

Мир науки. Социология, филология, культурология <https://sfk-mn.ru>
World of Science. Series: Sociology, Philology, Cultural Studies

2020, №1, Том 11 / 2020, No 1, Vol 11 <https://sfk-mn.ru/issue-1-2020.html>

URL статьи: <https://sfk-mn.ru/PDF/04SCSK120.pdf>

Ссылка для цитирования этой статьи:

Кривоухов А.А. К оценке уровня безопасности личности в информационно-коммуникационной среде со стороны криминала // Мир науки. Социология, филология, культурология, 2020 №1, <https://sfk-mn.ru/PDF/04SCSK120.pdf> (доступ свободный). Загл. с экрана. Яз. рус., англ.

For citation:

Krivoukhov A.A. (2020). To assess the level of personal security in the information and communication environment by the criminal. *World of Science. Series: Sociology, Philology, Cultural Studies*, [online] 1(11). Available at: <https://sfk-mn.ru/PDF/04SCSK120.pdf> (in Russian)

УДК 316.77

ГРНТИ 04.51.54

Кривоухов Анатолий Анатольевич

ФГБОУ ВО «Курская государственная сельскохозяйственная академия имени И.И. Иванова», Курск, Россия
Доцент кафедры «Гуманитарных дисциплин»
Кандидат юридических наук, доцент
E-mail: anatka@rambler.ru
РИНЦ: http://elibrary.ru/author_profile.asp?id=735837

К оценке уровня безопасности личности в информационно-коммуникационной среде со стороны криминала

Аннотация. Статья посвящена исследованию уровня безопасности личности в информационно-коммуникационной среде со стороны криминала. Целью данной работы является определение субъективного мнения граждан об уровне информационной безопасности в информационно-коммуникационной среде со стороны криминала. Основным методом сбора информации выступил социологический опрос, проведенный в 2019 году среди населения Курской области как медианной по уровню информатизации. Выборку составили 1000 респондентов в возрасте от 16-лет и старше, проживающих в городских и сельских поселениях области. Далее результаты опроса были систематизированы и проанализированы.

Автор приходит к пониманию информационно-коммуникационной среды как антропосоциотехнического феномена, что позволяет рассмотреть личность как одно из ключевых звеньев информационной безопасности в триаде (человек – коммуникации – техника). Оценка информационной безопасности позволяет сделать вывод, что пользователи оценивают жизнедеятельность в современном обществе как опасную. Но в тоже время, несмотря на попадание под криминальные действия злоумышленников значительной части населения, последняя не торопится признать интернет криминальным и возлагает ответственность на саму личность. Это позволяет сделать вывод о готовности граждан жить в условиях рисков информационной безопасности. В заключении автор приходит к выводу о необходимости формирования компетентности в области информационной безопасности.

Ключевые слова: информационно-коммуникационная среда; киберпреступление; Интернет; информационная безопасность личности; информационно-телекоммуникационные технологии; социологический опрос

Введение

Интенсивное развитие информационно-телекоммуникационных систем, средств и систем связи, а также всеобщая информатизация существенно усилили зависимость эффективности функционирования общества и государства от состояния информационно-коммуникационной среды. Сегодня имеется настоятельная потребность в глубоком научном анализе проблемы безопасности в информационно-коммуникационной среде. Активизация и глобализация информационных взаимодействий в обществе диктуют иные, повышенные требования к обеспечению безопасности информационно-коммуникационной среды. Данная среда представляет собой слабоструктурированную систему, в которой совокупность граждан осуществляет совместную деятельность по хранению, передаче, переработке информации посредством информационно-телекоммуникационных технологий. При этом в структурной организации и функционировании данной среды можно выделить три стороны [1]. Первая сторона – это техническая сторона, отражающая возможности компьютерных систем по регистрации, записи, обработке и передаче информации. Вторая – социокультурная, отражающая движение знания и культурных смыслов в системе социальных коммуникаций. И наконец, третья – это сам человек. Поэтому можно утверждать, что данная среда имеет антропосоциотехнический характер, поскольку она состоит из людей, социальных коммуникаций, из информационно-телекоммуникационных технологий, причём все её элементы взаимно дополняют друг друга. Это позволяет рассматривать безопасность информационно-коммуникационной среды в триединстве – безопасность личности, безопасность коммуникаций и безопасность информационно-телекоммуникационных технологий.

