DOI: 10.18522/2070-1403-2021-87-4-80-88

ФИЛОСОФИЯ

(специальность: 09.00.11)

УДК 101

И.П. Скворцов

Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

г. Краснодар, Россия

igskvorcov@yandex.ru

А.С. Селиверстов

Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

г. Краснодар, Россия

as.seliverstov93@gmail.com.

С.А. Селиверстов

Южно-Уральский государственный гуманитарно-педагогический университет

г. Челябинск, Россия

seliverstovsa@gmail.com.

О ФОРМИРОВАНИИ КУЛЬТУРЫ ЛИЧНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЕННОСЛУЖАЩЕГО

[*Igor P. Skvortsov, Alexander S. Seliverstov, Sergey A. Seliverstov*

On the formation of a culture of personal information security of a military]

It is considered the issue of the relevance of the information security culture formation for a soldier's personality, which is understood as the degree of his information development, which implies the ability to satisfy his information needs with minimization of negative information and psychological impact. The criterion and indicators of information security culture of a soldier's personality, its components and conditions of formation are presented. The important role of the stability of values and value orientations, personal convictions, formed in the process of military-political work, is emphasized. The culture of information security of an individual is characterized by the development of values, traditions, language, symbols and rules for the functioning of the information sphere and their rootedness in the activities of a serviceman.

Key words: information, information security, information security culture, information security culture of a soldier's personality.

Актуальность исследования проблемы формирования культуры личной информационной безопасности военнослужащих обусловливается рядом обстоятельств.

Современная концепция «гибридной войны» подразумевает ведение войн смешанного типа, в которых сочетаются различные стратегии ведения боевых действий (применения ядерного, биологического, химического и информационного оружия) во всех пространствах, в том числе и информационной сфере.

В Военной доктрине Российской Федерации отмечается смещение военных опасностей и военных угроз в информационное пространство. Стало возможным использование информационных и коммуникационных технологий в военно-политических целях, а также деятельность по информационному воздействию на население, в первую очередь на молодых граждан страны, имеющая целью подрыв исторических, духовных и патриотических традиций в области защиты Отечества [3]. С ростом информатизации различных сфер жизни общества и увеличения числа точек доступа в открытую сеть «Интернет», растут и возможности негативного информационного воздействия на население и военнослужащих.

В Стратегии национальной безопасности Российской Федерации отмечается, что все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, так как некоторые страны стремятся использовать информационные и коммуникационные технологии для достижения геополитических целей [7].

В Доктрине информационной безопасности Российской Федерации кроме технических мер обеспечения информационной безопасности предлагаются среди прочих следующие организационные меры:

- развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;
- обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности [8].

Исходя из данных положений, можно согласиться с отечественными авторами в том, что в перечень основных путей совершенствования социального управления информационной безопасностью военнослужащих необходимо включать и формирование их информационной культуры в процессе информационного обмена [5].

В научной литературе понятие информационной безопасности личности исследуется достаточно активно. Нам представляется продуктивным определение информационной безопасности Г.Г. Гафарова и В.В. Смелянской, считающих, что информационная безопасность характеризуется отсутствием угрозы причинения вреда информации, которой владеет личность и угрозы нанесения вреда личности информацией [1]. Но факт отсутствия подобной угрозы, или минимального уровня ее воздействия, несомненно, связан с информационной культурой личности, степенью ее развития в том числе в аспекте культуры информационной безопасности.

Несомненно, что культура информационной безопасности не может анализироваться вне изучения ее содержательного аспекта, поэтому распространенной позицией является характеристика культуры личной информационной безопасности как совокупности информационного мировоззрения и системы знаний и умений, обеспечивающих целенаправленную самостоятельную деятельность по оптимальному удовлетворению индивидуальных информационных потребностей с использованием как традиционных информационных и коммуникационных технологий (ИКТ), так и автоматизированных ИКТ, на принципах защищенности личной информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб личности [6].

Как нам представляется, в сущностном плане культура личной информационной безопасности военнослужащего есть степень его информационного развития, подразумевающая способность удовлетворять свои информационные потребности с минимизацией негативного информационно-психологического воздействия на знания, ценности, убеждения, поведение военнослужащего. Негативное информационно-психологическое воздействие означает распространение информации, ведущей:

- к ослаблению чувства гордости за свою страну, за принадлежность к ее Вооруженным Силам, к подрыву убежденности военнослужащих в необходимости выполнять конституционный долг по защите своей Отчизны;
- к снижению морального духа, созданию обстановки неуверенности и беспокойства относительно своего будущего, будущего Вооруженных Сил и государства, ослаблению воли к проведению конструктивных реформ, а в военное время к вооруженному сопротивлению;

- к снижению боеспособности, то есть понижению служебной активности, к уклонению от военной службы, симуляции болезней, уклонению от выполнения приказов командиров, сомнениям в надежности вверенного оружия, подавлению воли, созданию искаженной картины боевых действий, боевой обстановки;
- неверному восприятию военнослужащим существующих угроз национальной безопасности, истинных планов и намерений вероятного противника, развитию обстановки благодушия;
- к расколу воинских коллективов по политическим, религиозным, этническим, служебным и другим факторам [4].

