УДК 004.056.53

А. В. Тонкошкурова

Тренды применения социальных технологий в киберпространстве

Аннотация:

В статье рассматривается одна из глобальных проблем цифровой среды – использование социальных технологий для манипулирования пользователями социальных сетей и Интернет-ресурсов. Главная причина возникновения этой проблемы заключается в том, что в условиях активного развития информационных технологий формируется информационная зависимость, касающаяся людей, участвующих в процессе производства, хранения и использования информации в ходе информационного взаимодействия. Оно порождает ряд социальных трансформаций, формируя новые виды рисков, вызовов и угроз, таких как информационные войны, информационное оружие, информационный терроризм, информационная преступность, изменяя и социальные технологии воздействия на пользователей сети Интернет. Все это обусловливает актуальность исследования отношения населения к социальным технологиям манипулирования пользователями цифровой среды для выявления причин их уязвимости перед кибератаками.

Ключевые слова: цифровая среда, социальные технологии, социальная инженерия, информационная безопасность, кибермошенники, фишинг, вирусные ссылки, троянская программа, обратная социальная инженерия.

Об авторе: Тонкошкурова Анастасия Витальевна, МГТУ им. Н.Э. Баумана, магистр кафедры «Социология и культурология»; эл. почта: paleeva1772@mail.ru

Научный руководитель: Сазонова Анна Львовна, МГТУ им. Н.Э. Баумана, кандидат социологических наук, доцент кафедры «Социология и культурология»; эл. почта: sazonova@bmstu.ru

Жизнь современного человека протекает в уникальных условиях – человек оказывается включенным в «интегральную реальность» как область соотношения естественной, социальной

и виртуальной сред. В этой области функционируют эффекты, возникшие в результате взаимодействия процессов и феноменов естественного, социального и виртуального характеров. К ним относят эффект технологизации человека, «апгрейда реальности» и др. [1]. Активность подобного рода эффектов приводит к изменениям физического и психического состояния человека, влияя на его мышление, трансформируя индивидуальную и социальную ментальность, предопределяя поведение и выбор жизненных стратегий. Значительную роль в процессах развития современного человека и общества играет информационно-сетевая среда – неотъемлемый компонент интегральной реальности. Эта среда отличается рядом особенностей: функционирование в онлайн-режиме, цифровое содержание, оформленность в киберпространстве, знаково-символьная перегруженность, безграничность информационных полей, сетевая структура, наличие мем-комплексов и их реконструкции [2].

Благодаря процессу информатизации в обществе происходят системные изменения, в соответствии с которыми каждый человек включаются в глобальное информационное пространство, становясь элементами глобальной информационной системы и, соответственно, в той или иной степени зависимым от нее. При этом интеграция человека в информационно-сетевое пространство за два-три десятилетия активного пользования Интернетом позволила почувствовать себя комфортно и безопасно. Но так ли это на самом деле? Может ли человек чувствовать себя в безопасности в новом высокотехнологичном мире? Инновационные и нестандартные технологические подходы к развитию общества обусловливают риски нарушения всей системы кибербезопасности. Иными словами, возникает проблема, с которой сталкиваются пользователи сети Интернет – манипулировать ими, применяя социальные технологии, становится гораздо легче.

В анкетном онлайн-опросе приняли участие жители Московского региона, активные пользователи Интернет, сталкивающиеся с социальными технологиями манипулирования ими в цифровой среде. Было выявлено отношение населения Московского региона к этим технологиям. Гипотеза исследования заключалась в следующем: специфика отношения активных пользователей социальных сетей и Интернет-ресурсов к социальным технологиям как инструменту кибермошенничества проявляется в низкой степени информированности о способах воздействия; в наличии технического образования у пользователей социальных сетей и Интернет-ресурсов; в возрастной категории пользователей (наиболее подверженными технологиям манипулирования становятся подростки и пожилые люди).

Социальные технологии и социальная инженерия в контексте информационной безопасности

В современном обществе значительно возрастает не только производство новых знаний, но и возможность целевой манипуляционной «настройки» тех знаний, которые усваивает человек. Такая «настройка» осуществляется при помощи специально разработанных социальных технологий, многократно усиливающих уровень воздействия на индивида. Социальные технологии могут быть потенциально применены кибермошенниками в качестве способа управления действиями людей в цифровой среде. Они многосубъектны и представляют собой структурированные действия по «обработке людей людьми», включая то, что называется человеческим фактором. Социальные технологии можно определить как «социальное знание, трансформированное в конкретные модели практических действий для достижения заранее определенных целей» [5, с. 333-334].