Отметим, что ключевой проблемой следует признать проблему соблюдения интересов личности в информационно-коммуникационной среде, к которым следует отнести реализацию конституционных прав гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность [2–4]. Поэтому представляется состоятельным выделять, точнее, отделять от общего понятия информационной безопасности понятие информационной безопасности личности, смещая акцент в сторону решения проблемы обеспечения личной безопасности. Под информационной безопасностью личности будем понимать состояние и условия жизнедеятельности индивида, при которых отсутствует или минимизирована угроза нанесения вреда приватному пространству коммуникаций индивида и той информации, которой он обладает.

Именно социологический анализ информационной безопасности личности в современных условиях становится важнейшей потребностью научного общества. Целью данной работы является определение субъективного мнения граждан об уровне информационной безопасности в информационно-коммуникационной среде со стороны криминала.

Методологические подходы и методы исследования

Методологической базой научного исследования послужили труды зарубежных и российских авторов в области информационной безопасности, а также методы, принципы и модели системного подхода, лежащие в основе современной концепции национальной безопасности. Эмпирической базой исследования стали данные опроса, проведенного в Курской области как медианного субъекта РФ по уровню информатизации. В ходе опроса было

проанкетировано 1000 респондентов, квотированных по полу, возрасту и месту проживания. Результаты исследования были систематизированы и проанализированы.

Основные результаты исследования

Согласно проведенному опросу, респонденты в целом отмечают (рисунок 1), что сегодня вследствие внедрения информационно-телекоммуникационных технологий жизнедеятельность в современном обществе становится опаснее или скорее опаснее – (так считают 17,6 % и 40,1 % соответственно).



Рисунок 1. Распределение ответов на вопрос «Жизнедеятельность в современном обществе вследствие внедрения информационно-телекоммуникационных технологий в последнее время стала опаснее или безопаснее?», в % (а) на основе полевого опроса; (б) на основе Интернет-опроса. Прим.: Без учета позиции «затрудняюсь ответить»

При этом следует отметить, что сопоставление этих данных с результатами опроса Интернет-пользователей, проведенного в 2018 году в социальных сетях «Вконтакте» и «Твиттере», показывает следующее. Пользователи всемирной компьютерной сети несколько выше оценивают опасность деятельности в сети Интернет (25,0 % признают, что жизнедеятельность стала опаснее и ещё 37,0 % утверждают, что «скорее опаснее»).

Изменение ощущений личной безопасности в информационно-коммуникационной среде за последние годы представлено на рисунке 2.

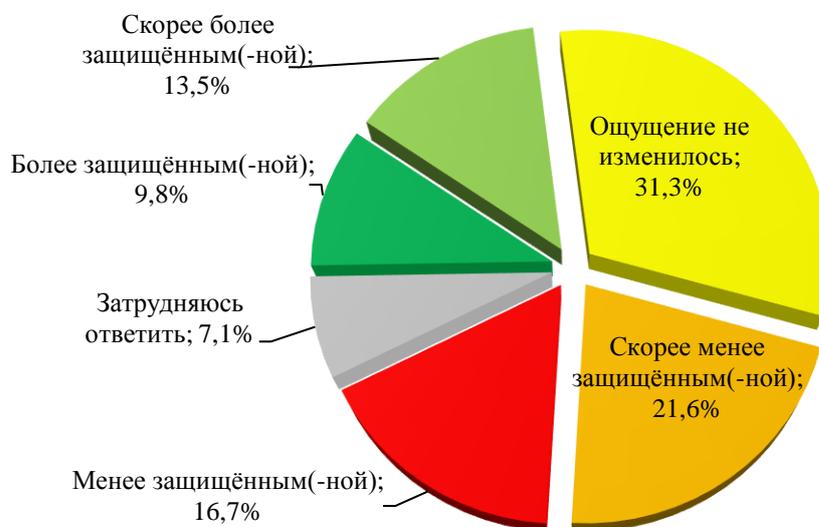


Рисунок 2. Распределение ответов на вопрос «Ваше ощущение личной безопасности в информационно-коммуникационной среде за последние годы изменилось или не изменилось? Если изменилось, то как Вы стали себя чувствовать – более защищенным(-ной) или менее защищенным(-ной)?», в %

Для 38,3 % опрошенных жителей региона идет нарастание ощущения незащищенности в информационно-коммуникационной среде. При этом можно было бы связать это ощущение с тем, что Интернет становится рассадником преступности [5]. Он не только повышает эффективность человеческой деятельности, но и открывает новую криминальную платформу для киберпреступности как спектра преступлений с помощью или посредством информационно-телекоммуникационных технологий в киберпространстве [6]. По объекту посягательства выделяют следующие группы киберпреступлений [7; 8]: компьютерные преступления против личных прав и неприкосновенности частной сферы, экономические компьютерные преступления, компьютерные преступления против общественных и государственных интересов.

