■ ■ ■ Оценка информационной безопасности интернет-среды пользователями социальных сетей

Кривоухов А.А.

Курская государственная сельскохозяйственная академия имени И.И. Иванова, Курск, Российская Федерация.

Аннотация. В статье приводятся оценка изменений в безопасности жизнедеятельности вследствие внедрения информационно-телекоммуникационных технологий. На основе данных опроса, проведённого в режиме онлайн в социальных сетях «ВКонтакте» и «Twitter», автор показывает, что пользователи этих сетей оценивают жизнедеятельность в современном обществе как более опасную, а уровень открытости своих персональных данных в сети как высокий или средний, что сопровождается распространением чувства незащищённости от преступных посягательств при работе в сети интернет. В то же время, из-за опасений виктимизации и определённой закрытости сетевых сообществ, пользователи социальных сетей выбирают взаимное информирование в качестве меры борьбы с информационными угрозами. В итоге автор приходит к выводу о необходимости формирования компетентности в области информационной безопасности как составляющей информационной и коммуникационной культуры современного человека.

Ключевые слова: информационная безопасность, информационно-коммуникационная среда, интернет среда, социальные сети, киберпреступление

Для цитирования: Кривоухов А.А. Оценка информационной безопасности интернет-среды пользователями социальных сетей. *Коммуникология*. 2018. Том 6. №1. С. 107-117. DOI 10.21453/2311-3065-2018-6-1-107-117.

Сведения об авторе: Анатолий Анатольевич Кривоухов, кандидат юридических наук, доцент кафедры гуманитарных дисциплин Курской государственной сельскохозяйственной академии имени И.И. Иванова. Адрес: 305021, г. Курск, ул. Карла Маркса, 70. E-mail: anatka@rambler.ru.

Статья поступила в редакцию: 18.12.2017. *Принята к печати:* 10.01.2018.

Понятие информационной безопасности

Современная информационно-коммуникационная среда служит новой средой жизнедеятельности для миллиардов людей, но одновременно с этим являющейся для них новой информационной опасностью. Ещё в конце прошлого века С. Паринов писал: «*Мы строим Интернет-цивилизацию, которая будет обладать высокой гибкостью и быстрым коллективным разумом. Наш инстинкт самосохранения должен помочь нам встроить в её конструкцию защитные механизмы, которые уберегут нас от «вавилонской» катастрофы*» [Паринов].

Нарастание информационных потоков, проникновение коммуникации во все сферы жизнедеятельности общества, возникновение и развитие качественно нового типа коммуникационных структур требуют глубокого переосмысления без-

опасности человека в целом, и информационной безопасности, в частности. На наш взгляд, понятие информационная безопасность нужно связывать с коммуникативными практиками, реализуемыми в информационно-коммуникационной среды, которая, будучи местом, где синхронизируют информационное взаимодействие множество социальных субъектов, способна наиболее широко обеспечить коммуникацию между индивидами [Зотов]. Нормальная жизнедеятельность современного общества определяется качеством функционирования и уровнем безопасностью информационно-коммуникационной среды, в первую очередь социальных сетей. Данная среда используется для разных целей. Например, для целей общения, размещения информации, совершения сделок, продвижение бизнес-услуг и многое другое. Информационно-коммуникационная среда может быть прекрасным и полезным средством для обучения, отдыха или общения. Несмотря на положительную сторону расширения использования социальных сетей, существуют определённые недостатки: пока одни извлекают пользу от существования социальных сетей, в первую очередь экономя своё время, другие используют их для пропаганды насилия, экстремизма, вымогательства, шантажа, мошенничества, совершения преступлений. В целом, есть серьёзные основания предполагать, что опасности и угрозы, связанные с тотальной информатизацией общества, сопоставимы с открываемыми этим процессом новыми возможностями.

В настоящее время уже достаточное количество научных публикаций, исследующие данную среду как антропо- или социотехнический феномен [Геворкян; Зубрилин]. Это позволяет рассматривать информационную безопасность как антросоциотехнический феномен. А саму информационную безопасность определить, как состояние защищённости от негативных информационных воздействий информационной сферы и её субъектов, циркулирующей информации, при котором риск ухудшения функционирования и развития социума и его элементов минимален [Кривоухов, Зотов].