Развитие информационных технологий значительно облегчает и усиливает влияние на людей. Во-первых, проблема заключается в излишней доверчивости пользователей Интернет к фейк-ньюс и новостям, затрагивающим непосредственное окружение «жертвы» кибератаки. Во-вторых, уже сегодня существует множество разнообразных технологий, которые кибермошенники используют для «выслеживания жертвы». Совокупность эмоционального и технического воздействия и формирует систему социальных технологий в информационной среде.

Особое внимание в структуре информационной безопасности занимают не только социальные технологии, но и социальная инженерия. Она имеет многогранное и широкое толкование – в научной литературе под ним часто подразумевают деятельность, ориентированную на целенаправленное изменение и регулирование различных организационных структур, а также теоретическую и практическую деятельность, направленную на создание и использование набора средств воздействия на поведение людей [3, с. 53]. Так, например, бывший хакер Кевин Митник прямо определял социальную инженерию как искусство обмана, а социального инженера как манипулятора, использующего обман, влияние и убеждение для того, чтобы получить информацию [4]. Это напрямую отражает главную проблему исследования.

Социальные технологии определяются как модели, благодаря которым кибермошенники осуществляют воздействие на пользователей социальных сетей и Интернет, а социальная инженерия – конкретные методы воздействия с применением инженерных

подходов. Социальная инженерия непосредственно входит в состав модели социальных технологий, являясь частью системы. За сохранность данных отвечают их непосредственные владельцы, для которых они имеют ценность. Существующие или предполагаемые нарушители могут придавать значение этим данным, что приводит к возникновению угроз.

Характеристика респондентов

В анкетном опросе населения Московского региона об их отношении к социальным технологиям как инструменту кибермошенничества приняло участие 139 респондентов в период с 5 по 14 мая 2023 г. Отметим, что объект исследования – активные пользователи социальных сетей и Интернет-ресурсов, которые сталкивались с социальными технологиями воздействия на них в цифровой среде. Поэтому в опросе было два отсеивающих вопроса, которые позволили произвести чистку выборки и оставить ответы респондентов, важные для исследования. В ходе выбраковки из 139 респондентов к анализу предлагаются ответы 115 ответивших на анкетный опрос.

Характеристика респондентов такова: в опросе приняло участие 69 женщин (60%) и 46 мужчин (40%). Проведем краткую характеристику по каждой категории респондентов.

1. В анкетном опросе приняло участие 69 женщин преимущественно в возрасте от 18 до 24 лет, с уровнем дохода от 20 до 50 тысяч рублей, с гуманитарным уклоном образования. Большинство из них часто используют социальные сети и Интернет-ресурсы (от 6 до 8 часов в сутки) и это становится частью их профессиональных обязанностей.

2. В анкетном опросе приняло участие 46 мужчин преимущественно в возрасте от 25 до 55 лет. Уровень дохода варьируется от 51 до 100 тысяч рублей и более. Уклон образования в большей степени гуманитарный. Большинство респондентов часто используют социальные сети и Интернет-ресурсы, в частности, в рамках рабочего времени, в общении с коллегами для решения рабочих вопросов.

Отношение респондентов к технологиям воздействия на них в социальных сетях и Интернет-ресурсах делится на информированность об этом явлении и его оценку.

Степень информированности о характере социальных технологий

Только половина (52%) утверждает, что знает о социальных технологиях как инструменте кибермошенничества в социальных сетях и Интернет-ресурсах. 40% заявляют о своей частичной информированности. Активные пользователи социальных сетей и Интернет прекрасно понимают, что в настоящее время в цифровой среде ведутся активные действия

кибермошенников, которые направлены на их персональные, личные и конфиденциальные данные.

Наиболее понятными для респондентов стали следующие социальные технологии: фишинг (83%), вирусные ссылки (73%), а также троянская программа (70%) и сбор информации из открытых источников (70%). В целом, можно утверждать, что кибератаки совершаются в основном на логины и пароли аккаунтов социальных сетей и Интернет-ресурсов – на это направлены фишинг, вирусные ссылки и частично сбор информации о жертве.

