Научная статья
УДК 101.1
DOI: 10.17213/2075-2067-2023-1-212-218

БЕЗОПАСНОСТЬ ЛИЧНОСТИ В СОВРЕМЕННОЙ ГЛОБАЛЬНОЙ СЕТИ

Сергей Александрович Дементьев

Южно-Российский гуманитарный институт, Ростов-на-Дону, Россия
s.a.dementiev2014@yandex.ru, ORCID: 0009-0002-6201-3686

Аннотация. ***Цель статьи*** *заключается в изучении особенностей обеспечения безопасности личности в глобальной сети Интернет.*

Результаты исследования. *Автор сосредотачивает внимание на различиях сетевой и реальной личности индивида и делает вывод о том, что отношение к собственной безопасности значительно отличается в виртуальной реальности. Объясняется это технической опосредованностью и асинхронным характером сетевой коммуникации. Безопасность личности в Интернете связывается, в первую очередь, с безопасностью личных данных и позиционируется как фундамент комфортной жизнедеятельности. Автор анализирует риски, с которыми сталкивается пользователь при внесении своих персональных данных в социальные сети на примере групп, имеющих интерес к конфиденциальным данным пользователей. Сделан вывод о том, что этикет общения в глобальной сети и низкая интернет-грамотность является важнейшим фактором в повышении рискогенности интернет-коммуникаций.*

Перспективы исследования *заключаются в дальнейшем осмыслении механизмов обеспечения безопасности личности в цифровом пространстве.*

Ключевые слова: *Интернет, сетевая личность, виртуальная реальность, безопасность личности, персональные данные, информационная безопасность, социальные сети*

Для цитирования: *Дементьев С. А. Безопасность личности в современной глобальной сети // Вестник Южно-Российского государственного технического университета. Серия: Социально-экономические науки. 2023. Т. 16, № 1. С. 212–218. http://dx.doi.org/10.17213/2075-2067-2023-1-212-218.*

© Дементьев С. А., 2023

Original article

PERSONAL SECURITY IN TODAY'S GLOBAL NETWORK

Sergey A. Dementiev

South Russian Humanities Institute, Rostov-on-Don, Russia
s.a.dementiev2014@yandex.ru, ORCID: 0009-0002-6201-3686

Abstract. ***The purpose of the article*** *is to study the features of personal security in the global Internet.*

The results of the study. *The author focuses on the differences between the network and the real personality of an individual and concludes that the attitude to one's own security is significantly different in virtual reality. This is explained by the technical mediation and asynchronous nature of network communication. Personal security on the Internet is associated, first of all, with the security of personal data and is positioned as the foundation of a comfortable life. The author analyzes the risks that a user faces when entering his personal data into social networks using the example of groups that have an interest in confidential user data. It is concluded that the etiquette of communication in the global network and low Internet literacy is the most important factor in increasing the risk of Internet communications.*

The prospects of the research *are to further comprehend the mechanisms of ensuring the security of the individual in the digital space.*

Keywords: *Internet, network personality, virtual reality, identity security, personal data, information security, social networks*

For citation: *Dementiev S.A. Personal security in today's global network // Bulletin of the South Russian State Technical University. Series: Socio-economic Sciences. 2023; 16(1): 212–218. (In Russ.). http://dx.doi.org/10.17213/2075-2067-2023-1-212-218.*

Introduction. Глобальная сеть Интернет является важной частью жизни почти всех современных и прогрессивных людей, её охват по США — 93 %, в Европе — 88.2 %, а самый низкий — в Африке, где лишь 43 % населения имеет доступ к всемирной паутине [1]. Интернет изначально позиционировался как международная база данных, в которой люди будут иметь доступ к важной информации, но современные тренды развития сети направлены, в первую очередь, на коммуникацию пользователей. Иными словами, база данных и «всемирная цифровая библиотека» возросла до полноценной виртуальной реальности, в которой люди общаются друг с другом посредством социальных сетей и мессенджеров. С одной стороны, коммуникация позволяет стирать границы, возводимые между людьми, но с другой имеет опасности, связанные с безопасностью цифровой личности индивида. В этой работе мы предпримем попытку рассмотреть угрозы, которые представляет глобальная сеть Интернет для безопасности личности.

