ISSN 2524-2369 (Print)
ISSN 2524-2377 (Online)
УДК 316.485.6
https: //doi.org/ 10.29235/2524-2369-2019-64-2-145-150

Поступила в редакцию 25.09.2018
Received 25.09.2018

А. Г. Климашин

Институт социологии Национальной академии наук Беларуси, Минск, Беларусь

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ В ЦИФРОВУЮ ЭПОХУ

Аннотация. Рассматриваются актуальные вопросы, связанные с появлением новых технологий и технических решений, в частности, в сфере использования глобальной сети Интернет. В последние годы значимость использования цифровых инструментов для решения задач по коммуникации среди преступных сообществ, поиску и сбору персональных данных как для их вербовки, так и воздействия на психику значительно возросла. Вместе с тем цифровое пространство активно используется отдельными государствами, корпорациями и группами лиц для ведения информационно-алгоритмической войны и воздействия на общественное сознание, а технологии распределенных сетей стали способствовать финансированию запрещенных организаций. Автор анализирует не только юридические и технические возможности по обеспечению безопасности личности, но и социологический аспект, связанный с тем, как в целом появление рассмотренных факторов влияет на обеспечение безопасности государства и личности.

Ключевые слова: управление интернетом, информационный поток, фейк-ньюс, информационно-алгоритмическая война, цифровое пространство, распределённые сети, теневой интернет, блокировка

Для цитирования. Климашин, А. Г. Информационная безопасность личности в цифровую эпоху / А. Г. Климашин // Вес. Нац. акад. навук Беларусі. Сер. гуманіт. навук. – 2019. – Т. 64, № 2. – С. 145–150. https: //doi.org/ 10.29235/2524-2369-2019-64-2-145-150

A. G. Klimashin

Institute of Sociology of the National Academy of Sciences of Belarus, Minsk, Belarus

INDIVIDUAL INFORMATION SECURITY IN DIGITAL ERA

Abstract. The article presents topical issues related to the emergence of new technologies and technical solutions, in particular connected to the Internet. Over the last years, the importance of digital technologies for solving the problems of communication between criminal communities, of search and collecting personal data not only for their recruitment, but also for psychoactivity has increased significantly. At the same time, the digital space is actively used by separate States, corporations and groups of individuals for information and algorithmic warfare and impact on public consciousness, and technologies of distributed networks began to promote financing of the prohibited organizations. The author analyzes not only legal and technical possibilities to ensure safety of the individual, but also the sociological aspect associated with the impact that these considered factors have on safety and security of the state and individual.

Keywords: internet governance, information flow, fake news, information and algorithmic warfare, digital space, distributed networks, dark net, blocking

For citation. Klimashin A. G. Individual information security in digital era. *Vestsi Natsyyanal'nai akademii navuk Belarusi. Seryia humanitarnykh navuk = Proceedings of the National Academy of Sciences of Belarus. Humanitarian Series*, 2019, vol. 64, no. 2, pp. 145–150 (in Russian). https: //doi.org/ 10.29235/2524-2369-2019-64-2-145-150

По данным Информационно-аналитического центра (далее – ИАЦ) при Администрации Президента Республики Беларусь, в нашей стране более 4,5 млн активных пользователей глобальной сети Интернет. На данный момент средний белорус скачивает информацию из сети со скоростью почти в 14 Мбит/с. При этом 39 % респондентов проводят в Интернете более трех часов ежедневно. Компьютер есть более, чем в половине домохозяйств, 62 % совершеннолетних жителей страны являются пользователями, 87 % из них входят в сеть ежедневно. Среди студенческой молодёжи эта цифра достигает 94 %. При этом потребление трафика от внутренних ресурсов Республики Беларусь составило лишь 6 % от объемов внешнего шлюза [1]. Согласно данным исследований ИАЦ при Администрации Президента Республики Беларусь, почти 85 % белорусских пользователей отмечают, что используют интернет как главный источник информации, 46 % кон-

кретизируют, что ищут в том числе и политические новости. На вопрос о том, какой сайт запускают первым, пользователи отвечают – поисковик (32 %), социальную сеть (28 %) и новостной сайт (24 %). Поступающей информации от новостных сайтов доверяют 58 %, и больше трети – социальным сетям, примерно столько же прислушиваются к мнениям других пользователей, 96 % пользователей Беларуси имеют профиль хотя бы в одной из социальных сетей (*«ВКонтакте», «Одноклассники», «Facebook»* и др.) [2; 3].

