Интернет-коммуникации военнослужащих и членов их семей в социальных сетях как объект изучения цифровой социологии

УДК 316.2 DOI 10.26425/2658-347X-2019-4-17-24

Получено 01.11.2019 Одобрено 02.12.2019 Опубликовано 31.12.2019

Ильина Наталья Валерьевна

Канд. юрид. наук, научный сотрудник, Научно-исследовательский (социологический) центр Министерства обороны России, г. Москва, Российская Федерация

ORCID: 0000-0001-6842-8247

E-mail: nataval_ilina@mail.ru

Суховская Юлия Юрьевна

Научный сотрудник, Научно-исследовательский (социологический) центр Министерства обороны России, г. Москва, Российская Федерация

ORCID: 0000-0003-3845-2267

E-mail: suhovskaya_jj@mail.ru

АННОТАЦИЯ

Рассмотрены концептуальные, методические и технологические подходы к организации социологического изучения коммуникативной интернет-активности военнослужащих в социальных сетях, специфика поведения в соответствии с требованиями к ним как членам военно-профессиональной корпоративной группы людей в информационно-коммуникационной сети «Интернет». Сделан анализ конституционных норм, ограничивающих права военнослужащих в различных сферах социального взаимодействия, а также нормы отечественного законодательства, которые конкретизируют эти требования. Указанный вид интернет-коммуникаций охарактеризован как объект изучения военной социологии на различных уровнях: общенаучном, частнонаучном и эмпирическом. Авторами установлена связь между рассматриваемой проблемой и концепциями «информационного общества», «цифрового социума», «цифровой экономики» и виртуализации социальных отношений, а также концепции «прав человека».

Выявлена общая тенденция включать в военно-доктринальные документы различных стран противоборства с вероятным противником в виртуальном пространстве. При этом обеспечение военной безопасности предполагает защиту сознания своих военнослужащих от негативного воздействия, в том числе в случае использования ими услуг в интернет-пространстве. Проведено описание опыта других стран по регулированию социальной активности военнослужащих и членов их семей в сети «Интернет». На основе обобщения социальной практики представлены выводы из рискологического анализа участия субъектов военно-профессиональной деятельности в социальных сетях, в связи с угрозами определения места дислокации воинских частей, планов перемещения войск, вооружения, штатного и персонального состава, то есть сведений, составляющих военную тайну. Также приведен перечень иных угроз, связанных с социальными коммуникациями военнослужащих и членов их семей в виртуальном пространстве. Представлены пути снижения рисков негативного воздействия на военнослужащих и членов их семей участия в социальных сетях и других видах интернет-коммуникаций через проведение нормативно-правовых, организационно-технологических и информационно-просветительских мероприятий.

Ключевые слова

Интернет-коммуникации, Интернет, военнослужащие, цифровая социология, семьи военнослужащих, нормы, социальный контроль, социальные сети.

Цитирование

Ильина Н.В., Суховская Ю.Ю. Интернет-коммуникации военнослужащих и членов их семей в социальных сетях как объект изучения цифровой социологии//Цифровая социология. 2019. Т. 2. № 4. С. 17–24.

Internet communications of military personnel and their families in social networks as an object of digital sociology's study

DOI 10.26425/2658-347X-2019-4-17-24

Received 01.11.2019 Approved 02.12.2019 Published 31.12.2019

Il'ina Natalia

Candidate of Jurisprudence, Researcher, Research (Sociological) Center of the Russian Ministry of Defense, Moscow, Russian Federation

ORCID: 0000-0001-6842-8247

E-mail: nataval_ilina@mail.ru

Sukhovskaya Yuliya

Researcher, Research (Sociological) Center of the Russian Ministry of Defense, Moscow, Russian Federation