Materials and methods. В этой работе мы будем опираться на когнитивную теорию личности. Тематика цифровой личности и её особенностей в сети Интернет популярна среди множества исследователей. М. Ким вместе с коллегами анализировали влияние черт цифровой личности на агрессивное поведение [9], коллектив авторов во главе с М.А. Оливеро выявляли уязвимости и проблемы цифровой личности [11], а М. Диллер, М. Ассен и Т. Спет концентрировали своё внимание

1 Internet Usage Statistics. The Internet Big Picture. World Internet Users and 2023 Population Stats. [Electronic resource] // Internet World Stats. URL: https://www.internetworldstats.com/stats.htm.

на том, как трансформируется личность человека при переходе в цифровое пространство [8]. Примечательны также работы психологов К. Монтаг и Дж. Д. Эльхай, рассматривающих психологический аспект формирования цифровой идентичности. Д. Азукар с коллегами предприняли попытку предсказать пять черт личности, наиболее часто проявляющихся в цифровой среде [7], а К. Салливан рассмотрел цифровую личность в правовом контексте [12]. Начнем с того, что «сетевая» личность человека значительно отличается от обычной. А.Е. Войскунский вместе с коллегами установили, что сетевая и реальная идентичности отличаются, в первую очередь, степенью влияния человека на неё [2]. Объясняется это следующим образом: в глобальной сети индивид имеет возможность корректировать черты своей личности так, как посчитает нужным, в то время как в реальности это реализовать намного сложнее. Другим важным фактором, отличающим сетевую личность от реальной, является доступность персональных данных другим пользователям, благодаря чему безопасность личности может оказаться под угрозой.

Results. В реальности персональные данные доступны только уполномоченным лицам, представителям власти, правоохранительным органам и другим компетентным группам, которые, предположительно, не смогут использовать персональные данные человека против него. Кража такой информации, как банковские реквизиты, паспортные данные, адрес и т.д., считается серьезным преступлением, вызывающим настороженность и опасения почти у всех обитателей «оффлайн»-реальности. Однако в глобальной сети персональные данные являются априори скомпрометированными, а процесс кражи в большинстве случаев остается незамеченным. Наибольшую опасность для личности в сети Интернет представляет кража персональных данных, которая может произойти как по вине самого пользователя, так и из-за внешних угроз (вирусы, мошенники, корпорации).

Персональные данные в реальности хранятся в двух видах: физически в сохранности у владельца или в оцифрованном виде у представителей власти и других компетентных лиц, имеющих возможности сохранить их и не предать огласке. Для примера возьмем паспорт гражданина РФ. Он хранится в его физическом воплощении у владельца, а вся «цифровая» информация о нем может быть найдена у представителей власти, правоохранительных органов, банков и т.д. При этом потеря паспорта в его физическом воплощении вызывает серьезную панику практически у всех, ведь процедура его восстановления требует значительного времени и усилий. Аналогична ситуация и с информацией о банковских реквизитах. Потеря физической дебетовой карты может ввергнуть индивида в панику и заставить его звонить в банк и запрашивать блокировку карты. Однако в цифровой реальности человек добровольно предоставляет вышеописанные данные третьим лицам, надежность которых может находиться под вопросом, а сам факт потери персональных данных может быть не известен тому, кто их потерял [4].

Объясняется это самой сущностью интернет-среды — она нестабильна и небезопасна, так как протоколы безопасности требуют постоянного обновления, а мошенники постоянно улучшают свой рабочий инструментарий [1]. На основе этого можно сказать, что главную опасность для личности в сети Интернет представляет сам пользователь, зачастую не обладающий всей полнотой знаний о принципе работы всемирной сети и не умеющий реализовывать все необходимые процедуры для сохранения своих персональных данных.

Вышеописанные «персональные данные» в философском смысле являются «фундаментом» личности, так как, по сути, личность человека является можно считать их суммой. Знание социального статуса, хобби, семейного положения, материального достатка и адреса позволяет сказать о том, что о человеке «известно всё». Если представить теоретическую ситуацию, в которой мошенник, вымогатель или шантажист подойдёт к жертве и скажет, что «знает все её секреты», то это вызовет экзистенциальный страх, связанный с повышенным чувством опасности за свою жизнь. Безопасность личности, по существу, является состоянием, в котором человек может быть уверен в том, что тайное, сокровенное и личное не попадет в чужие руки и не будет использовано против него.