Проведенный нами опрос показал, что сегодня определенная часть населения сталкивалась с такого рода преступлениями. Как видно из данных таблицы 1, граждане сталкиваются чаще всего со спамом, то есть с рассылкой корреспонденции лицам, не выразившим желания её получать. Чаще всего такая информация носит рекламный характер, но анонимность спама создает идеальные условия для разного рода мошенничества – злоумышленники рассылают спам, посредством которого выманивают деньги у доверчивых пользователей электронных почтовых ящиков. На втором месте по частоте встречаемости находятся вирусы, ведущие к блокированию браузера или компьютера. С данной проблемой сталкивалось 78,7 % опрошенных нами респондентов. И наконец на третьем и четвертом месте находится фишинг (как попытка несанкционированного доступа к логинам и паролям) и его частная версия – взлом или воровство страниц в социальных сетях.

Таблица 1

Распределение ответов на вопрос «В своей практике использования ресурсов ИНТЕРНЕТА с какими обстоятельствами Вы сталкивались?», в %

	Да	Нет	Затрудняюсь ответить
1) вирусы, блокирование браузера или компьютера	78,7	16,4	4,9
2) спам	86,1	9,0	4,9
3) фишинг (попытка доступа к логинам и паролям)	40,7	32,6	26,7
4) взлом или воровство страниц в соц. сетях	47,3	42,2	10,5
5) взлом почтового ящика	25,3	64,7	10,0
6) мошенничество/кража денежных средств	20,3	71,0	8,6
7) оскорбление и унижение	33,4	57,3	9,3
8) сексуальные домогательства	14,9	76,4	8,8
9) вымогательство, угрозы	14,2	76,9	9,0
10) призывы к терроризму и экстремизму	11,7	79,7	8,6
11) призывами причинить вред себе, к самоубийству	8,3	83,4	8,3

Но в то же время данные опроса не позволяют отнести криминал в информационно-коммуникационной среде к ключевым проблемам безопасности личности (рисунок 3). В целом чувствуют себя защищёнными от преступных посягательств при работе в Интернете 51,4 % опрошенных (14,2 % полностью и 37,2 % частично), в то время как не чувствуют себя защищёнными от криминалитета в Сети – 36,6 % (10,1 % полностью и 26,5 % частично).

Но это свидетельствует о том, что в современном обществе отечественный интернет-пользователь учится жить в условиях постоянных информационных угроз, но не о том, что проблемы информационной безопасности уходят на задний план. Подтверждением данного положения служит и распределение мнения респондентов о том, кто должен обеспечивать безопасность граждан в информационно-телекоммуникационной среде (рисунок 4). Более 2/3 опрошенных считают, что каждый человек должен сам заботиться о своей безопасности в информационно-коммуникационной среде. Поэтому подходом к обеспечению

информационной безопасности личности должен стать личностно-компетентный, а не ограничительно-запретительный [9].

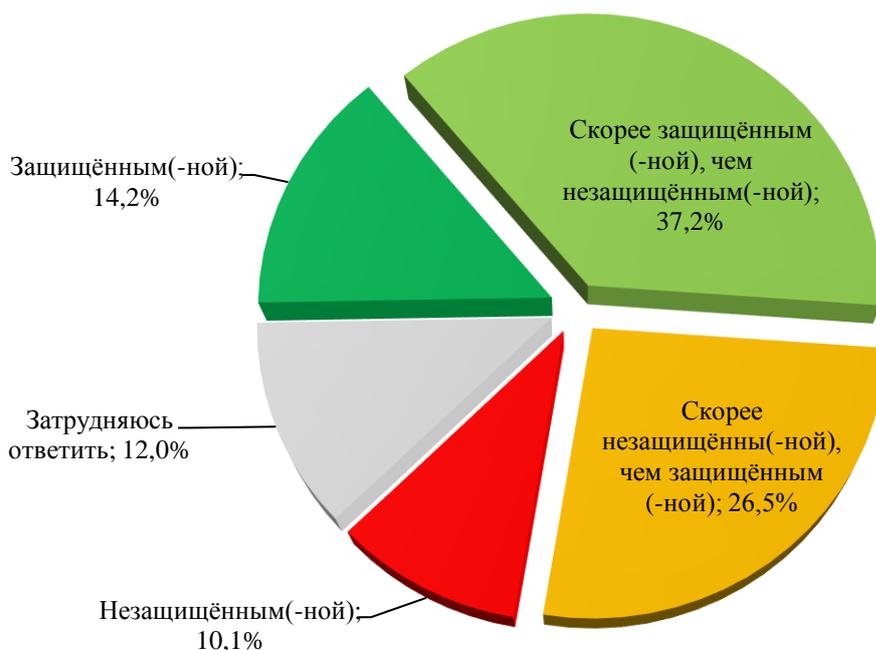


Рисунок 3. Распределение ответов на вопрос «Вы в целом чувствуете себя защищённым(-ной) или незащищённым(-ной) от преступных посягательств при работе в Интернете?», в %