В связи с тем, что РУП «Белтелеком» создало прямые пиринговые каналы с российскими представительствами наиболее посещаемых белорусами сайтов, мобильные операторы стали создавать тарифные планы, где не ведётся учёт трафика популярных мессенджеров (*«Viber», «Telegram», «WhatsApp», «WeChat»* и др.). Получает распространение новый вид Интернет-услуг – мобильное видеовещание и телевидение.

В связи с этим можно отметить быстрый рост интереса за последние несколько лет к обеспечению информационной безопасности как государства и общества, так и отдельной личности [4]. Организация Объединённых Наций (далее – ООН) инициировала проект «Форум по управлению интернетом» (сокращённо – IGF), который ежегодно проходит в каждом государстве с целью аккумулирования всех существующих вопросов и идей, связанных с управлением и безопасностью в цифровом пространстве. Это мероприятие служит объединению людей из различных групп и заинтересованных сторон на равных в обсуждении вопросов государственной политики, связанных с Интернетом. На текущий момент нет конкретных результатов, но в переговорах самым активным образом задействовано межсекторальное сотрудничество (*бизнес, государство, некоммерческие организации*), что доказывает высокую актуальность и значимость вопроса. На своем ежегодном совещании делегаты обсуждают, обмениваются информацией и передовым опытом друг с другом. IGF призван максимизировать возможности Интернета и снизить социальные риски и проблемы. Форум учреждён резолюцией Генеральной Ассамблеи ООН от 16 декабря 2015 г. № 70/125 [5].

Следует различать защиту информации и информационную безопасность. Защита информации – это комплекс мероприятий, направленных на сохранность накопленной информации и недопущение её разглашения. Основные её составляющие: конфиденциальность, целостность, доступность. Под информационной безопасностью следует понимать защиту интересов субъектов информационных отношений. Следовательно, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Угрозы информационной безопасности – это противоположная сторона использования информационных технологий [6; 7].

Однако при социологическом анализе для нас важна не столько техническая сторона вопроса, сколько **оценка влияния технологии на общество и оценка рисков, связанных с появлением технологии**. С появлением и развитием международной сети Интернет очевидно возникла проблема соотношения соблюдения прав человека и обеспечения национальной безопасности. Соблюдение прав человека напрямую связано с защитой личности, так как ограничение её прав и свобод влияет на уменьшение возможностей для отстаивания своих интересов и ценностей. Однако при этом человек может неосознанно подвергаться другим видам воздействия, таким как психологическое, информационное, кибермошенничество и прочее, что также существенным образом подвергает его и наше общество опасности.

Одна из наиболее дискуссионных проблем заключается в том, что в сети Интернет известные субъекты осуществляют слежение за неопределённым кругом лиц вопреки процессуальному законодательству, т. е. осуществляют оперативный поиск потенциальных правонарушений через изучение среды, а не через оперативные мероприятия в отношении конкретного подозреваемого. В то же время даже такие меры не позволяют предотвращать террористические акты, наращивание потенциала террористических движений, распространение порнографической продукции, хищение денежных средств через компьютерные сети и т. д. Фактически проблема трудно разрешаема в силу несовместимости решений. По сути это новая плоскость спора правозащитных организаций и так называемого «силового блока». Человек должен смириться либо с отказом от личной жизни и анонимности в сети Интернет, либо самостоятельно заботиться о состоянии

защищенности своих информационных систем и психики, не уповая на органы внутренних дел, что также проблематично для обывателя.

С технической стороны серьезной проблемой по ликвидации анонимности в сети стала технология так называемой распределённой сети и нестандартные протоколы, используемые в DarkNet (*теневой Интернет*). Помимо него существует и ряд других распределённых одноранговых сетей, но в «теневом Интернете» файлообмен происходит полностью анонимно (*поскольку IP-адреса не доступны публично*), и, следовательно, пользователи могут общаться без государственного вмешательства. Именно поэтому он часто воспринимается людьми как инструмент для осуществления коммуникации в различного рода «подпольях» и незаконной деятельности. В более общем смысле термин «DarkNet» может быть использован для описания некоммерческих «узлов» интернета или относиться ко всем «подпольным» интернет-коммуникациям и технологиям, которые в большинстве связаны с нелегальной деятельностью или инакомыслием. Подобные технические решения сегодня реализуются при обороте криптовалют (например, *BitCoins*) и соединении субъектов информационных отношений для обхода блокировок либо при необходимости в безопасной передаче данных. Использование распределённой сети и нетипичных протоколов не поддаётся контролю через информационную среду, и, по мнению специалистов, полностью лишает возможности достоверно установить субъектов обмена информацией. Это лишь означает, что от значительной массы угроз в информационном пространстве личности всё же придется каждому индивиду самостоятельно оказывать противодействие. Для этого необходимо обладать цифровой грамотностью и ответственно подходить к своим действиям в информационном поле настолько же, насколько и в реальной жизни.