Информированность о социальных технологиях непосредственно связана с кибератаками, совершенными на конфиденциальные, персональные и личные данные активных пользователей цифровой среды, поскольку именно фишинг (63%), несуществующие ссылки (50%) и троянская программа (41%) отмечены респондентами, как наиболее часто примененными против них.

Стоит отметить, что наиболее опасными социальными технологиями, по мнению опрошенных, выступают троянские программы (59%), фишинг (55%) и «дорожное яблоко» (51%), большинство из которых направлены на полное уничтожение данных с электронного носителя. При этом, чаще всего респонденты используют мобильный телефон (96%) и ноутбук (70%), в то время как на смартфон чаще всего проводились все перечисленные ранее кибератаки (90%).

Степень информированности о последствиях негативного воздействия социальных технологий

Респонденты обратили внимание на кибермошенников, с которыми им приходилось чаще всего сталкиваться, а именно на хакеров (66%), аферистов (49%) и воров личной информации (41%). Прежде всего, это люди, занятые цифровым взломом, кражей, удалением или подменой данных, выведением оборудования из строя, вымогательством, шантажом, использованием данных для оформления кредитов и т.д. Иными словами, они осуществляют несанкционированный доступ к цифровой информации и электронным системам, что и становится одной из главных проблем цифровой среды. Об этом же заявляют 87% опрошенных, считая социальные технологии и все, что с ними связано, одной и главных проблем информационной среды. Активные пользователи социальных сетей и Интернет-ресурсов заявляют, что действия киберпреступников нацелены напрямую на денежные средства жертвы (88%) и личную информацию с целью шантажа (59%). Таким образом, все действия направлены на получения максимальной денежной выгоды, в свою очередь их

отследить практически невозможно, как и вернуть обманутым пользователям или жертвам финансовые средства.

Что касается количества кибератак, совершаемых на активных пользователей социальных сетей и Интернет-среды, то здесь можно использовать таблицу сопряженности, чтобы отразить не только количество атак, но и проследить, кто в наибольшей степени им подвержен.

Таблица 1. Распределение респондентов по полу в зависимости от количества кибератак

	Количество респондентов	**% от числа ответивших**
1 кибератака	**28**	**24%**
Женский	14	12%
Мужской	14	12%
2-3 кибератаки	**55**	**48%**
Женский	44	38%
Мужской	11	20%
4-5 кибератак	**15**	**13%**
Женский	3	3%
Мужской	12	10%
Более 5 кибератак	**17**	**15%**
Женский	8	7%
Мужской	9	8%
Общий итог	**115**	**100%**

Чаще всего происходило от 2 до 3 кибератак, в большинстве случае с которыми сталкивались женщины. Стоит отметить, что мужчины чаще всего сталкивались с 4 и более кибератаками (в общей сложности 21 респондент – практически половина опрошенных мужчин). В общей сложности около 76% всех респондентов более 2 раз сталкивались с кибермошенничеством. Это не просто единичные случаи, а целенаправленные атаки на персональные данные респондентов и их финансовые средства. В свою очередь, это доказывает значимость этой проблемы в рамках цифровой среды.

Что касается мнения опрошенных о самой незащищенной социальной сети, то здесь стоит отметить социальную сеть «Вконтакте» (VK) (об этом заявляет 90% всех респондентов). У полученной статистики есть свои причины. Обратимся к блогу Д. Куликова: «Опасность

социальной сети Вконтакте для пользователей», расположенном на официальном сервисе Яндекс.Дзен. Эксперт обращает внимание на нарушение тайны переписки, что представляет собой одну из самых больших угроз, которую представляет данная социальная сеть. Переписку активно используют маркетологи, чтобы предоставлять рекламные объявления для продвижения своих товаров или услуг. Любой человек видит, когда вы пользуетесь социальной сетью с компьютера, а когда с телефона. С помощью этой информации можно сразу же понять, дома пользователь или нет. На каждой странице можно увидеть надпись «заходил час назад» или «заходил в 03:59». Любой человек может узнать, когда пользователь ложится спать, а когда просыпается, что нарушает конфиденциальность данных [6]. Чужие профили легко скопировать, тем самым шантажируя родных и близких. Средствами защиты в VK становятся предупреждение о том, что в аккаунт кто-то зашел; перевод аккаунта в «закрытый» режим; ограничение возможности отправки сообщений для посторонних лиц. Однако, по мнению респондентов, этого недостаточно для того, чтобы чувствовать себя в безопасности.