Само понимание того, что кто-то знает о месте жительства, работе, семейном положении и прочих вещах, может привести к состоянию тревоги и оказать негативное влияние на психическое здоровье индивида. Из этого следует, что безопасность личности (личных данных) может считаться важнейшим условием безопасности экзистенциальной.

Особый интерес представляет отношение человека к безопасности своей личности в реальности и в сети, а именно — серьезные различия, наблюдаемые в отношении важности их сохранения. Мы считаем, что ощущение опасности имеет фундаментальные отличия в контексте онлайн- и оффлайн-реальностей. Объясняется это тем, что в реальности кража персональных данных является атакой на «личность» конкретного человека и последствия от этого ощущаются в более традиционном формате. Иными словами, причина и следствие носят устоявшийся характер и являются известными большинству людей. Потеря паспорта по невнимательности ведёт к серьезным неприятностям, ведь его нашедший может использовать документ для совершения противоправных действий. Аналогично оценивается и попытка вытащить условный паспорт из сумки: злоумышленник хочет навредить и совершает противоправное действие. В глобальной сети это работает совершенно по-другому: персональные данные в абсолютном большинстве случаев не теряются по оплошности и не крадутся конкретным мошенником, имеющим интенцию навредить конкретному индивиду. Персональные данные крадутся большими партиями, выкупаются, сливаются и достаются в результате массивных хакерских атак [3]. Ни в одной из этих ситуаций конкретный пользователь не задействован и не понимает, что кто-то совершал противоправное действие по отношению к нему. Из этого следует, что асинхронность и опосредованность коммуникаций в Интернете притупляет чувство опасности и стремление защищать себя от нападок. Стоит добавить, что множество пользователей просто не понимают ценности своих персональных данных в Интернете и не придают им серьезного значения.

Discussion. Исходя из вышеописанных результатов, остановимся подробнее на группах лиц, негативно влияющих на безопасность личности в Интернете.

Мошенники. Используют персональные данные для совершения противоправных действий. Банковские реквизиты могут быть использованы для покупок в сети Интернет без ведома владельца счёта в банке, паспортные данные могут быть использованы для оформления микрозаймов под высокий процент, номера телефонов и адреса электронной почты могут оказать содействие в рассылке спама. Мошенники могут украсть персональные данные пользователей, а могут приобрести украденные базы данных и использовать их в своих интересах. С 2020 года участились случаи телефонного мошенничества, когда преступники представляются сотрудниками банка и под разными предлогами просят жертв продиктовать им данные своих банковских карт [2]. Чаще всего от них страдают люди старшего возраста, не обладающие знаниями о том, как противодействовать подобным нелегальным схемам. Увеличение числа подобных преступлений также может быть связано с пандемией коронавируса, из-за которой мошенничество, как и почти все сферы жизни общества, перешло в дистанционный формат[3].

Корпорации. Такие компании, как Google, Facebook, Twitter, Apple, Microsoft и др., обладают огромным влиянием на информационную среду сети Интернет и имеют возможности им пользоваться для получения персональных данных пользователей способами различной степени законности [6]. Множество россиян пользуется американскими социальными сетями и ведет в них профили, наполняя их своими персональными данными. В случае обострения геополитической ситуации они могут быть использованы властями

2 Число дел о мошенничестве рекордно выросло на фоне пандемии. Каким преступлениям поспособствовала самоизоляция [Электронный ресурс] // РБК. URL: https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d (дата обращения: 03.07.2021).

3 Эксперты назвали новые виды мошенничества киберпреступников в пандемию [Электронный ресурс] // РБК. URL: https://www.rbc.ru/technology_and_media/23/10/2020/5f92846e9a79472ef8480c45 (дата обращения: 03.07.2021).

и силовыми структурами против интересов российских граждан. Вышеописанные корпорации также промышляют продажей рекламных площадей и применяют технологии таргетированной рекламы, запоминающие интересы пользователей и предоставляющие рекламные материалы, им соответствующие. На первый взгляд, это может показаться безобидным, но это, по сути, является использованием персональных данных в коммерческих целях.