В последнее время возросла угроза рисков информационной безопасности не столько технического (*вирусы, атаки на информационные системы, хищения*), сколько психологического характера.

Сегодня в сфере информационной безопасности главенствующей угрозой безопасности являются отсутствие системного подхода в государственных реформах, связанных с управлением информационными потоками, и ***постоянные вбросы лживой информации*** в массы населения со стороны враждебно настроенных субъектов, что дискредитирует отдельные институты власти. При этом ответственности за так называемые *«фейк-ньюс»* не существует. Актуальность этой проблемы подтверждают и темы последних российских политических ток-шоу, и научные дискурсы. В частности, на конференции «Проблемы обеспечения национальной и региональной безопасности: правовые и информационные аспекты», проведённой в Институте национальной безопасности КГБ Республики Беларусь, проблема информационной безопасности выделена в отдельную, самую массовую секцию [8]. Кроме того, контент пропагандистского характера выполняет весомую роль при психологической обработке личности для последующей вербовки в террористические сообщества. Так, например, по оценке специалистов, в террористической организации ИГИЛ насчитывается около 3 000 граждан стран СНГ, значимую роль в вербовке которых сыграла публичная коротко-текстовая социальная сеть «Twitter» [8, с. 110–115].

Вербовка новых членов в такие организованные группы возможна благодаря следующей формуле: ***мотивы для девиантного поведения + доступ к информации + возможность анонимной коммуникации с представителями группировок***. Отсюда следует, что для борьбы с формами деликвентного (*форма девиантного поведения, заключающаяся в совершении деликтов, т. е. правонарушений*) поведения необходимо создавать социальные условия для самореализации личности, защиты её прав и законных интересов в рамках существующего общественного строя; контролировать доступ к персональным данным и блокировать деструктивный контент; иметь технические и кадровые возможности для контроля подозреваемых как через информационную среду, так и в режиме реального времени через профессиональное осуществление оперативно-розыскных мероприятий. Для совершенствования способов борьбы и способов защиты личности необходимо понимание того, как система работает сейчас.

Наличие мотивов совершения тех или иных действий у потенциальных жертв вербовки оценивается благодаря открытым данным в социальных сетях. Кроме того, отследить посетителей своих информационных ресурсов можно как через IP-адреса, отображаемые у системного администратора ресурса, так и через так называемые «лайки» и «репосты». Стоит отметить, что по-

добная схема является достаточно универсальной для большинства радикальных течений, поскольку общение через Интернет и социальные сети для рядовых граждан – наиболее понятный способ социальной коммуникации.

В настоящее время существует много нелегального контента, расположенного в «Twitter» [8, с. 111–114] (*зарегистрировано в Сан-Франциско, США*). И если юридически новые поправки в Закон «О средствах массовой информации» помогают с лёгкостью блокировать доступ пользователей к отдельным страницам, то с технической стороны вопрос значительно сложнее, так как любой пользователь может обойти блокировку, используя «DarkNet» (*TorBrauser, 2P2, Kaspersky Security Connection, VPN Brauser, Orbot* и другие инструменты). Намного более эффективно бороться с контентом, оказывающим деструктивное воздействие на психику и мировоззрение граждан, с помощью полного удаления контента с серверов. Однако в случаях, когда хостинг расположен в других странах, возможность воздействия на него зависит исключительно от позиции государства, которое не всегда может вести борьбу с таким контентом.