ORCID: 0000-0003-3845-2267

E-mail: suhovskaya_jj@mail.ru

ABSTRACT

The conceptual, methodological and technological approaches to organization of sociological study of communicative Internet activity ofmilitary personnel in a social networks, the specific behavior in accordance with the requirements as to members ofthe militaryprofessional corporate group of people in the information-communication network "Internet" have been considered. The constitutional norms that restrict the rights of military personnel in various spheres of social interaction, as well as the norms of domestic legislation that specify these requirements have been analyzed. The described type of Internet communication has been characterized as an object of study of military sociology at various levels: general scientific, private scientific and empirical. The author's found a connection between a considered problem with the concepts of "information society", "digital society", "digital economy" and virtualization of social relations, as well as the concept of "human rights". The general tendency to include of various countries confrontation with a likely enemy in the virtual space in the military-doctrinal documents has been revealed. At the same time, ensuring military security involves protecting the minds of their military personnel from negative impact, including in the case of their use of services in the Internet space. The experience of other countries in regulating the social activity of military personnel and their families in the Internet has been described. Based on the generalization of social practice, conclusions from the risk analysis of the participation of subjects of military professional activity in social networks, which is associated with threats to determine the location of military units, plans for the movement of troops, weapons, staff and personnel, that is, information constituting a military secret, have been presented. A list of other threats related to social communications of military personnel and their families in the virtual space also has been adduced. The ways to reduce the risk of negative impact on military members and their families participate in social networks and other Internet communications by implementing legal, organizational and outreach activities have been presented.

Keywords

Internet communications, Internet, military personnel, digital sociology, military families, norms, social control, social networks.

For citation

Il'ina N.V., Sukhovskaya Yu.Yu. (2019) Internet communications of military personnel and their families in social networks as an object of digital sociology's study. *Digital sociology*. Vol. 2, no 4, pp. 17–24. DOI: 10.26425/2658-347X-2019-4-17-24

ВВЕДЕНИЕ

Объективной реальностью в современном обществе, которое характеризуется учеными как «сетевое» и «информационное», является высокий уровень включенности населения в целом, а также особых профессиональных групп, в том числе военнослужащих, в интернет-коммуникации, с помощью которых они не только получают доступ к соответствующим информационным ресурсам, но и во многом реализуют свои потребности в социальных коммуникациях, удовлетворении других потребностей, получении виртуальных услуг.

В рамках цифровой социологии эти позитивные аспекты участия различных категорий населения в социальных сетях нашли свое отражение в литературе [Юдина, 2017].

Вместе с позитивными возможностями использования интернет-ресурсов в различных сферах жизни возрастают и риски коммуникаций в виртуальном пространстве, на что обращают внимание отечественные доктринальные документы информационной безопасности[1], а также ученые и практики [Мерцалова, 2015; Хайбулина, 2012].

Феномен виртуализации социальных коммуникаций оказался связан с появлением деструктивных форм социальной активности, к которым, в частности, относят:

– киберпреступность во всех ее проявлениях;

– системы тотальной слежки, глобального прослушивания;

– «электронное мошенничество» в финансово-банковской сфере и интернет-телефонии;

– целенаправленные недобросовестные информационные компании и информационные войны;

– различные формы электронного терроризма и виртуальные формы вербовки террористов;

– неограниченный доступ к интернет-ресурсам, противоречащим основам правопорядка и нравственности (детская порнография, практики самоубийства, реклама наркотических веществ и др.);

– негативные интернет-технологии манипулирования общественным сознанием с целью достижения финансово-экономических выгод (финансовые кризисы, кризисы доверия, недобросовестная конкуренция) и политических задач (цветные революции) и др.

Необходимо учесть, что образ жизни современного человека характеризуется его тесной связью с виртуальным пространством, которое выступает зачастую источником получения референтных экспертных мнений по различным проблемам своей жизни, а виртуальные собеседники оказывают существенное влияние не только на содержание досуга, обмен информацией, но и на формирование оценок, ценностей, направленности личности.