Исходя из объектного понимания безопасности как проявления способности объектов сохранять устойчивость при различных отрицательных влияниях, критерием развитой культуры личной информационной безопасности военнослужащего выступает его способность поддерживать целостность структуры личности, что определяет его готовность к решению поставленных перед ним задач.

К показателям культуры личной информационной безопасности военнослужащего можно отнести:

- развитость когнитивных качеств личности, богатство соответствующих знаний, критичность и самостоятельность мышления;
- устойчивость ценностей, установок и ценностных ориентаций личности;
- развитость навыков ориентации в информационном пространстве, поиска, отбора, анализа, хранения и использования информации в ее различных аспектах;
- согласованность когнитивного, аксиологического, эмоционально-чувственного, волевого, мотивационного контуров сознания и поведения и др.

Деятельность человека по преобразованию информационной сферы основана на общепризнанных ценностях, выражается через традиции, ценности, язык, символы, правила. В этом смысле культура информационной безопасности включает в себя ряд составляющих.

Традиции – сложившиеся исторически или сформированные в конкретном коллективе повторяющиеся нормы деятельности и поведения. Традиция постоянно анализировать возможные информационные угрозы и на основании этих знаний развивать модель своего поведения в информационной сфере должна непременно войти в привычку всех пользователей.

Ценность – важность, значимость, польза, полезность чего-либо. Все пользователи должны понимать необходимость обеспечения информационной безопасности, понимать, что негативные последствия от их действий могут нанести ущерб не только себе, но и Вооруженным Силам, государству в целом.

Язык – сложная знаковая система, естественно или искусственно созданная и соотносящая понятийное содержание и типовое звучание (написание). Инциденты информационной безопасности зачастую происходят из-за того, что специалистам в области информационной безопасности не удалось донести до пользователей необходимость строгого соблюдения правил в информационной сфере. Многие пользователя относятся к вопросам обеспечения информационной безопасности формально, не понимая их важность.

Символы – это схематичное, отвлеченное, многозначное отображение образа предмета, понятия или явления. В этой связи представляется важным формирование символов информационной безопасности, которые поддерживали бы и объединяли людей в стремлении обеспечения информационную безопасность.

Правила – требования для исполнения неких условий поведения всеми участниками какого-либо действия. Правила должны быть понятны всем субъектам информационной сферы, а в совокупности с созданием единого поля коммуникации, пользователи должны ощущать себя частью общего коллектива, в котором необходимость выполнять правила положительно влияет на всех.

Формирование культуры личной информационной безопасности имеет решающее значение для грамотного поведения пользователей в информационной сфере. Информационная сфера динамична, она постоянно меняется в зависимости от развития информационных технологий, соответствующим образом должна меняться, развиваться с течением времени, адаптироваться под современный мир и культура личной информационной безопасности.

Вооруженным Силам необходимо создать среду, в которой они могут безопасно использовать современные средства управления и связи, основанные на информационных технологиях и дополнительно повышать осведомленность военнослужащих об информационной сфере. В этой связи можно сформулировать некоторые методы повышения компетенции пользователей в вопросах информационной безопасности:

- погружение пользователей в реально возможные ситуации;
- разработка агитационных материалов и их распространение;
- непосредственное обучение пользователей, проведение обучающих игр.

Также формирование культуры личной информационной безопасности невозможно без реализации таких условий, как:

- определения краткой и всем понятной цели обеспечения информационной безопасности, которая применима ко всем сферам деятельности Вооруженных Сил;
- разработки простой и понятной политики информационной безопасности;
- введения четких дисциплинарных и административных мер к нарушителям политики информационной безопасности;
- постоянного доведения до всех военнослужащих анализа инцидентов информационной безопасности;
- разработки стратегии формирования культуры личной информационной безопасности у военнослужащих;
- проведения регулярной оценки состояния информационной безопасности технических средств и культуры информационной безопасности военнослужащих.

Опыт вооруженных конфликтов последнего десятилетия, а также практика оперативной подготовки войск и штабов позволяют констатировать, что в настоящее время в Вооруженных Силах Российской Федерации сложилась целостная система деятельности, призванная обеспечить эффективное сдерживание, предотвращение и разрешение конфликтов в информационном пространстве.

Обеспечение информационной безопасности, повышение боевой готовности Вооруженных Сил заключается в комплексном подходе к решению данного вопроса. Необходимо не только совершенствовать технические и программные средств защиты информации, но и формировать у личного состава культуру обращения с информацией, умение правильно её оценивать, знания возможных угроз, направленных на информацию или угроз, из нее исходящих, умение пользоваться средствами защиты информации, понимание личной ответственности за совершаемые действия в информационной сфере. Очень важно для военнослужащих осознавать, что уровень их информационной культуры безопасности имеет решающее значение для защи-

ты государства от информационных угроз. Развитие культуры личной информационной безопасности позволит сформировать у военнослужащих представления о том, что информационные угрозы реальны, и их ежедневные действия влияют на их нейтрализацию.