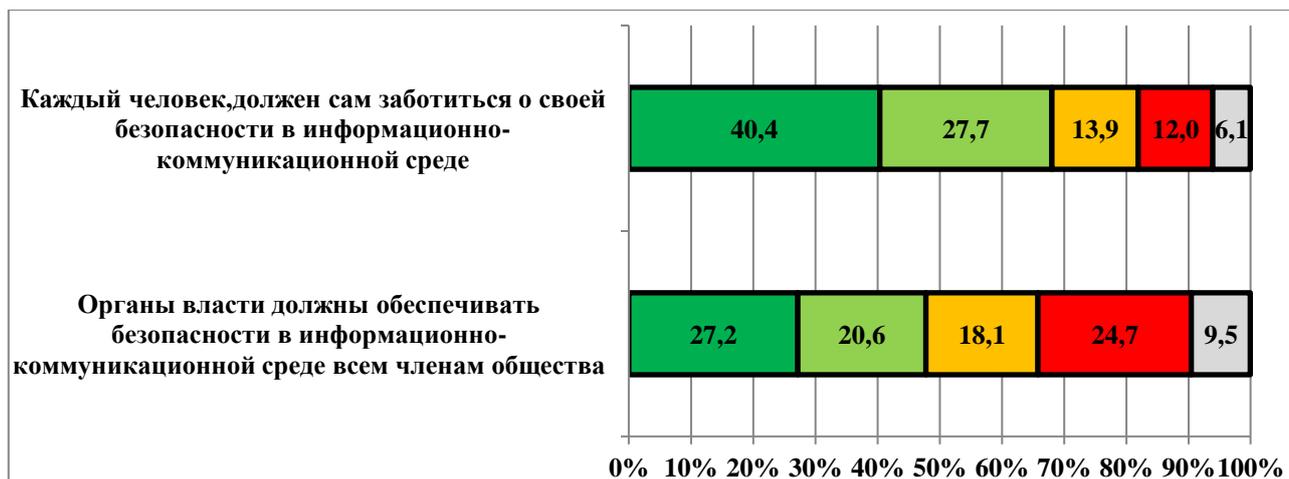


Рисунок 4. Мнение респондентов о том, кто должен обеспечивать безопасность граждан в информационно-телекоммуникационной среде

Выводы и рекомендации

К сожалению, самое слабое звено – это конечный пользователь. Хорошая безопасность требует глубокого понимания проблем и способов защиты от индивидов, которые ведут свою деятельность в информационно-коммуникационной среде. Для защиты пользователей предпринимается целый ряд мер безопасности. Эти инструменты постоянно развиваются в направлении усложнения для противодействия угроз информационной безопасности, то есть той совокупности потенциально возможных событий, процессов или действий, которые могут угрожать безопасности в информационно-коммуникационной среде.

Однако успешное функционирование мер безопасности по своей сути связано с конечным пользователем, который должен иметь навыки их применения [10]. Пользователь должен иметь хоть какое-то понятие об информационной безопасности, вредоносном программном обеспечении, чтобы своими действиями не нанести ущерб организации и самому себе. Пользователи интернета должны не только знать о возможных видах и схемах мошенничества, но и заботиться о методах защиты программного обеспечения, таких, как антивирус и своевременное обновление всех приложений, браузеров и систем. Только будучи в курсе событий, постоянно участь и интересуясь как новыми угрозами, так и методами их защиты пользователи могут обезопасить себя и своих близких от потерь.