При этом именно личность является ключевым звеном информационной безопасности в триаде (человек – общество – техника). Между тем личность, по мнению некоторых исследователей, зачастую оказывается за гранью большинства существующих нормативных документов, регулирующих отношения в сфере информационной безопасности [Шиловцев]. Но, как и реальный мир, информационно-коммуникационная среда может быть опасна для человека: в ней проявляются свои информационные опасности, то есть возникать ситуации, при которой человеку может быть причинён существенный вред, а также скрываются угрозы для информационной безопасности, то есть совершаться действия, явления или процессы, способные оказать нежелательное воздействие на человека, систему его знаний, ценностей и норм.

Методы исследования оценок пользователей социальных сетей информационной безопасности Интернет-среды

Основная цель проведённого исследования заключалась в получение оценок пользователей социальных сетей информационной безопасности Интернет-

среды. На конец лета 2017 года суточная аудитория интернета (ответившие, что выходили в Сеть в последние сутки) составила 60% взрослых россиян, недельная – 67%, месячная – 70% (что составляет соответственно 70,4, 78,5, 81,8 млн. человек)[1]. Количество проявивших себя в социальных сетях за май 2017 года составило 38 млн. человек (32,4% населения). В связи с этим в последнее время широкое распространение получают методы онлайн-исследований (онлайн-опросов). Опрос проводился в режиме онлайн в социальных сетях «ВКонтакте» и «Twitter». Выбор данных платформ обоснован следующими факторами:

– высокая востребованность среди интернет-пользователей;

– универсальность охватываемой аудитории пользователей;

– наличие специального функционала, позволяющего проведение опроса мнений пользователей.

Общий охват аудитории, аккаунтов, применяемых для проведения исследования, превышает 300 тыс. пользователей. В среднем, на каждый из представленных вопросов ответило около 400 уникальных пользователей. Социальный портрет респондента, выбравшего форму опроса онлайн в целом соответствует половозрастной структуре пользователей интернет. Мужская аудитория преобладает в Интернете – по данным разных исследовательских компаний, насчитывается от 52 до 56% от общего числа пользователей. Наиболее массовая аудитория Сети – граждане РФ в возрасте от 18 до 34 лет – в среднем 62% пользователей. Примерно 33% аудитории Сети – люди от 35 до 54 лет.

Оценка информационной безопасности жизнедеятельности и уровня публичности личных данных

Разумеется, изменения, происходящие в обществе под влиянием сетевых средств массовой коммуникации, не ограничиваются только определёнными преимуществами и выгодами – они порождают массу опасностей для человека. В итоге более половины (52%) считают, что жизнедеятельность в современном обществе вследствие внедрения информационно-телекоммуникационных технологий стала опасней (см. рис.1).

Следует отметить, что ряд исследователей фиксирует, что в последнее время доля населения России, столкнувшегося с проблемами информационной безопасности, сокращается: если в 2013 году они в общей массе пользователей составляли 67,8%, то в 2015 году – только 34,1% [Подольная]. Но это говорить не столько о том, что проблемы информационной безопасности уходят на задний план, а том, что в современном обществе отечественный интернет-пользователь учится жить в условиях постоянных информационных угроз. Он стал внимательней относиться к защите персональной информации в Интернете. В период с 2013 по 2016 год существенно меньше стало тех, кто оставляет без внимания вопросы безопасности данных (с 32% до 20%). Среди принимаемых мер самая

[1] Интернет в России: динамика проникновения [лето 2017] // Фонд Общественное Мнение: http://fom.ru/SMI-i-internet/13783