Управление по раскрытию преступлений в сфере высоких технологий МВД занимается борьбой с хищениями с использованием компьютерной техники (ст. 212 Уголовного кодекса) и преступлениями против информационной безопасности (гл. 31 Уголовного кодекса). Раскрываемость этих преступлений достаточно высокая. По мировым стандартам, она составляет около 50 % и выше. В 2015 году она составила 56,5 %. Это высокий процент, если учитывать, что большинство подобных преступлений совершается в условиях неочевидности. Тем не менее количество преступлений против информационной безопасности растет. В 2016 году их было около 500. Как отмечает руководитель специальной следственной группы Следственного комитета Республики Беларусь по киберпреступности Александр Сушко, наибольшую проблему в расследовании этих дел как раз представляет их осложнённость иностранным элементом [9]. Ведь преступники, даже не находясь за пределами государства, в своих деяниях пользуются иностранными прокси-серверами. Так, например, сервера социальных сетей «ВКонтакте», «Facebook» также находятся в юрисдикции других государств, что затрудняет процесс расследования преступных дел. Именно поэтому для установления местонахождения преступника и получения свидетельств об этом требуется активная коммуникация соответствующих органов на международном уровне. Но такая коммуникация не всегда возможна в силу закрытости специальных служб, межгосударственных противоречий, отсутствия опыта совместной работы.

Более того, в последнее время получили широкое распространение такие сервисы, как CLOUDFLARE, privacyguardian.org, netprotect.support и т. д., которые предоставляют пользователям сокрытие информации об их IP-адресах, хостингах, e-mail, заменяя их своими. Несколько раз даже встречались случаи, когда RIPE вообще писал, что у такого доменного имени нет IP-адреса. При расширении такой практики бороться с нелегальным контентом непросто.

Но если вопрос с публикацией пропагандистского контента (содержания) технически может быть решен в ближайшей перспективе с помощью блокировки или удаления нелегального контента через многочисленные запросы в иностранные правоохранительные структуры, то проблема наличия доступа к персональным данным через информационные банки данных, социальные сети и публикации объявлений все же существует. Вопрос заключается в противоречивости позиций гражданского общества и государства. Безусловно, открытость данных для развития общества является благом. И сегодняшние тенденции ведут к повышению транспарентности деятельности государственных органов и различных организаций. Это помогает людям принимать более взвешенные решения, упрощает административные процедуры и способствует более быстрому поиску и контакту с подходящими лицами. Однако открытость данных позволяет также злоумышленникам получать почти полные данные о потенциальных жертвах преступлений и потенциальных агентах преступного сообщества. Несмотря на исключительную компетенцию специальных служб и правоохранительных органов на обращение с персональными данными, многие из них доступны коммерческим организациям (*сотовые операторы, банки, страховые организации, визовые центры* и т. д.). Сегодня для поиска информации о человеке не требуется специальной техники и большого объема специализированных знаний. Для установления личности необходимы усидчивость и высокоскоростное соединение с глобальной сетью. Фактически

любое лицо с аналитическими способностями и знаниями психологии может изучить политические взгляды и убеждения по тем или иным многочисленным комментариям, статусам, статьям в блогах, опубликованным научным статьям и т. д. Социальные сети позволяют установить место проживания, место работы и круг общения жертвы. Более того, с потенциальной жертвой очень просто вступить в коммуникацию. Фильтровать трафик таких сообщений весьма сложно по ряду причин. Во-первых, это будет усложнять проблему соблюдения прав человека, во-вторых, это слишком большой объём работы, поскольку на подсознательном уровне и в приватных беседах проследить склонности к смене общественного строя можно у многих людей, но при этом преследовать их лишь за умысел будет незаконно и не совсем правильно.

Что касается отслеживания коммуникации участников радикальных течений, то контроль через информационную среду также видится более сложным решением, чем контроль через подозреваемых в режиме реального времени. Одним из нескольких известных способов конспиративной связи посредством сети Интернет являются компьютерные онлайн-игры. Большая часть сообщений идёт через игровую консоль, в которой технически невозможно фильтровать трафик.

Правозащитный подход к проблеме заключается в том, что специальные службы должны больше концентрироваться на работе в реальной жизни, чем в цифровом пространстве, так как в противном случае это неизменно ведёт к тому, что в процессе оперативно-розыскных мероприятий происходит нарушение прав человека и незаконным образом отслеживается его личная переписка. На специальной комиссии после инцидента с участием Эдварда Сноудена директор Агентства национальной безопасности США признался в том, что в процессе специальной деятельности проводится собирание личных данных как иностранцев, так и граждан США. Однако он отметил, что это происходит неумышленно, а в силу специфики технологического процесса. Следовательно, например, при выявлении покупателей оружия могут отслеживаться поисковые запросы в системе Google, но вместе с таким мониторингом корпорация собирает и хранит поисковые запросы всех остальных граждан. Подобные технологические возможности в США привели к тому, что уже неоднократно возникали судебные споры с участием Google, Apple по подозрению их в установлении средств негласного получения информации на свою продукцию. При этом даже такие беспрецедентные меры не привели к снижению уровня террористической угрозы и снижению количества актов терроризма ни в США, ни в мире.

