информационной безопасности.
E-mail: dairbekova.z@mail.ru

ПОЛУЯН Анна Юрьевна
Донской государственный технический университет, Россия.
Доцент кафедры вычислительных систем и информационной безопасности, канд. техн. наук.
E-mail: orfiki@rambler.ru
URL: https://elibrary.ru/author_items.asp?authorid=549590

DAIRBEKOVA Zhulduz Muratkanovna
Don State Technical University, Russia.
Master's student at the Department of Computing Systems and Information Security.
E-mail: dairbekova.z@mail.ru

POLUYAN Anna Yuuryevna
Don State Technical University, Russia.
Associate Professor of the Department of Computer Systems and Information Security, Ph.D. tech. sciences.
E-mail: bogdanov_marat@mail.ru
URL: https://elibrary.ru/author_items.asp?authorid=549590