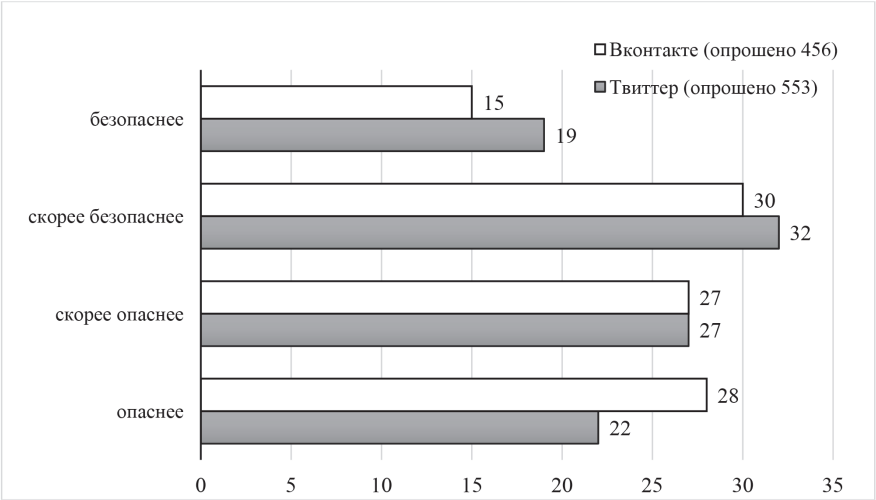

Рисунок 1. Мнения респондентов о том, стала ли жизнедеятельность в современном обществе вследствие внедрения информационно-телекоммуникационных технологий более безопасной, или нет (Respondents' opinions on whether social activity in modern society in consequence of the introduction of information and telecommunication technologies has become more secure, or not)

распространённая – использование антивирусных программ. К данной мере защиты информации прибегают 53%, причём сегодня её применяют существенно чаще, чем три года назад (31%). Сегодня 29% пользователь избегает публикации личной информации в социальных сетях, 26% – использует сложные пароли и часто их меняет (В 2013 году таких было по 17%). Заметно выросло и количество тех, кто «чистит кэш», удаляя информацию о введённых паролях, истории просмотров и загрузок – с 9% до 16%, соответственно[1].

Интернет-пространство поражает уровнем публичности жизни любого человека: конфиденциальность личной информации утрачивается без согласия индивида. Вконтакте, Фейсбук, Одноклассники, Твиттер, Инстаграм, как и любая другая социальная сеть, в которой активно ведётся аккаунт, полностью раскрывает человека. Любой заинтересованный в раскрытии личностных особенностей человека по странице в социальной сети составить его портрет, получив информацию об увлечениях, политических взглядах, круге общения. По музыке, которую слушает пользователь, можно сделать выводы о его предпочтениях, характере, настроении.

Ежедневно каждый пользователь интернет сети делает более десятка запросов в поисковых системах. Вся эта информация сохраняется и анализируется.

[1] Новое о цифровой грамотности, или россияне осваиваются в сети // Всероссийский центр изучения общественного мнения. Пресс-выпуск №3084 [опубликовано 15.04.2016]: https://wciom.ru/index.php?id=236&uid=115657

Уже сегодня за каждым пользователем идёт незримая и автоматизированная слежка. Где бывает, с кем разговаривает, что ищет в сети интернет. Современные системы обработки данных научились анализировать практически всю информацию о человеке, а в ближайшем будущем они смогут составлять психологический портрет, что позволит вычислительным машинам иметь информации о человеке больше, чем он сам знает о себе.

На основе этого минимум предлагается таргетированная реклама, а максимум – создание двойника, аккаунт которого соответствует информационному образу жизни реального человека. Неслучайно треть опрошенных нами респондентов оценивают уровень открытости персональных данных в сети как высокий, и ещё треть как средний.

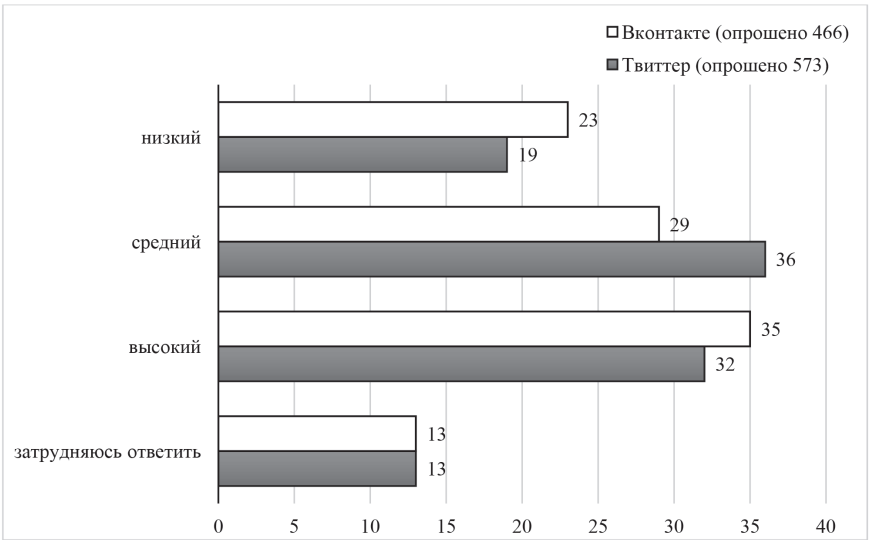

Рисунок 2. Распределение ответов на вопрос «Как Вы оцениваете уровень открытости ваших персональных данных в сети?», % (Distribution of answers to the question "How do you assess the level of openness of your personal data on the network", as %)