В XXI веке дипломатические, информационные, военные, экономические и правоохранительные компоненты национальной мощи будут оперировать в глобальной среде, характеризуемой социально-экономической сложностью, неопределенностью и динамичностью. В новой глобальной цифровой среде процветание и безопасность народов в значительной мере зависят от обеспечения стратегического преимущества и мощи национальной безопасности в сфере использования «электромагнитного спектра технологий». Эти инструменты действуют независимо от геополитических границ, что придает новые возможности и создает дополнительные риски для их использования в сфере коммерции, управления, безопасности и военного дела в рамках отдельных государств, их сообществ и глобальном масштабе в целом [10, с. 71–79].

Для защиты личности в указанной области в Республике Беларусь в целях разрешения подобных проблем была создана специальная группа – Национальный центр по реагированию на компьютерные инциденты при Оперативно-аналитическом центре (CERT) [11]. Официальный сайт подразделения CERT.BY осуществляет сбор, хранение и обработку статистических данных, связанных с распространением вредоносных программ и сетевых атак на территории Республики Беларусь, а также реагирование на сами инциденты как в информационных системах государственных органов и организаций, так самостоятельно обратившихся субъектов национального сегмента сети Интернет. Задачей группы является не только борьба с киберпреступностью, но и выработка механизма по работе в этой сфере. Как отмечает руководитель группы, сложность работы во многом заключается в том, что компьютерные инциденты, как правило, выражаются в новых и новых формах. Поэтому при появлении нетипичных событий действовать требуется скорее в соответствии с профессиональной интуицией, нежели по предписанным правилам.

Таким образом, в идеологическом и мировоззренческом плане решение видится в том, что в первую очередь появление новых цифровых технологий не должно заменять реальной жизни. Это скорее должно являться дополнительной возможностью и дублированием неких функций. Способы

социальной коммуникации должны развиваться и давать человеку выбор, но ни в коем случае не вгонять его в рамки навязываемого США и их союзниками нового мирового порядка. Именно тогда человек как личность сможет быть более самодостаточным и независимым от какой-либо системы, в том числе цифровой.

Список использованных источников

1. Емкость внешнего шлюза в сеть Интернет за пять лет увеличилась в 15 раз [Электронный ресурс] // Белтелеком : нац. оператор электросвязи Респ. Беларусь. – Режим доступа: http://beltelecom.by/news/company/emkost-vneshnego-shlyuza-v-set-internet-za-pyat-let-uvelichilas-v-15-raz. – Дата доступа: 29.12.2017.

2. Медиасфера Беларуси. Социологический аспект [Электронный ресурс] / под общ. ред. В. О. Дашкевича. – Минск, 2017. – Режим доступа: http://iac.gov.by/sbornik/Mediasfera_Belarusi.pdf. – Дата доступа: 29.12.2017.

3. Более 87 % белорусских юзеров обращаются к интернету практически ежедневно [Электронный ресурс] // БелТА : белорус. телеграф. агентство. – Режим доступа: http://www.belta.by/tech/view/bolee-87-belorusskih-juzerov-obraschajutsja-k-internetu-prakticheski-ezhednevno-176980-2016/. – Дата доступа: 02.01.2016.

4. Бабосов, Е. М. Обеспечение информационной безопасности – фактор устойчивого развития Беларуси / Е. М. Бабосов // Весн. Брэсц. ун-та. Сер. 1, Філасофія. Паліталогія. Сацыялогія. – 2012. – № 2. – С. 133–141.

5. Internet Governance Forum (IGF) [Electronic resource]. – Mode of access: www.intgovforum.org/multilingual/tags/about. – Date of access: 29.04. 2018.

6. Бобкова, В. А. Информационная безопасность и её составляющие [Электронный ресурс] / В. А. Бобкова. – Режим доступа: https://studfiles.net/preview/2012615/. – Дата доступа: 29.04.2018.