Все это ставит перед цифровой и военной социологией особый круг исследовательских задач, связанных с изучением виртуальных коммуникаций военнослужащих в информационно-коммуникационной сети «Интернет» (далее – Интернет) на основе собственного методического арсенала анализа.

СОЦИОЛОГИЧЕСКИЕ ИССЛЕДОВАНИЯ ФЕНОМЕНА ВИРТУАЛЬНЫХ КОММУНИКАЦИЙ

В цифровой социологии в научно-практический оборот введены различные феномены виртуальных коммуникаций: поиск сведений, использование государственных сервисов, установление личных и групповых контактов в социальных сетях. Все эти формы изучаются военными социологами с точки зрения соответствия нормам военно-социального порядка, угроз нарушения военной и служебной тайны, повышения уязвимости военнослужащих и членов их семей вследствие недружественных воздействия спецслужб вероятного противника.

Социальные сети, как феномен цифрового общества, в общем виде диагностируется следующей совокупностью операциональных индикаторов:

– наличие интерактивного многопользовательского сайта как цифровой платформы виртуальных коммуникаций;

– процесс наполнения контентом добровольными участниками социальных сетей;

– группа (сообщество) пользователей, объединенных на основе взаимных интересов и выбравших виртуальную форму социального взаимодействия на едином ресурсе.

Цифровая социология реализует свою познавательную функцию на нескольких уровнях социального взаимодействия субъектов социального действия с институтами регулирования его активности в виртуальном пространстве социетальном, институциональном, организационном, конкретно-социальном.

Социетальный уровень социологического изучения участия военнослужащих и членов их семей в социальных сетях предполагает выявления характеристик глобального цифрового пространства как доступной виртуальной сферы реализации ими потребностей в получении информации, услуг, установления контактов между людьми. На этом уровне цифровая социология использует концептуальные взгляды на развитие «информационного общества» и превращение его в «коммуникационное общество», а в перспективе и «общество знания». Не менее важны и «цифровые» аспекты

[1] Стратегия национальной безопасности Российской Федерации (Утверждена Указом Президента Российской Федерации от 31 декабря 2015 г. № 683). Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/ (дата обращения: 12.10.2019).

проекции этих концепций в виде научного осмысления современных практик и коммуникационных интернет-платформ, облачных технологий, социальных сетей, возрастание у современного человека доли потребностей, которые удовлетворяются посредством виртуальных сервисов.

На методологическом уровне особым образом проявляются проблемы социального управления в цифровом обществе. В частности, в системе государственного управления вводятся в научно-практический оборот понятия «электронное правительство», «государство в смартфоне» и другие.

ВОЕННО-СОЦИАЛЬНАЯ ПРОБЛЕМАТИКА В СФЕРЕ ИНТЕРНЕТ-КОММУНИКАЦИЙ

Для функционирования социального института военной службы, эффективности военной организации и системы обеспечения военной безопасности в нашей стране целесообразно осмыслить в рамках цифровой социологии влияние на эту сферу становления информационного, цифрового общества, расширения виртуального пространства. Выделяя такой аспект военно-социальной проблематики, как участие субъектов военно-профессиональных отношений в социальных сетях, социологическое знание может иметь существенное значение для обоснования совокупности правил, ограничений и рекомендаций для военнослужащих по размещению персональной информации в социальных сетях, с другой стороны, обеспечить необходимую правовую защиту информации персональных сведений о военнослужащих и членах их семей, прежде всего, имеющих отношение к особо важной информации в сфере военной безопасности.

Отечественное законодательство, как составная часть общей системы социального порядка и социального контроля общества, обеспечивает закрепление особой правосубъектности военнослужащих, характеризующий его специфический статус в применении средств вооруженного насилия в интересах обеспечения военной безопасности страны, ее жителей. Возникающая при этом конкуренция конституционных норм о неотчуждаемости и принадлежности каждому от рождения основных прав и свобод человека, с одной стороны, а также возможностью ограничения прав и свобод человека и гражданина, в частности в целях обеспечения обороны страны и безопасности государства – с другой стороны[2], требуют отдельного концептуального осмысления применительно, в частности, к участию военнослужащих и членов их семей в социальных сетях.