Оценка уровня защищённости от киберпреступлений и меры по предотвращению угроз информационной безопасности

В современном мире значительное число правонарушений совершается посредством использования информационно-телекоммуникационных технологий. Это так называемые киберпреступления, которые включают как распространение вредоносных вирусов, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, фишинг, так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) че-

рез Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем. Статистика киберпреступности имеет высокие показатели. В 2017 году (за 10 месяцев) количество преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий составило 82440, что составляет 4,2% от всех преступлений[1]. Следствием широкого распространения данного явления является распространение чувства незащищённости от преступных посягательств при работе в сети интернет. Такое чувство испытывают более половины опрошенных (19% дали ответ в категорической форме, 32% – в более либеральной). В этих условиях закономерно, что намерениями совершить какие-либо действия (транзакции) сильно зависят от текущей оценки безопасности социальных сетей (наличие/отсутствие уведомлений об уровне информационных угроз).

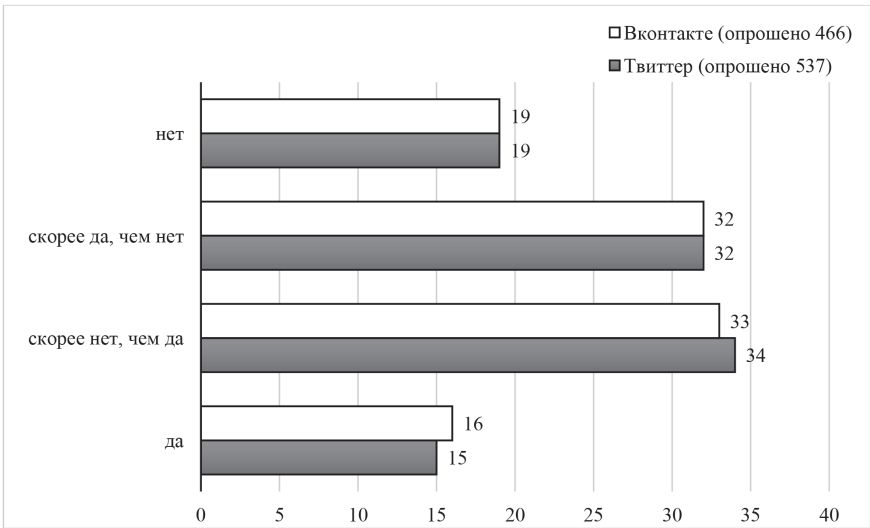

Рисунок 3. Распределение ответов на вопрос «Чувствуете ли вы себя защищённым от преступных посягательств при работе в сети интернет?» (Distribution of answers to the question “Do you feel protected from criminal attacks when working on the Internet?”)

Сегодня в большинстве случаев (48%) пользователи социальных сетей при столкновении с информационными угрозами чаще всего обходятся лишь предупреждением своего ближайшего круга о возникновении такой ситуации (рис. 4). Обращение в правоохранительные органы или иные организации, регулирующие деятельность пользователей в информационно-коммуникационной среде не распространено.

[1] Состояние преступности в России (за январь-ноябрь 2017 года) // ФКУ «Главный информационно-аналитический центр» Министерства внутренних дел Российской Федерации: https://xn--b1aew.xn--p1ai/folder/101762/item/11830347/