Среди главных последствий столкновения пользователей социальных сетей и Интернет-ресурсов с кибератаками в цифровой среде можно выделить взлом страницы в социальных сетях с целью вымогательства денежных средств у друзей и близких (61%), а также воровство паролей социальных сетей, интернет-магазинов и учетных записей (59%) для дальнейшего распоряжения данными.

Психологическое состояние опрошенных после взаимодействия с социальными технологиями достаточно разнообразно:

- у 34% респондентов возникало чувство паники, страха, смятения, замешательства;
- 26% почувствовали мнительность, тревожность и излишнюю подозрительность к происходящему в цифровой среде;
- 25% опрошенных отнеслась к сложившейся ситуации спокойно, смогла ее преодолеть или же вовремя устранить последствия.

Действия респондентов, направленные на преодоления последствий взаимодействия с социальными технологиями

Главной возможностью определения кибератаки на персональные данные респондентов становится получение электронного письма и сообщения, что конфиденциальные данные пытаются украсть или взломать (64%). Второй по значимости возможностью, но менее популярной, выступает использование менеджеров паролей, которые не только безопасно их

хранят, но и отслеживают, не попали ли они третьим лицам (29%). 30% опрошенных утверждают, что, к сожалению, определить этого вовремя не удалось.

Среди мер, которые предпринимают пользователи Интернет в результате совершения кибератаки, 82% определяют смену пароля для аккаунтов и звонок в банк для своевременной помощи и сохранения финансовых средств (36%). Учитывая, что большинство атак направлены на социальную сеть VK, смена пароля личной страницы оказывается одной из эффективных мер, как для предотвращения атаки, так и после ее совершения, которой могут воспользоваться респонденты.

Несмотря на попытки респондентов защитить свои данные, киберпреступность продолжает ежегодно расти, и респонденты осознанно признают, что в утечках персональных, личных и конфиденциальных данных виноваты лично они (57%), а также непосредственно хакеры (56%), которым достаточно трудно противостоять.

Главная ошибка, по их мнению, заключается в низкой информированности о социальных технологиях как способе кибермошенничества (83%), а также чрезмерной активности в цифровой среде (49%) и безответственности к угрозам манипулирования (35%).

Оценка социальных технологий как инструмента кибермошенничества

Анализируя оценку социальных технологий как инструмент кибермошенничества, обратимся к индексу этого показателя, диапазон которого находится в пределах от – 1 до + 1. Значение индекса составило –0,86, что говорит о негативном отношении респондентов к явлению. Если рассматривать индекс в разрезе полового признака, то у мужчин наблюдается менее отрицательное отношение (у мужчин индекс составляет –0,8, а у женщин –0,91).

Оценивая средства, обеспечивающие информационную безопасность личных, персональных и конфиденциальных данных, 70% опрошенных отдают предпочтение программным – это антивирусное ПО, межсетевые экраны, средства обнаружения атак и многое другое. Также 62% утверждают, что обеспечивать защиту должны правовые средства, т.е. те, что основываются на действующих в Российской Федерации законах, гарантирующих права и обязанности участникам при работе с информационными ресурсами. При этом, лишь 9% респондентов реально обращаются в правоохранительные органы для решения проблемы, связанной с утечкой данных. Из этого можно вывести несколько предположений: во-первых, по мнению, респондентов законодательство РФ в области информационной безопасности находится не на достаточном уровне для обеспечения реальной защиты; во-вторых, существует недостаточная возможность реальной поимки кибермошенников и возвращения денежных

средств; в-третьих, респонденты понимают, что в утечке данных виноваты лично они, и правоохранительные органы не смогут помочь в данной ситуации; и в-четвертых, сумма денежных средств на столько мала, что не стоит потраченного времени на судебные разбирательства и поимку кибермошенников.