Тролли и доксеры. Троллями можно охарактеризовать людей, получающих удовольствие от страданий других в сетевом пространстве. Определить тех, кто применяет кибербуллинг (цифровую травлю) против различных жертв, практически невозможно, следовательно, интернет-тролли не ограничивают себя в выражениях и способах нанести вред психике своих оппонентов и жертв. Доксеры — группы лиц, систематически крадущие и публикующие персональные данные пользователей сети Интернет в открытом доступе. Доксинг является относительно новым для России явлением, связанным с поиском и опубликованием персональной или конфиденциальной информации о человеке без его согласия [5]. Использование персональной информации индивида против него самого может нанести серьезный урон по психическому здоровью индивида, выбить его из привычной жизненной колеи, а в некоторых случаях даже разрушить отношения с друзьями и близкими людьми.

Стоит упомянуть, что деятельность вышеописанных акторов зависит, в первую очередь, от той среды, в которой они работают, а также от общего уровня коммуникативной интернет-грамотности человека, пользующегося глобальной сетью. Мошенники и прочие злоумышленники чаще опираются не на технические средства, а на неграмотность жертвы, не имеющей представления о том, как правильно обезопасить себя от незаконных действий в Интернете.

Conclusion. Как видно из вышеописанного, в глобальной сети существует множество рисков, связанных со снижением безопасности личности. Она связана, в первую очередь, с самой сущностью Интернета — постоянно меняющейся и трудно контролируемой виртуальной реальностью, выход в которую не всегда безопасен для человека. Техническая опосредованность и асинхронность процесса коммуникации могут притупить чувство опасности и сделать жертву более восприимчивой к технологическим и психологическим влияниям различных групп, заинтересованных в использовании персональных данных против человека. Интернет — реальность информационная, следовательно, вред человеку можно нанести лишь при помощи информации. Безопасность человека в Интернете напрямую связана с безопасностью его персональных данных, а именно — с уверенностью в том, что злоумышленники не смогут получить к ним доступ и использовать в своих целях. Таким образом, для повышения безопасности личности в Интернете необходимо работать над культурой общения, интернет-грамотностью и совершенствованием правовых норм, связанных с обеспечением безопасности личности в глобальной сети Интернет.

Список источников

1. Богданов А. В., Ильинский И. И, Хазов Е. Н. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Криминологический журнал. 2020. №1. С. 15–20.

2. Войскунский А. Е., Евдокименко А. С., Федунина Н. Ю. Сетевая и реальная идентичность: сравнительное исследование // Психология. Журнал Высшей школы экономики. 2013. Т. 10. №2. С. 98–121.

3. Герасимова А. В., Смирнов В. М. Обеспечение сохранности персональных данных в информационном пространстве // Международный журнал гуманитарных и естественных наук. 2021. №5-1. С. 13–15.

4. Дуданец К. И. Неправомерное использовании персональных данных // Вестник Московского университета МВД России. 2011. №8. С. 221–223.

5. Летова Н. В., Полякова Т. А. Защита персональных данных граждан: особенности и проблемы // Образование и право. 2019. №10. С. 77–83.

6. Муромцева А. В., Муромцев В. В. Проблемы информационной безопасности в социальных сообществах в сети Интернет //

Вестник РГГУ. Серия «Экономика. Управление. Право». 2016. №3 (5). С. 84–91.

7. Azucar D., Marengo D., Settanni M. Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis // Personality and Individual Differences. 2018. Vol. 124. P. 150–159.

8. Diller M., Asen M., Späth T. The effects of personality traits on digital transformation: Evidence from German tax consulting [Electronic resource] // International Journal of Accounting Information Systems. 2020. Vol. 37. URL: https://doi.org/10.16/j.accinf.2020.100455.

9. Kim M., Clark S.L., Donnellan M.B., Burt S.A. A multi-method investigation of the personality correlates of digital aggression [Electronic resource] // Journal of Research in Personality. 2020. Vol. 85. URL: https://doi.org/10.1016/j.jrp.2020.103923.

10. Montag C., Elhai J.D. A new agenda for personality psychology in the digital age? [Electronic resource] // Personality and Individual Differences. 2019. Vol. 147. P. 128–134. URL: https://doi.org/10.1016/j.paid.2019.03.045.

11. Olivero M.A., Bertolino A., Domínguez-Mayo F. J., Escalona M.J., Matteucci I. Digital persona portrayal: Identifying pluridentity vulnerabilities in digital life [Electronic resource] // Journal of Information Security and Applications. 2020. Vol. 52. URL: https://doi.org/10.1016/j.jisa.2020.102492.