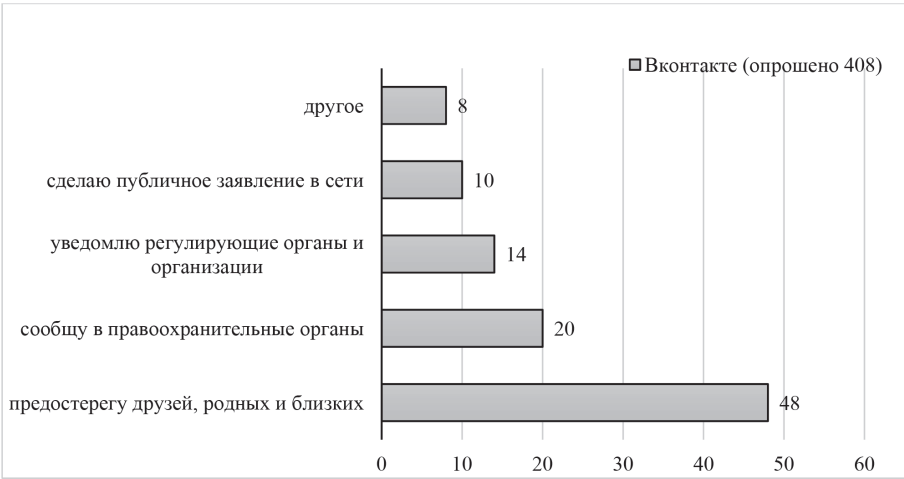

Рисунок 4. Распределение ответов на вопрос «Сообщите ли Вы кому-либо об опасной / вредной информации, если найдёте ее в сети Интернет?», % (Distribution of answers to the question “Do you inform anyone about dangerous / harmful information if you find it on the Internet?”, as %)

Такое поведение может быть связано с виктимизацией пользователя социальных сетей [Saridakis, Benson, Ezingeard, Tennakoon], его обвинением в ненадлежащем поведении, приведшем к проявлению информационной угрозы: «не стоило посещать данный ресурс», «не нужно было переводить деньги за товар сомнительного происхождения» и т.д. Кроме того, столкнувшись с информационной угрозой, пользователь социальной сети не желает терять своё время и материальные ресурсы на бюрократические процедуры, тем более, если сотрудники ведомств, ответственных за информационную безопасность, не проявляют интерес к данной теме.

В тоже время не стоит забывать, что социальные сети – это осознанно выстраиваемые связи, основанные на доверии агентов-партнёров, осуществляющих целенаправленную деятельность, ориентированную на взаимное достижение желаемого для сетевого сообщества результата [Заякина]. Возможно поэтому по отношению циркулирующей в сети информацией запускаются процессы фильтрации и механизмы предупреждения «своих».

Повышенный уровень информационных угроз в информационно-коммуникационной среде заставляет её акторов искать возможность формирования компетентности в области безопасности, которые позволили бы ему самостоятельно оценивать опасность тех или иных ресурсов, противостоять возникающим в глобальной сети Интернет новым угрозам и рискам, компьютерной и интернет-зависимости. Такую необходимость испытывают более – опрошенных (рис. 5). Наиболее предпочитаемой формой формирования данной компетентности для респондентов, представляющих пользователей социальных сетей, является дистанционное прохождение специальной обучающей программы (39%).

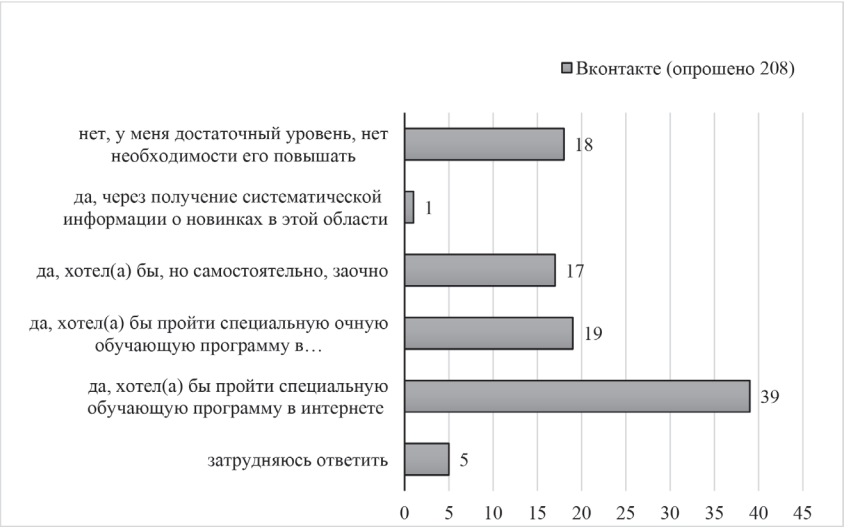

Рисунок 5. Распределение ответов на вопрос «Хотели бы Вы повысить свою компетентность в области безопасности при работе в информационно-коммуникационной среде?», % (Distribution of answers to the question "Would you like to increase your competence in the field of security when working in the information and communication environment?", as %)

В этих условиях важной задачей является формирование и дальнейшее развитие информационной и коммуникационной культуры как компетентности современного пользователя социальной сети. Важнейшей чертой данной компетентности является эффективное использование в повседневных социальных практиках информационно-телекоммуникационных технологий, открывающее широкий доступ к информации и ведущее к новому уровню коммуникации [Шарков, Зотов].