Институциональный уровень социологического анализа в рамках цифровой социологии связан с использованием собственного эвристического потенциала, а также возможностей военной социологии в познании феномена вооруженной борьбы, института обеспечения военной безопасности, функционирования военной организации. Трансформация военно-теоретических основ вооруженной борьбы, обоснование новых типов войн и вооруженных конфликтов, разработка и принятие в войска средств вооруженной борьбы «шестого поколения» [Слипченко, 2002] корреспондирует с глобальными трендами становления нового коммуникационного интернет-пространства.

Некоторые аспекты этой проблематики описаны в военных доктринальных документах США, которые положены в основу соответствующих научно-теоретических основ американской военной науки.

Военно-социальные отношения, возникающие в процессе реализации полномочий военнослужащими (субъектами вооруженного насилия) при рассмотрении виртуального пространства как особой сферы военных конфликтов целесообразно осмыслить на методологическом аппарате «цифровой социологии». Более того, военно-теоретические концепции «сетевой войны», «сетецентрической войны» могут быть развиты в социальной проекции их места и роли в современной системе военной безопасности. Более того, цифровая социология имеет достаточный методический арсенал для исследования социальной активности военнослужащих в социальных сетях как фактора, влияющего на эффективность военной организации и военную мощь государства.

Используя результаты социологических исследований, органы военного управления и отдельные военнослужащие, получают дополнительную информацию для рефлексии содержания, целеполагания и норм военно-профессиональной деятельности в различные периоды – мирное время (повседневные условия), в период предвоенных мероприятий, а также в условиях военного конфликта (вооруженного конфликта, войны) с учетом социального факта использования им интернет-сервисов и участия в социальных сетях.

На следующем уровне исследований – организационном, исходя из социально-конструирующей функции цифровой и военной социологии, на основании полученных исследовательских данных необходимо проектирование системы мер, программ, моделей по снижению рисков интернет-активности военнослужащих.

Проведение этой работы предусматривает в частности научную рефлексию зарубежного опыта регулирования социальных отношений в виртуальном пространстве с целью его экстраполяции в функционирование института военной службы в российском обществе.

Военный социолог при этом изучает источники, связанные с освещением проблем социальных

[2] Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.) // Собрание законодательства Российской Федерации от 4 августа 2014 г. №31 ст. 4398. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 12.10.2019).

отношений в военной организации[3], документы методического и нормативного характера, в частности, доступные разнообразные административные сводные регламенты в различных армиях по:

– целесообразности и задачам использования военнослужащими социальных сетей;

– формам и ограничениям участия различных категорий военнослужащих в виртуальных социальных практиках взаимодействия с незнакомыми людьми[4], и общему регулированию активности людей в виртуальном пространстве.

Изучение современной практики социального контроля за соблюдением принципов гарантий свободы распространения информации и, одновременно, норм защиты от неправомерного использования частной и служебной информации военнослужащих, которая может быть получена из анализа их деятельности в социальных сетях, позволяет утверждать, что в различных странах устанавливают весьма специфические нормы правового регулирования этой сферы.

С точки зрения широкого толкования персональных данных, характерного для французской, шведской, венгерской и других правовых систем, к таким данным относится любая информация, связанная субъектом социального взаимодействия. Одновременно в системе социального контроля за поведением военных в Интернете в других государствах, в частности, в Великобритании, принято проводить операционализацию и законодательное закрепление конкретных компонентов личной информации, подлежащих ограничению со стороны государственных органов и специальных служб, а также критериев отнесения сведений к открытой или закрытой части информации о военнослужащем.