7. Бабаш, А. В. Информационная безопасность. История защиты информации в России : [учеб. пособие] / А. В. Бабаш, Е. К. Баранова, Д. А. Ларин. – М. : Университет, 2013. – 736 с.

8. Проблемы обеспечения национальной и региональной безопасности: правовые и информационные аспекты : материалы Междунар. науч.-практ. конф., Минск, 2 нояб. 2017 г. : в 2 т. / Ком. гос. безопасности Респ. Беларусь, Ин-т нац. безопасности Респ. Беларусь ; [редкол.: А. Л. Лычагин (гл. ред.) и др.]. – Минск : ИНБ, 2018. – Т. 2. – 307 с.

9. Безопасность в Сети: практика борьбы с киберпреступлениями [Электронный ресурс] // БелТА : белорус. телеграф. агентство. – Режим доступа: https://www.belta.by/onlineconference/view/bezopasnost-v-seti-praktika-borby-s-kiberprestuplenijami-906/. – Дата доступа: 29.07.2018.

10. Ларина, Е. С. Мировойна. Все против всех / Е. С. Ларина, В. С. Овчинский. – М. : Кн. мир, 2015. – 416 с.

11. CERT.BY – Национальный центр реагирования на компьютерные инциденты при ОАЦ при Президенте Республики Беларусь [Электронный ресурс]. – Режим доступа: https://cert.by. – Дата доступа: 29.04.2018.

References

1. The capacity of an external gateway to the Internet has increased 15 times over five years. *Beltelekom* [Beltelecom]. Available at: http://beltelecom.by/news/company/emkost-vneshnego-shlyuza-v-set-internet-za-pyat-let-uvelichilas-v-15-raz (accessed 29.12.2017) (in Russian).

2. Dashkevich V. O. (ed.) *Media sphere of Belarus. Sociological aspect*. Minsk, 2017. Available at: http://iac.gov.by/sbornik/Mediasfera_Belarusi.pdf (accessed 29.12.2017) (in Russian).

3. More than 87 % of Belarusian users access the Internet almost daily. *BelTA*. Available at: http://www.belta.by/tech/view/bolee-87-belorusskih-juzerov-obraschajutsja-k-internetu-prakticheski-ezhednevno-176980-2016/ (accessed 02.01.2016) (in Russian).

4. Babosov E. M. Provision of information security as a factor for sustainable development of Belarus. *Vesnik Brestskaga universiteta. Seryya 1. Filasofiya. Palitalogiya. Satsyyalogiya = Vesnik of Brest University. Series 1. Phylosophy. Politology. Sociology,* 2012, no. 2, pp. 133–141 (in Russian).

5. *Internet Governance Forum (IGF).* Available at: www.intgovforum.org/multilingual/tags/about (accessed 29.04. 2018).

6. Bobkova V. A. *Information security and its components*. Available at: https://studfiles.net/preview/2012615/ (accessed 29.04.2018) (in Russian).

7. Babash A. V., Baranova E. K., Larin D. A. *Information security. History of information security in Russia*. Moscow, Universitet Publ., 2013. 736 p. (in Russian).

8. Lychagin A. L. (et al.) *Problems of ensuring national and regional security: legal and informational aspects: materials of the International scientific and practical conference, Minsk, November 2, 2017. Vol. 2.* Minsk, Institute of National Security of the Republic of Belarus, 2018. 307 p. (in Russian).

9. Security on the Web: the practice of combating cybercrime. *BelTA*. Available at: https://www.belta.by/onlineconference/view/bezopasnost-v-seti-praktika-borby-s-kiberprestuplenijami-906/ (accessed 29.07.2018) (in Russian).

10. Larina E. S. arina E. S., Ovchinskii V. S. *World War. All against all*. Moscow, Knizhnyi mir Publ., 2015. 416 p. (in Russian).

11. *CERT.BY – National Computer Emergency Response Team of the Republic of Belarus*. Available at: https://cert.by (accessed 29.04.2018) (in Russian).

Информация об авторе

Климашин Александр Геннадьевич – аспирант. Институт социологии, Национальная академия наук Беларуси (ул. Сурганова, 1, корп. 2, 220072, Минск, Республика Беларусь). E-mail: alexandr89by@mail.ru.

Information about the author

Alexandr G. Klimashin – Postgraduate student. Institute of Sociology of the National Academy of Sciences of Belarus (1 Surganov Str., Bldg 2, Minsk 220072, Belarus). E-mail: alexandr89by@mail.ru.