Вывод

Таким образом, понимание информационно-коммуникационной среды как антропосоциотехнического феномена позволяет рассмотреть личность как один из ключевых звеном информационной безопасности в триаде (человек – общество – техника). Оценка информационной безопасности Интернет-среды для пользователей социальных сетей проводилась на основе данных опроса, проведённого в режиме онлайн в социальных сетях «ВКонтакте» и «Twitter». Результаты исследования позволяют сделать вывод, что пользователи оценивают жизнедеятельность в современном обществе как ставшую более опасной, а уровень открытости своих персональных данных в сети как высокий или средний, что сопровождается распространение чувства незащищённости от преступных посягательств при работе в сети интернет. В то же время, пользователи соци-

альных сетей, из-за опасений виктимизации и определённой закрытости сетевых сообществ, в качестве меры борьбы с информационными угрозами выбирают взаимное информирование, а не обращение в правоохранительные органы или органы, ответственные за информационные процессы. Автор приходит к выводу о необходимости формирования компетентности в области информационной безопасности как составляющей информационной и коммуникационной культуры современного человека. В свете результатов данного исследования целесообразность контроля российского государства за виртуальным пространством не вызывает сомнений.

Источники

Геворкян А.В. (2006). Роль человека в современных социотехнических системах: Дис. ... канд. филос. наук: 09.00.08. Москва.

Заякина Р.А. (2016). Информационная безопасность в социальных сетях: топологический подход // Проблемы правового обеспечения безопасности личности, общества и государства: сборник статей по материалам ежегодной международной научно-практической конференции в 3 т. / коллектив авторов: под ред. С.А. Полякова. Новосибирск: Изд-во НГТУ. Т. 1. С. 52-57.

Зотов В.В. (2007). Становление информационно-коммуникативной среды современного общества: социологический анализ институциональных трансформаций. Курск: Изд-во КурскГТУ.

Зубрилин А.А. (2001). Интернет: технологический и социальный аспекты // *Информатика и образование*. № 7. С. 53-62.

Кривоухов А.А., Зотов В.В. (2017). Информационная безопасность как антропосоциотехнический феномен // *Коммуникология*. Том 5. №4. С. 71-81

Паринов С. (1999). Истоки Интернет-цивилизации // *INTER.NET*. № 15 [электронный ресурс]: http://www.inter.net.ru/

Подольная Н.Н. (2016). Информационная безопасность использования домашними хозяйствами России сети интернет в условиях обострения угроз кибертерроризма // Национальная безопасность в современной России: стратегия противодействия экстремизму и терроризму и перспективы преодоления глобальных проблем: материалы Всероссийской научной конференции: в 2 тт. Т. 1. Саранск: ИП Афансьев. С. 102-108.

Шарков Ф.И., Зотов В.В. (2016). Информационная и коммуникативная культура как необходимая компетенция профессиональных стандартов специалиста в сфере рекламы и связей с общественностью // XX международная научно-методическая конференция заведующих кафедрами маркетинга, рекламы, связей с общественностью, дизайна и смежных направлений / Сборник материалов: под общ. ред. В.А. Евстафьева. М.: Экон-Информ. С. 159-166.

Шиловцев А.В. (2012). Современные информационные технологии как фактор угроз безопасности личности в современной России: аксиологический аспект // *Информационное право.* № 2 (29). С. 13-17

Saridakis G., Benson V., Ezingeard J.N., Tennakoon H. (2016). Individual Information Security, User Behaviour and Cyber Victimisation: an empirical study of social networking users // *Technological Forecasting and Social Change*. No. 102. P. 320-330.