Эффективность противодействия негативному информационно-психологическому воздействию будет выше, если оно будет носить системный, комплексный характер и строиться с учетом всех его аспектов [2]. Ключевая роль при этом, как нам представляется, принадлежит развитости и устойчивости ценностей и ценностных ориентаций, убеждений личности. Отсюда вытекает важнейшая роль качеств патриотизма, понимания личной ответственности и примерности военнослужащего в выполнении воинского долга.

В заключение отметим, что информационную безопасность следует рассматривать прежде всего как сочетание следующих явлений: отсутствие опасностей и угроз; достаточная степень устойчивости к возникающим угрозам, определенный иммунитет, запас прочности тех или иных объектов. Культура информационной безопасности военнослужащего обеспечивает такое состояние его жизнедеятельности, которое гарантирует качественную определенность личности в параметрах надежности существования, устойчивости развития, способности к решению поставленных задач.

Л И Т Е Р А Т У Р А

1. *Баринов С.В.* О правовом определении понятия «информационная безопасность личности». – URL: https://cyberleninka.ru/article/n/o-pravovom-opredelenii-ponyatiya-informatsionnaya-bezopasnost-lichnosti (дата обращения 18.05.2021).
2. *Борский Н., Урсул В.* Информационная безопасность войск. – URL: https://voen-pravo.ru/komandirskaya-podgotovka/konspekty/voenno-politicheskaya-podgotovka/316/. (дата обращения 11.05.2021).
3. Военная доктрина Российской Федерации: Указ президента Российской Федерации от 25 декабря 2014 г. № 2976. – URL: https://base.garant.ru/70830556/ (дата обращения 28.04.2021).
4. *Колесников А.* Информационная безопасность войск и защита личного состава от негативного информационно-психологического воздействия – URL:

http://voenservice.ru/boevaya_podgotovka/ogp/informatsionnaya-bezopasnost-voysk-i-zaschita-lichnogo-sostava-ot-negativnogo-informatsionno-psihologicheskogo-vozdeystviya/. (дата обращения 20.05.2021).

5. *Мешков Е.* Новации в управлении информационной безопасностью военнослужащих Вооруженных Сил РФ // Власть. 2012. № 9. – URL: https://cyberleninka.ru/article/n/novatsii-v-upravlenii-informatsionnoy-bezopasnostyu-voennosluzhaschih-vooruzhennyh-sil-rf (дата обращения 18.05.2021).
6. *Миндзаева Э.В.* Разработка концепции информационной безопасности личности: информационный/когнитивный подходы. – URL: https://cyberleninka.ru/article/n/razrabotka-kontseptsii-informatsionnoy-bezopasnosti-lichnosti-informatsionnyy-kognitivnyy-podhody (дата обращения 18.05.2021).
7. О Стратегии национальной безопасности Российской федерации: Указ президента Российской Федерации от 31 декабря 2015 г. № 683. – URL: https://base.garant.ru/71296054/ (дата обращения 28.04.2021).
8. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646. – URL: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения 28.04.2021).

R E F E R E N C E S

1. *Barinov S.V.* On the legal definition of the concept of "personal information security". URL: https://cyberleninka.ru/article/n/o-pravovom-opredelenii-ponyatiya-informatsionnaya-bezopasnost-lichnosti (accessed 18.05.2021).
2. *Borsky N., Ursul V.* Information security of troops. URL: https://voen-pravo.ru/komandirskaya-podgotovka/konspekty/voenno-politicheskaya-podgotovka/316/. (accessed 11.05.2021).
3. Military doctrine of the Russian Federation: Decree of the President of the Russian Federation of December 25, 2014 No. 2976. URL: https://base.garant.ru/70830556/ (accessed 28.04.2021).
4. *Kolesnikov A*. Information security of troops and protection of personnel from negative information and psychological impact URL: http://voenservice.ru/boevaya_podgotovka/ogp/informatsionnaya-bezopasnost-voysk-i-za-

schita-lichnogo-sostava-ot -negativnogo-informatsionno-psihologicheskogo-vozdeystviya /. (accessed 20.05.2021).

5. *Meshkov E*. Innovations in information security management of military personnel of the RF Armed Forces // Power. 2012. No. 9. URL: https://cyberleninka.ru/article/n/novatsii-v-upravlenii-informatsionnoy-bezopasnostyu-voennosluzhaschih-vooruzhennyh-sil-rf (accessed 18.05.2021).
6. *Mindzaeva E.V.* Development of the concept of personal information security: informational / cognitive approaches. URL: https://cyberleninka.ru/article/n/razrabotka-kontseptsii-informatsionnoy-bezopasnosti-lichnosti-informatsionnyy-kognitivnyy-podhody (accessed 18.05.2021).
7. On the National Security Strategy of the Russian Federation: Decree of the President of the Russian Federation of December 31, 2015 No. 683. URL: https://base.garant.ru/71296054/ (accessed 28.04.2021).
8. On the approval of the Doctrine of information security of the Russian Federation: Decree of the President of the Russian Federation of December 5, 2016 No. 646. URL: https://www.garant.ru/products/ipo/prime/doc/71456224/ (accessed 28.04. 2021).

17 июня 2021 г.