нарушителем, вероятности продолжения атаки на соседние элементы. Также модель позволяет рассматривать вопросы защиты информации ИС в пространстве состояний ее элементов с учетом динамики изменений состава элементов ИС и правил доступа.

Показана возможность применения результатов для оценки рисков, реализации угроз, потенциала нарушителя, а также для определения актуальных угроз безопасности информации.

Литература:

1. *Остапенко А.Г., Радько Н.М., Калашников А.О. Остапенко О.А., Бабаджанов Р.К.* Эпидемии в телекоммуникационных сетях. – М: Горячая линия – Телеком, 2018. – С. 123-149 .

2. Банк данных угроз безопасности информации. Термины // FSTEC.RU: ФСТЭК России. – URL: https://bdu.fstec.ru (дата обращения 27.09.2021).

3. *Калашников А.О., Бугайский К.А.* Методика оценки возможности реализации информационных угроз // Информация и безопасность. – 2020. – Т. 23. № 2(4). – С. 163-178.

4. *Костина Н.В.* Применение индексов сходства и различия для районирования территорий на основе локальных флор // Известия Самарского научного центра Российской академии наук. – 2013. – Т.15. № 3 (7). – С. 2160-2168.

5. *Калашников А.О.* Модели и методы организационного управления информационными рисками корпораций. – М.: Эгвес, 2011. – 311 с.

6. *Новиков Д.А., Остапенко А.Г., Калашников А.О., Остапенко Д.Г., Соколова Е.С., Уразов М.Ю.* Информационные риски и эпистойкость безмасштабных сетей // Информация и безопасность. – 2015. – Том 18. № 1. – С. 5-18.

Муромцев В.В., Муромцева А.В.

Цифровизация – угрозы и риски

Аннотация: Рассматриваются процессы, происходящие в современном информационном пространстве, которые в условиях глобализации цифровых информационных потоков ставят перед современным обществом целый ряд серьезных проблем и прежде всего в сфере безопасности.

Ключевые слова: цифровизация, технология Веб 2.0, глобализированное информационное сообщество, виртуальное пространство, психоинформационная безопасность

В Доктрине информационной безопасности РФ в разделе «Стратегические цели и основные направления обеспечения информационной безопасности» отмечено, что одним из основных направлений обеспечения информационной безопасности в области государственной и общественной безопасности являются: «обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности».

Наверное, это важнейший тезис в области психоинформационной безопасности населения потому, что касается каждого человека, всего общества особенно в период реализации процесса цифровизации.

Цифровизация – это процесс, о котором сегодня не говорит только ленивый. Предполагается, что он замечательным образом преобразует к лучшему все вокруг, включая производственную и социальную сферы. Однако необходимо понять, насколько безоблачно будущее.

Прежде всего, настораживает та настойчивость и безаппеляционность, с которой формируется цифровое общество и агрессивность действий, с которой реализуется этот процесс, а если обратиться к уже реальному опыту Китая, то возникают определенные сомнения в полезности этих преобразований.

Отметим также, что формирование цифрового общества реализуется в соответствии с определенными решениями давосского клуба и в рамках концепции «Индустрия 4.0», которая была сформулирована в 2011 г. президентом Всемирного экономического форума в Давосе Клаусом Швабом.

Отметим, что информатизация представляла собой процесс создания и добровольного использования информационной инфраструктуры, поддерживающий формирование информационного общества.

Цифровизация – это процесс, поддерживающий становление цифрового общества, в рамках которого реализуется

принудительное использование, созданной информационной инфраструктуры. Такое положение заставляет обратить особое внимание на обеспечение защищенности граждан от информационных угроз.

Без знания цифровых технологий, т.е. без определенной информационной культуры, существование человека в цифровом обществе станет невозможным или весьма некомфортным. Процессы, происходящие в современном информационном пространстве, определяют сегодня тенденции изменения всей мировой информационной культуры.

Глобализация информационных потоков, ставшая следствием тотальной цифровизации информации, ставит перед современным обществом целый ряд серьезных проблем и прежде всего в сфере безопасности.