Benson V., Saridakis G., Tennakoon H., Jean-Noel E. (2015). The Role of Security Notices and Online Consumer Behaviour: an empirical study of social networking users // *International Journal of Human-Computer Studies*. No. 80. P. 36-44.

■ ■ ■ Assessment of Information Security of the Internet Environment by the Users of Social Networks

Anatoliy A. Krivoukhov

Kursk State Agricultural Academy, Kursk, Russian Federation.

Abstract. The paper provides the evaluation of changes in the safety of social activity in the aftermath of the introduction of information and telecommunication technologies. Based on the data of the online poll on social networks "VKontakte" and "Twitter", the author shows that users of these networks evaluate the activity in modern society as more dangerous, and the level of openness of their personal data in the network as high or medium. This raises the feeling of insecurity from criminal encroachments when working on the Internet. At the same time, due to the fears of victimization and a certain closeness of network communities, social network users choose mutual information as a measure to combat information threats. As a result, the author concludes that it is necessary to increase public competence in the field of information security as a component of the information and communication culture of modern man.

Keywords: information security, information and communication environment, social networks, cybercrime

For citation: Krivoukhov A.A. Assessment of Information Security of the Internet Environment by the Users of Social Networks. *Communicology (Russia).* 2018. Vol. 6. No.1. P. 107-117. DOI 10.21453/2311-3065-2018-6-1-107-117.

Inf. about the author: Krivoukhov Anatoliy Anatolievich, Cand. Sc. (Law), senior lecturer at the Department of Humanitarian Disciplines, Kursk State Agricultural Academy. Address: 305021, Kursk, Karl Marx st., 70. E-mail: anatka@rambler.ru.

Received: 18.12.2017. *Accepted:* 10.01.2018.

References

Gevorkian A.V. (2006). The role of man in modern sociotechnical systems: Diss. Cand. Sc. (Philos.). Moscow (In Rus.).

Zaiakina R.A. (2016). Information security in social networks: topological approach. Legal problems of the security of the individuals, society and the state: a collection of articles on the materials of the annual international scientific and practical conference in three volumes / ed. S.A. Polyakova. Novosibirsk: Novosibirsk State Technical University. Vol. 1. P. 52-57 (In Rus.).

Zotov V.V. (2007). The evolvement of the information and communication environment of modern society: the sociological analysis of institutional transformations. Kursk: Kursk State Technical University (In Rus.).

Zubrilin A.A. (2001). Internet: technological and social aspects. *Informatics and Education*. No. 7. P. 53-62 (In Rus.).

Krivoukhov A.A., Zotov V.V. (2017). Information security as anthroposociotechnical phenomenon. *Communicology*. Vol. 5. No. 4. P. 71-81 (In Rus.).

Parinov S. (1999). The origins of the Internet civilization. *INTER.NET*. No. 15 [electronic journal]: http://www.inter.net.ru/ (In Rus.).

Podolnaya N.N. (2016). Information Security of the Use of the Internet by Russian Households in the Conditions of Aggravation of Cyber Terrorism Threats. National Security in Modern Russia: Strategy for Countering Extremism and Terrorism and Prospects for Overcoming Global Problems: Proceedings of the All-Russian Scientific Conference: in 2 volumes. T. 1. Saransk: Afansiev. P. 102-108 (In Rus.).

Sharkov F.I., Zotov V.V. (2016). Informational and communicative culture as a necessary competence of the professional standards of a specialist in the sphere of advertising and public relations. XX International Scientific and Methodical Conference of the Heads of the Departments of Marketing, Advertising, Public Relations, Design and Related Disciplines. Ed. V.A. Evstafyeva Moscow: Econ-Inform. P. 159-166 (In Rus.).

Shilovtcev A.V. (2012). Modern Information Technologies as a Factor of Threats to Personal Security in Modern Russia: the Axiological Aspect. *Information Law*. No. 2 (29). P. 13-17 (In Rus.).

Saridakis G., Benson V., Ezingeard J.N., Tennakoon H. (2016). Individual Information Security, User Behaviour and Cyber Victimisation: an empirical study of social networking users. *Technological Forecasting and Social Change*. No. 102. P. 320-330.

Benson V., Saridakis G., Tennakoon H., Jean-Noel E. (2015). The Role of Security Notices and Online Consumer Behaviour: an empirical study of social networking users. *International Journal of Human-Computer Studies*. No. 80. P. 36-44.