Общими характеристиками развития системы правового регулирования Интернета, участия в использовании его ресурсов, в части участия в социальных сетях отдельных категорий граждан (в частности, военнослужащих) в большинстве стран являются:

– развитие в национальных правовых системах относительно автономных групп норм, связанных с хождением информации, использованием персональных данных; при этом эти нормы в ряде случаев отграничены от норм охраны частной жизни и гарантий неприкосновенности личного приватного пространства;

– институциализация самостоятельной группы органов, уполномоченных на осуществление комплекса мер по защите персональных данных, административного контроля за соблюдением информационного законодательства;

– криминализация (введение норм уголовного наказания) за правонарушения в информационной сфере, неправомерный доступ и использование персональных данных.

Обзор доступных источников позволяет заключить, что специального законодательства и контролирующих органов, регламентирующих использование зарубежными государственными чиновниками социальных сетей, не существует. Вместе с тем, наряду с правовой защитой персональной информации, организованной на государственном уровне в абсолютном большинстве зарубежных стран, существует вполне достаточно негласных правил соблюдения этических норм использования персональных данных.

ЗАРУБЕЖНЫЙ ОПЫТ ПРАВОВОЙ РЕГЛАМЕНТАЦИИ ИНТЕРНЕТ-КОММУНИКАЦИЙ ОТДЕЛЬНЫХ КАТЕГОРИЙ НАСЕЛЕНИЯ

Рассмотрим основные особенности и тенденции нормативной и этической регламентации размещения в социальных сетях персональной информации о должностных лицах органов государственной власти и муниципалитетов в некоторых зарубежных странах.

Социальные, нормативно-правовые и программно-аппаратные системы защиты частной информации и, одновременно, ограничения реализации прав отдельных категорий населения (государственные служащие, военные, правоохранители, работники спецслужб) на получение информации различаются в разных странах. Прежде всего это относится к частной (личной) информации, персональным данным, которые относят в настоящее время к категории «чувствительной информации». Это обстоятельство позволяет расширить поле социологического исследования феноменов развития информационного общества в цифровой социологии, в том числе за счет методов сравнительного трансграничного и межкультурного анализа.

Изучение социального опыта регулирования безопасного размещения личной, служебной и корпоративной информации в Интернете позволяет представить следующий перечень механизмов защиты персональной информации от несанкционированного доступа и недобросовестного использования:

– закрепление индивидуальных и групповых социальных практик регулирования хождения информации в виртуальном пространстве в форме общедоступных правил поведения;

– установление корпоративных норм использования интернет-ресурсов и администрирования контента;

– привлечение государственно-правовых механизмов регулирования.

Так, например, при отсутствии в Великобритании конституционного акта в английском законодательстве

[3] Гиснель Ж. Французская армия вводит кодекс поведения в социальных сетях. Режим доступа: https://bit.ly/2URUUtX (дата обращения: 02.09.2019).

[4] Social Media Handbook (2013). Режим доступа: http://www.nationalguard.mil (дата обращения: 02.09.2019).

персональная информация определяется как информация о физическом лице, при помощи которой оно может быть идентифицировано. При этом в состав такой информации в юридическом смысле включено также и любое выраженное индивидуальное или групповое мнение о конкретном лице, хотя и без обозначения установок у человека, который пользуется личными сведениями при обнародовании информации.

Положения о конфиденциальности персональной информации содержатся в английском праве и в ряде других законодательных норм, регламентирующих ведение медицинских записей и хранение информации о потребительских кредитах, реабилитации правонарушителей, функционирование системы телекоммуникаций, деятельности полиции, институциональных основах вещания в этой стране, а также механизмах защиты от преследований.

Юридические нормы правовой системы Германии на конституционном уровне определяют, что такие формы передачи информации, как письма, почтовые отправления, различные виды телекоммуникации являются неприкосновенными, а ограничения, если в них возникает необходимость, могут вводиться только соответствующим законодательным актом.

Ограничение свободы информации в немецком законодательстве возможно, если оно направлено на:

– защиту строя страны – демократического и свободного;
– обеспечение существования страны;
– безопасность страны.