Немалую роль в исследовании играет мнение респондентов о том, кто должен предусматривать сохранность персональных данных пользователей социальных сетей и Интернет-ресурсов. 48% опрошенных утверждают, что лично они должны отвечать за сохранность данных. Еще 30% обращают внимание на органы власти, которые занимаются обеспечением информационной безопасности на территории РФ.

Заключение

Механизмы обеспечения безопасности данных сегодня активно изменяются и совершенствуются, благодаря чему у пользователей возникает иллюзия полной безопасности нахождения в сети Интернет. Однако человека потенциально подстерегают множество киберловушек – фишинг, троянские программы, ссылки на мошеннические сайты и т.д. Развитие Интернета настолько стремительно, что имеющиеся исследования информационных технологий, программного обеспечения и разработок в сфере защиты информации за короткий срок утрачивают актуальность. Вместе с тем специалисты, контролирующие оборот информации, не всегда оказываются ответственными и добропорядочными. В таких условиях актуальными задачами становятся исследование социальных технологий, применяемых киберпреступниками в отечественном Интернет-пространстве.

Преступления в цифровой среде обретают разнообразные формы. Во-первых, это кибератаки, направленные на сети и устройства пользователей (ботнеты, вирусы, вредоносные программы и т.д.); во-вторых, преступления с применением технических устройств (социальная инженерия, фишинговые письма, кибер-сталкинг, кража онлайн-личности). При этом схемы киберпреступлений, совершаемые посредством социальных технологий, остаются одними и теми же на протяжении последних десятилетий, в то время как кибероборона и иные практики обеспечения информационной безопасности не дают нужного эффекта.

Согласно гипотезе, специфика отношения активных пользователей Интернет к социальным технологиям как инструменту кибермошенничества проявляется в низкой степени информированности о способах воздействия, в наличии технического образования у пользователей социальных сетей и Интернет-ресурсов, в возрастной категории пользователей (наиболее подверженными технологиям манипулирования являются подростки и пожилые люди). Исследование показало, что специфика отношения проявляется и в низкой степени

информированности о способах манипулирования (83%), но не проявляется в возрастной категории пользователей и наличии технического образования, поскольку оно не повлияло на большое количество кибератак (в большинстве случаев это от 2 до 3 кибератак).

Библиографический список:

1. Гаврилова Ю. В. Деструктивные социальные технологии в Интернет-пространстве: мировой опыт / Ю. В. Гаврилова, А. В. Тонкошкурова // Социально-гуманитарные знания. 2023. № 4. С. 51-57.

2. Гаврилова Ю. В. Ментальность в контексте взаимодействия социальной и виртуальной реальностей // Гуманитарный вектор. 2022. Т. 17, № 2. С. 82-93.

3. Горбачев А. В. Психологические основы социальной инженерии / А. В. Горбачев, Е. В. Котенко // Обзор.НЦПТИ. 2021. № 3. С. 53-57.

4. Митник К. Искусство обмана / К. Митник, В. Саймон. М.: ДМК Пресс, 2006. 124 с.

5. Орлова И. Б. Социальные технологии и социально-этическая экспертиза инноваций // Вестник Российской академии наук. 2018. Т. 88, №4. С. 333-340.

6. Куликов Д. Опасность социальной сети Вконтакте для пользователей [Электронный ресурс] // Дзен: Издательская платформа компании Яндекс. Режим доступа: https://dzen.ru/a/YhdI3iCDrhLKBYgT (дата обращения 12.04.2023).

Tonkoshkurova A.V. **Trends of application of social technologies in cyberspace**

The article examines one of the global problems of the digital environment – the use of social technologies to manipulate users of social networks and Internet resources. The main reason for this problem is that in the conditions of active development of information technologies, information dependence is formed concerning people involved in the production, storage and use of information during information interaction. It generates a number of social transformations, forming new types of risks, challenges and threats, such as information wars, information weapons, information terrorism, information crime, changing and social technologies of influence on Internet users. All this determines the relevance of studying the attitude of the population to social technologies of manipulating users of the digital environment in order to identify the causes of their vulnerability to cyber attacks.

Keywords: digital environment, social technologies, social engineering, information security, cybercriminals, phishing, viral links, Trojan horse, reverse social engineering.