ЛИТЕРАТУРА

1. Кривоухов А.А., Зотов В.В. Информационная безопасность как антропосоциотехнический феномен // Коммуникология. – 2017. – Т. 5. № 4. – С. 71–81.
2. Артамонов Д.С. Информационная безопасность личности в сети интернет // Стратегические коммуникации в современном мире: от теоретических знаний к практическим навыкам: Материалы Четвертой Международной научно-практической Интернет-конференции молодых ученых (26–30 октября 2015, г. Саратов). [Электронный ресурс]. – Саратов: СГУ им. Н.Г. Чернышевского, 2016. – С. 7–14.
3. Терехов А.В., Терехова О.А. Современные проблемы обеспечения информационной безопасности личности в интернет // Проблемы борьбы с киберпреступлениями в современном обществе: Сборник материалов Первой всероссийской конференции (13 мая 2016 г.) – Тамбов: Издательство Першина Р.В., 2016., – С. 23–28.
4. Шоричева А.Ю. Информационная безопасность личности в коммуникационной сети // Инновационные технологии: теория, инструменты, практика. – 2014. – Т. 2. – С. 180–182.
5. Кривоухов А.А. Оценка информационной безопасности интернет-среды пользователями социальных сетей. – Коммуникология. – 2018. – Том 6. №1. – С. 107–117.
6. Zhang K., Zhao L., Cao H.Q. Research on the Computer Network Crime and Information Security // Applied Mechanics and Materials. – 2014. – Vol. 687–691. – P. 1806–1809.
7. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 1 (24). – С. 45–55.
8. Сериева М.М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. – 2017. – №1. – С. 104–106.
9. Петрова В.А. Проблема информационной безопасности личности в современной педагогической науке и образовательной практике // Вестник Томского государственного педагогического университета. – 2016. – № 4 (169). – С. 120–125.
10. Talib S., Clarke N.L., Furnell S.M. Establishing A Personalized Information Security Culture // International Journal of Mobile Computing and Multimedia Communications (IJMCMC). – 2011. – №3(1). – P. 63–79.

Krivoukhov Anatoliy Anatolyevich

Kursk state agricultural academy named after I.I. Ivanov, Kursk, Russia

E-mail: anatka@rambler.ru

To assess the level of personal security in the information and communication environment by the criminal

Abstract. The article is devoted to the study of the level of personal security in the information and communication environment by the criminal. The purpose of this work is to determine the subjective opinion of citizens on the level of information security in the information and communication environment by the criminal. The main method of collecting information was a sociological survey conducted in 2019 among the population of the Kursk region as the median in the level of informatization. The sample was 1000 respondents aged 16 and over living in urban and rural settlements in the region. The results of the survey were further systematized and analysed.

The author comes to understand the information and communication environment as an anthroposociotechnical phenomenon, which allows to consider personality as one of the key links of information security in the triad (individuum – communications – technology). Assessment of information security allows to conclude that users estimate life activity in modern society dangerous. But at the same time, despite falling under the criminal actions of the attackers of a large part of the population, the latter is in no hurry to recognize the Internet as criminal and places responsibility on the person himself. This makes it possible to conclude that citizens are ready to live in conditions of information security risks. In conclusion, the author concludes that competence in information security needs to be developed.

Keywords: information and communication environment; cybercrime; Internet; personal information security; information and telecommunication technologies; sociological survey

REFERENCES

1. Krivoukhov A.A., Zotov V.V. (2017). Information Security as an Anthroposociotechnical Phenomenon. *Communicology*, 4(5), pp. 71–81 (in Russian).
2. Artamonov D.S. (2016). Informatsionnaya bezopasnost' lichnosti v seti internet. [*Personal Information Security on the Internet.*] Saratov: Saratov National Research State University named after N.G. Chernyshevsky, pp. 7–14.
3. Terekhov A.V., Terekhova O.A. (2016). Sovremennye problemy obespecheniya informatsionnoy bezopasnosti lichnosti v internet. [*Modern problems of ensuring personal information security on the Internet.*] Tambov: Publishing House Pershina R.V., pp. 23–28.
4. Shoricheva A.Yu. (2014). Information security of a person in a communication network. *Innovative technologies: theory, tools, practice*, (2), pp. 180–182 (in Russian).
5. Krivoukhov A.A. (2018). Assessment of information security of the Internet environment by users of social networks. *Communicology*, 1(6), pp. 107–117 (in Russian).
6. Zhang K., Zhao L., Cao H.Q. (2014). Research on the Computer Network Crime and Information Security. *Applied Mechanics and Materials*, (687–691), pp. 1806–1809.
7. Nomokonov V.A., Tropina T.L. (2012). Cybercrime as a new criminal threat. *Criminology: yesterday, today, tomorrow*, 1(24), pp. 45–55 (in Russian).
8. Serieva M.M. (2017). Cybercrime as a new criminal threat. *New Legal Bulletin*, 1, pp. 104–106 (in Russian).
9. Petrova V.A. (2016). The problem of personal information security in modern pedagogical science and educational practice. *Bulletin of Tomsk State Pedagogical University*, 4(169), pp. 120–125 (in Russian).
10. Talib S., Clarke N.L., Furnell S.M. (2011). Establishing A Personalized Information Security Culture. *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)*, 3(1), pp. 63–79.