Более того, законом разрешается не оповещать об ограничении заинтересованных лиц, а судебное рассмотрение жалоб на неправомерность таких действий может заменяться упрощенными процедурами рассмотрения конфликта. Интересным представляется и тот факт, что попытки изменения конституционных норм защиты информации в немецкой правовой системе не завершаются успехом в силу ее консервативности.

В Германии на конституционном уровне берется под защиту право на неприкосновенность частной жизни, а в законодательство введено право на информационное самоопределение.

Во Франции отсутствуют конституционные нормы о каких-либо гарантиях неприкосновенности личности жизни граждан, а также частной (семейной) приватности. Однако в этой стране на законодательном уровне детально регламентируется порядок и условия обработки персональной информации. Под персональными данными, как объектом защиты, понимаются данные, которые позволяют в любой форме, прямо или косвенно, установить личность физического лица, в отношении которого эти данные собраны, независимо от того, физическим или юридическим лицом они были обработаны [Сергейчик, 2009].

Немецкий законодатель также закрепил правомерность дифференцированного подхода к работе с персональными (личными, частными) данными в зависимости от целеполагания их анализа и последующего использования.

На конкретно-социальном уровне проводится социологическое исследования социального взаимодействия, осуществляемого конкретными военнослужащими, которые проходят воинскую службу в подразделениях, частях, соединениях. Применяемые при этом методы онлайн или традиционных опросов сосредотачиваются преимущественно на выявлении:

– уровня вовлеченности различных категорий военнослужащих в социальные коммуникативные практики в виртуальном пространстве;
– уровня доверия к различным интернет-ресурсам и удовлетворенность использования их сервисов;
– оценке рисков разглашения военнослужащими служебной и военной тайны через коммуникации в социальных сетях.

Диагностируемые цифровой социологией риски негативного воздействия на статус, служебные и частные интересы военнослужащих вследствие применения противоправных форм завладения и использования личной информации связаны со следующими обстоятельствами:

– недостаточное правовое регулирование интернет-пространства;
– размещение базовых компонентов инфраструктуры глобального интереса в зарубежных странах, которые проводят недружественную политику в отношении Российской Федерации;
– низкий уровень цифровой культуры и компетенций по защите личных данных у существенного числа военнослужащих и членов их семей.

ГРУППЫ РИСКОВ УЧАСТИЯ ВОЕННОСЛУЖАЩИХ В СОЦИАЛЬНЫХ СЕТЯХ

Рассмотрим далее объектно-предметное поле рискологического анализа участия военнослужащих и членов их семей в социальных сетях в цифровой социологии, выделив отдельные группы рисков.

1. Первая группа рисков, которые могут диагностироваться методами цифровой социологии – риски нанесения ущерба личности военнослужащего, материальному благосостоянию, психическому здоровью, чести и достоинству проистекают в силу неправомерного получения доступа посторонних лиц к персональной, удостоверяющей, медицинской и финансовой информации, сведениям о семейных и родственных отношениях.

Военная история и анализ современных вооруженных конфликтов показывает, что сбор личной информации об участниках боевых действий, как

рядовых, так и офицеров спецназа, летчиках и т.п. осуществляется по всей совокупности личной информации, а затем адресно размещается на открытых интернет-ресурсах террористических группировок, ангажированных некоммерческих организаций и недружественных государств.

2. Вторая группа рисков, которые изучаются цифровой социологией, включает вероятность проведения информационно-психологических враждебных мероприятий в рамках информационной войны, осуществления негативных информационных вбросов фейковой информации, а также осуществления диффамации должностных органов военного управления, властных структур, реализующих полномочия в сфере военной безопасности.