Переход компьютерных коммуникаций на технологии Веб 2.0 изменил всю технологию коммуникаций в рамках Сети. На первом этапе функционирования Глобальной Сети пользователю предоставлялась возможность только «чтения и редактирования» информации в сети Интернет. Главной особенностью технологий Веб 2.0 стали программные решения, обеспечивающие ничем не ограниченный личностный обмен информацией при формировании глобального информационного пространства. Технологии SST (Social Software Technologies), предоставляют каждому пользователю Сети постоянную возможность ничем не ограниченного участия в создании информационного сообщения, его распространения (обнародования), изменения и продвижения (навязывания). Возникшие в результате появления Веб 2.0 простые возможности самореализации в результате действия эффекта «больших данных» (‘big data’) оказались способны изменить всю информационную структуру общества и потребовали существенной трансформации всех способов управления информационными потоками в социуме [1]. Сегодня на первый план выходит изучение и понимание того, как формируются и развиваются информационные системы, которые состоят из комбинации технических и социальных компонентов – «социотехнические системы». Таким образом, при создании любых технических решений и программных разработок социальные аспекты необходимо рассматривать и учитывать наряду с техническими. В

противном случае исключительно технократически ориентированные концепции делают технические решения не только неэффективными, неточными, но иногда и опасно ошибочными, если они встраиваются в социальный контекст, окружающий системы принятия решений.

Знание теории и практики функционирования социотехнических систем приобретает в современном обществе, которое вступило в эпоху т.н. «пост-цифрового вызова» (postdigital challenge), особую актуальность. Необходимо фундаментальное понимание того, как люди на самом деле работают и живут в группах, организациях, сообществах и других формах коллективной жизни, реализуемых в цифровом информационном пространстве [2]. Без теоретического осмысления этой проблемы и выработки практических рекомендаций по формированию сбалансированной эффективной политики управления современным глобализированным информационным сообществом мы обречены на обострение внутренних противоречий между разными общественными слоями и группами, которые будут усугублять цифровое информационное неравенство (digital divide) всех видов [3]. И здесь полезно обратиться к истории возникновения технологии цифрового социального взаимодействия, которая получила название Веб 2.0. Сегодня можно утверждать, что многие исходные теоретические предположения о социальных последствиях перехода современного информационного общества на этап Веб 2.0 реализовались в той или иной мере и превратились в настоящие вызовы для безопасного функционирования человеческого сообщества. Так, стало очевидным, что социальные сетевые взаимодействия участников коммуникации активно способствуют формированию новых ментальных и поведенческих стереотипов, а также беспрецедентно быстрому их распространению с охватом многомиллионной аудитории. В последнее время и теоретики, и практики информационных технологий все чаще говорят об опасности проявления в социальных сетях феномена группового «коллективного разума» (‘collective intelligence’), проявляющегося через т.н. эффект «мудрой толпы» (‘wisdom of crowd’). Этот эффект основан на презумпции истинности коллективного мнения в противовес мнению индивидуальному, что ведет к распространению и усиленному

навязыванию мнения некоторой референтной группы как единственного источника правильного знания. Можно заметить, что сегодня этот феномен повсеместно активно вторгается в сферу управления информационными потоками, способствуя тем самым плохо контролируемой трансформации информационного состояния общества в целом. В то же время хорошо известно, что реализация информационных связей по сценарной модели «мудрость толпы» приводит к тому, что большинство веб-ссылок в Интернете (семантических связей) формируется не на основе профессиональных знаний, а по принципу «овечьей тропы в горах», т.е. путей, которые «сформировались с течением времени, когда многие животные и люди просто случайно воспользовались ими» [4].

Одним из главных уроков новой информационной революции, начатой с появлением Веб 2.0, как отмечает O'Reilly, стало также то, что «сетевой эффект от личного вклада каждого пользователя становится ключом к доминированию на рынке в эпоху Веб 2.0» [1]. Личный вклад пользователя таким образом превращает самого пользователя в своеобразное «средство массовой информации», что, как показывает клинический опыт, имеет серьезные психологические последствия для личности, действия которой начинают определяться принципом «быть замеченным – это все» ("getting noticed is everything") [5].

Еще одним серьезным психологическим следствием всеобъемлющего вмешательства в жизнь каждого индивида технологий Веб 2.0 стало явление, отмеченное психологами очень рано, – когнитивная перегрузка современного человека, которая привела к изменению самой формы восприятия информационного потока, в котором он вынужден существовать, – наиболее часто в этой связи упоминается «клиповое мышление», управляющее всеми когнитивными процессами у т.н. поколения Z. Это явление признано особенно опасным в образовательной сфере, поскольку провоцирует серьезные изменения когнитивных способностей, проявляющиеся в нарушении концентрации внимания, ухудшении процесса запоминания информации, трудности ее анализа и рефлексии [6].