12. Sullivan C. Digital identity — From emergent legal concept to new reality. Computer Law & Security Review. 2018. Vol. 34(4). P.723–731.

References

1. Bogdanov A.V., Il'inskij I. I, Hazov E.N. Kiberprestupnost' i distancionnoe moshennichestvo kak odna iz ugroz sovremennomu obshhestvu [Cybercrime and remote fraud as one of the threats to modern society]. *Kriminologicheskij zhurnal* [*Criminological Journal*]. 2020; (1): 15–20. (In Russ.).

2. Vojskunskij A.E., Evdokimenko A.S., Fedunina N. Ju. Setevaja i real'naja identichnost': sravnitel'noe issledovanie [Network and real identity: a comparative study]. *Psihologija. Zhurnal Vysshej shkoly jekonomiki* [*Psychology. Journal of the Higher School of Economics*]. 2013; 10(2): 98–121. (In Russ.).

3. Gerasimova A.V., Smirnov V.M. Obespechenie sohrannosti personal'nyh dannyh v informacionnom prostranstve [Ensuring the safety of personal data in the information space]. *Mezhdunarodnyj zhurnal gumanitarnyh i estestvennyh nauk* [*International Journal of Humanities and Natural Sciences*]. 2021; (5-1): 13–15. (In Russ.).

4. Dudanec K.I. Nepravomernoe ispol'zovanii personal'nyh dannyh [Misuse of personal data]. *Vestnik Moskovskogo universiteta MVD Rossii* [*Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*]. 2011; (8): 221–223. (In Russ.).

5. Letova N.V., Poljakova T.A. Zashhita personal'nyh dannyh grazhdan: osobennosti i problemy [Protection of personal data of citizens: features and problems]. *Obrazovanie i pravo* [*Education and law*]. 2019; 10: 77–83. (In Russ.).

6. Muromceva A.V., Muromcev V.V. Problemy informacionnoj bezopasnosti v social'nyh soobshhestvah v seti Internet [Problems of information security in social communities on the Internet]. *Vestnik RGGU. Serija «Jekonomika. Upravlenie. Pravo»* [*Bulletin of the Russian State University. The series «Economics. Management. Right»*]. 2016; 3(5): 84–91. (In Russ.).

7. Azucar D., Marengo D., Settanni M. Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis // Personality and Individual Differences. 2018. Vol. 124. P. 150–159.

8. Diller M., Asen M., Späth T. The effects of personality traits on digital transformation: Evidence from German tax consulting [Electronic resource] // International Journal of Accounting Information Systems. 2020. Vol. 37. URL: https://doi.org/10.16/j.accinf.2020.100455.

9. Kim M., Clark S.L., Donnellan M.B., Burt S.A. A multi-method investigation of the personality correlates of digital aggression [Electronic resource] // Journal of Research in Personality. 2020. Vol. 85. URL: https://doi.org/10.1016/j.jrp.2020.103923.

10. Montag C., Elhai J.D. A new agenda for personality psychology in the digital age? [Electronic resource] // Personality and Individual Differences. 2019. Vol. 147. P. 128–134. URL: https://doi.org/10.1016/j.paid.2019.03.045.

11. Olivero M.A., Bertolino A., Domínguez-Mayo F. J., Escalona M.J., Matteucci I. Dig-

ital persona portrayal: Identifying pluriden-tity vulnerabilities in digital life [Electronic resource] // Journal of Information Security and Applications. 2020. Vol. 52. URL: https://doi.org/10.1016/j.jisa.2020.102492.

12. Sullivan C. Digital identity — From emergent legal concept to new reality. Computer Law & Security Review. 2018. Vol. 34(4). P. 723–731.

Статья поступила в редакцию 28.01.2023; одобрена после рецензирования 10.02.2023; принята к публикации 14.02.2023.
The article was submitted on 28.01.2023; approved after reviewing on 10.02.2023; accepted for publication on 14.02.2023.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Дементьев Сергей Александрович — кандидат социологических наук, доцент кафедры «Гуманитарные дисциплины», Южно-Российский гуманитарный институт.
Россия, г. Ростов-на-Дону, ул. Красноармейская, 108

Sergey A. Dementiev — Candidate of Sociological Sciences, Associate Professor of the Department of Humanities, South Russian Humanitarian Institute.
108 Krasnoarmeyskaya str., Rostov-on-Don, Russia