Практика показывает, что если военнослужащий свободно размещает личную информацию, фото на фоне военной техники и опознаваемой местности либо цифровые снимки с геолокационными метками, свои комментарии к блокам, осуществляет репосты либо создает собственный интернет-контент, или если делает общедоступным сам факт своего участия в какой-либо социальной сети, то эти материалы могут быть включены во враждебную информационную компанию против нашей страны, военной организации, командного состава и отдельных военнослужащих. Понятно, что особо актуальной эта информация становится в период реальных боевых действий, выполнения служебно-боевых задач, так как она может быть включена в проведение конкретных враждебных информационно-психологических операций.

3. Третья группа подлежащих социологическому изучению рисков связана с возможностью трансформации ценностно-нормативных основ поведения и деятельности военнослужащего под влиянием негативных явных и скрытых социально-психологических технологий на его сознание. Достаточно наглядным примером трансформации правосознания и ценностей на противоположные могут стать получившие широкую известность факты придания общедоступности американским военнослужащим Б. Менингом и сотрудником спецслужб США Э. Сноуденом доступной им в силу профессионального статуса секретной военной информации.

4. Четвертую группу изучаемых рисков составляет детермированность повышения уровня открытости частной жизни военнослужащих, а значит, и уязвимости к внешнему воздействию в силу увеличения каналов интернет-коммуникаций и повышения плотности (насыщенности) информационного потока у активных пользователей Интернета. Необходимо при этом подчеркнуть, что военнослужащий – не только частное лицо, но и носитель ограниченной для использования информации (служебной и военной тайн).

Повышенную опасность для утраты секретной и конфиденциальной информации представляют размещение в социальной сети и создание условий для доступа посторонних лиц не только к секретной информации, но и фрагментарные сведения о местах службы, регионах и способах передислокации, сослуживцах, событиях, командном составе и т.п., которая представляет определенную разведывательную ценность по результатам ее анализа и сопоставления. Снижению или исключению этих рисков служит реализация норм «правового ограничения» и «правового запрета» при проявлении социальной активности в виртуальном пространстве как средств социального контроля. Эти аспекты социальных отношений также подлежат изучению в рамках цифровой социологии.

5. Следующая (пятая) исследуемая цифровой социологией группа опасностей и угроз, связанных с участием военнослужащих и членов их семей в социальных сетях, связана с потенциальной возможностью враждебного завладения частной информацией о субъектах военной деятельности иностранными спецслужбами, зарубежными антироссийски настроенными информационно-аналитическими центрами. Помимо этого, необдуманные действия военнослужащего по использованию интернет-ресурсов может привести к созданию условий проникновения противника через установленные каналы обмена информации к конфиденциальным военным сведениям (ресурсам). Степень опасности подобных деяний возрастает в случае, если военнослужащий в статусе участника социальных сетей предоставляет идентификационные компьютерные данные, к которым относятся личные пароли, установленные им логины, а также ID персонального компьютера – ноутбука, планшета в ходе исполнения военно-профессиональных задач, а также обращения к корпоративным закрытым данным.

ЗАКЛЮЧЕНИЕ

Социопроектная, преобразующая функция цифровой социологии в системе социального управления предполагает разработку концептуальных и социоинженерных решений по оптимизации практики участия военнослужащих и членов их семей в социальных сетях. Основные организационно-технологические мероприятия предотвращения негативного воздействия социальных сетей с целью обеспечения их эффективности должны быть объединены в современную институциональную систему цифровой грамотности и цифрового социального контроля.

Социальное проектирование развития этой системы в рамках цифровой социологии предполагает совершенствование следующих компонентов:

– работы по профилактике распространение военнослужащими и членами их семей излишней информации в Интернете;

– правового просвещения по проблемам цифровой безопасности;

– мониторинга социальных сетей на предмет выявления угроз утраты военной (государственной) тайны;

– законодательного расширения прав должностных воинских частей по проверке контактов пользователей Интернета;

– изучения социальной интернет-активности членов семей военнослужащих на предмет возможной утечки служебной информации.