Таким образом, результаты глобальной сетевой социализации информационных процессов оказались довольно противоречивыми.

С одной стороны, масштабное вовлечение широких слоев населения в креативную информационную активность способствует обогащению и расширению глобального информационного пространства (примером может служить несомненный успех многих проектов, реализованных с использованием Вики-технологий), однако оборотной стороной информационной сетевой активности стало сегодня то, что в условиях нарождающегося цифрового общества недопонимание, искажения информации, подмена понятий, ложная интерпретация приводят к весьма печальным последствиям в социальной сфере.

В настоящее время разработаны и активно применяются различные технологии информационного управления. Информационное воздействие на объект управления, с целью формирования заданного поведения, возможно сегодня как под контролем объекта управления, так и без его контроля, непосредственно на его подсознание [7]. Использование технологий информационного управления в социотехнических системах является еще одной угрозой информационной безопасности граждан.

Следует отметить, что процессы в глобальном информационном пространстве во многом не являются спонтанными. Они реализуются, во многом целенаправленно, в соответствии с указаниями Давосского клуба и западного цифрового лобби, основной задачей которых является достижение цифрового доминирования и осуществление глобального информационного управления.

Цифровизация привела к возрастанию влияния действий в виртуальном пространстве на события в реальной жизни, причем не только в сфере социально-психологической, но и технической и технологической. В социальной сфере потоки ложной, неадекватной и откровенно враждебной информации приносят обществу большой вред. Кроме формирования негативных настроений, это отрицательно влияет на формирование понятийной базы общественных и специальных коммуникаций.

Еще одно явление характерное для современного информационного пространства это cancel culture — современная форма судов инквизиции, при которой человек или определенная группа лишаются поддержки и подвергаются осуждению в

социальных или профессиональных сообществах, как в онлайн-среде и в социальных медиа, так и в реальном мире.

Несомненную и весьма существенную опасность представляет практика цифровой диктатуры, которая реализуется не только в рамках коммуникации, но и путем ее ликвидации. Цифровые монополисты позволяют себе удалять из сети аккаунты по своему желанию, практически бесконтрольно. Это прямой путь к цифровой диктатуре, ее реализации во всех формах. Осуществление цифрового давления на социум во всех его проявлениях представляет собой новый этап в формировании современного информационного пространства, в котором сочетаются формы психоинформационного давления с психологией толпы и прямым технологическим терроризмом. Сегодня в условиях нарождающегося цифрового общества недопонимание, искажения информации, подмена понятий, ложная интерпретация и, наконец, цифровая диктатура могут привести к весьма печальным последствиям.

Таким образом, тезис Доктрины «обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности» требует выполнения не только за счет усилий государства, но и общество в целом должно знать и быть готовым парировать возникающие информационные угрозы.

Литература:

1. *O'Reilly T.* What is Web 2.0. Design patterns and business models for the next generation of software by Tim O'Reilly 09/30/2005. – URL: https://www.oreilly.com/pub/a/web2/archive/what-is-web20.html (дата обращения 11.04.2021).

2. *Ackerman M.S.* The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility // Human–Computer Interaction. – 2000. – Volume 15. Issue 2-3. – P. 179-203

3. *Eubanks V.* Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. – New York: St Martin's Press, 2017. – 272 p.

4. *Surowiecki J.* The wisdom of crowds: Why the many are smarter than the few and how collective wisdom shapes business, economies,

societies and nations. – New York: Random House, Doubleday Books, 2004. – 336 p.

5. *Andersen P.* What is Web 2.0?: ideas, technologies and implications for education. – Bristol: JISC, 2007. – Vol. 1. – P. 1-64.

6. *Гурьянов Н.Ю., Коротаева Т.В.* Девиации когнитивных способностей человека под воздействием информационных технологий // Вестник МГОУ. Серия: Философские науки. – 2021. – №1. – С. 111-118.

7. *Муромцев В.В., Немцова С.Р.* Проблемы психоинформационной безопасности в современном информационном пространстве // Информационные войны. – 2014. – №2. – С. 73-80.