Таким образом, цифровая социология расширяет объектно-предметную сферу своих исследований, включая в нее особенности социального влияния развития цифрового общества на различные страты общества, отдельные профессиональные группы. Достаточно перспективными темами для цифровой и военной социологии являются проблемы регулирования социальной активности военнослужащих и членов их семей в интернет-пространстве, социальных сетях и иных практиках, основанных на использовании цифровых платформ и технологий. При этом глубокое проникновение в проблему предполагает комплексное изучение возникающих при этом проблем в нормативно-правовом, социально-психологическом, организационно-управленческом и иных аспектах.

БИБЛИОГРАФИЯ

Мерцалова Т.А. (2015). Информационная открытость системы образования: вопросы эффективности государственной политики//Вопросы образования. № 2. С. 40–75.

Сергейчик А.Л (2009). Опыт правового регулирования режимов конфиденциальной информации в зарубежных странах и его использование в деятельности ФСИН России//Вестник Владимирского юридического института. № 3. С. 187–189.

Слипченко В.И. (2002). Войны шестого поколения: Оружие и военное искусство будущего. М.: Вече. 381 с.

Хайбулина Э.И. (2012). Информационная безопасность личности в виртуальном пространстве эпохи постмодерна//Известия ЮФУ. Технические науки. № 11. С. 159–164.

Юдина Е.Н. (2017). Социальные сети в зеркале социологии: монография / МПГУ, ИСГО, РАНХиГС, ИГСУ. М., Спутник+. 163 с.

REFERENCES

Khaibulina E.I. (2012) Information security of the individual in the virtual space of the postmodern era [Informatsionnaya bezopasnost' lichnosti v virtual'nom prostranstve epokhi postmoderna], *Izvestiya SFed.U. Engineering Sciences* [*Izvestiya YuFU Tekhnicheskie nauki*], no. 11, pp. 159–164.

Mertsalova T.A. (2015) Information openness of the education system: issues of efficiency of state policy [Informatsionnaya otkrytost' sistemy obrazovaniya: voprosy effektivnosti gosudarstvennoi politiki], *Educational Studies* [*Voprosy obrazovaniya*], no. 2, pp. 40–75.

Sergeichik A.L. (2009) Experience of legal regulation of confidential information regimes in foreign countries and its use in the activities of the Federal penitentiary service of Russia [Opyt pravovogo regulirovaniya rezhimov konfidentsial'noi informatsii v zarubezhnykh stranakh i ego ispol'zovanie v deyatel'nosti FSIN Rossii], *Bulletin of Vladimir Law Institute* [*Vestnik Vladimirskogo yuridicheskogo instituta*], no. 3, pp. 187–189.

Slipchenko V.I. (2002) *Wars of the sixth generation: Weapons and military art of the future* [*Voiny shestogo pokoleniya: Oruzhie i voennoe iskusstvo budushchego*], Veche, Moscow, Russia. [In Russian].

Yudina E.N. (2017) *Social networks in the mirror of sociology: monograph* [*Sotsial'nye seti v zerkale sotsiologii: monografiya*], MPSU, ISGO, Ranepa, MIGS, Sputnik+, Moscow, Russia. [In Russian].

TRANSLATION OF FRONT REFERENCES

[1] The Constitution of the Russian Federation (adopted by popular vote on December 12, 1993), Collection of legislation of the Russian Federation, No. 31, art. 4 398, dated on August 4, 2014. Available at: http://www.consultant.ru/document/cons_doc_LAW_28399/ (accessed 12.10.2019).

[2] National security strategy of the Russian Federation (approved by the Decree of the President of the Russian Federation dated on December 31, 2015, No. 683). Available at: http://www.consultant.ru/document/cons_doc_LAW_191669/ (accessed 12.10.2019).

[3] Gisnel' Zh. "The French army is introducing a code of conduct on social media". Available at: https://bit.ly/2URUUtX (accessed 02.09. 2019).

[4] Social Media Handbook (2013). Available at: http://www.nationalguard.mil (accessed 02.09.2019).