АКТУАЛЬНОСТЬ ПОДГОТОВКИ ВОЕННОСЛУЖАЩИХ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК СОСТАВЛЯЮЩЕЙ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

DOI: 10.25629/HC.2020.09.06

Останина Е.А.[1,2], Самойлов А.В.[2]

[1]Московский авиационный институт (национальный исследовательский университет)
Москва, Россия

[2]Военная академия Ракетных войск стратегического назначения имени Петра Великого
Балашиха, Россия

Аннотация. В последнее десятилетие внимание к проблемам информационной безопасности получило широкое распространение во всем мире, в том числе и в Российской Федерации. Усилия, направленные на обеспечение информационной безопасности, стали неотъемлемой частью деятельности практически любого государства. В статье приведен анализ категории «информационная безопасность», отражено текущее состояние общей компетентности офицерских кадров в области информационной безопасности в одном из родов войск. Раскрыто ее место и роль в вооруженных силах и в системе национальной безопасности в целом. Рассмотрено происхождение феномена информационной безопасности, ее сущность и структура.

В этой связи поднимаются вопросы обеспечения информационной безопасности государства в целом и гаранта национальной безопасности – вооруженных сил. Главенствующей задачей является подготовка военнослужащего к действиям в условиях информационного воздействия и способность противодействия ему. Решение обозначенных в статье частных задач призвано способствовать формированию профессиональной компетентности офицерских кадров в области информационной безопасности.

Ключевые слова: национальная безопасность, информация, информационная безопасность, информационное воздействие, информационное противоборство, государство, общество, личность, военнослужащий, защита информации, направления подготовки, утечка информации, угрозы, методы и средства защиты, информационные технологии.

Концепция национальной безопасности Российской Федерации в числе фундаментальных интересов сегодняшней России называет ее национальные интересы в информационной сфере. Это свидетельствует о том, что реализация интересов данной сферы является непременным условием жизнеобеспечения нашей страны, а сама информационная безопасность – неотъемлемым компонентом национальной безопасности России [9].

Сегодня национальная безопасность представляет собой состояние общественных отношений, которое характеризуется защищенностью жизненно важных интересов личности, общества, государства от внешних и внутренних опасностей (угроз). Национальная безопасность, под которой чаще всего понимают безопасность национального или многонационального общества, страны представляет собой сложное многоаспектное, неоднозначное явление. Важнейшей составной частью национальной безопасности является информационная безопасность.

Распространение понятия «информационная безопасность» связано с упорным желанием общества и государства закрепить свои завоевания в деле достижения устойчивого поступательного развития, стабильности, с развитием права, демократических ценностей, с повышением внимания к личности, как к высшей социальной ценности. Немаловажным фактором повышения интереса к названной проблеме стало острое осознание огромной значимости информации в жизни общества, государства и отдельных его граждан. Сила слова известна давно, отдельные люди и целые народы не раз испытывали на себе как позитивное, так и негативное его воздействие. Обмен информацией, информационные отношения в человеческом обществе нередко приобретают характер, выражаясь современным языком, информационного противоборства [2].

Осознание силы информационного воздействия побуждало людей на протяжении всей истории человечества создавать информационно-идеологические системы – религиозные, национальные, культурные, образовательные – с целью обеспечения власти над умами и судьбами народов, над ресурсами стран и континентов.

Таким образом, изучая аспекты информационной безопасности, нельзя дистанцироваться от понятия национальная безопасность, которая достигается стабильной реализацией государством всех его функций. Отправной точкой определения национальной безопасности являются национальные интересы. Из их реализации вытекают приоритетные направления внутренней и внешней политики государства. Главная составляющая национального интереса – это неотъемлемый принцип самосохранения и развития государства, который выражается в его интересах в самых различных областях.

Исходя из того, что национальные интересы определены как совокупность внутренних и внешних потребностей в обеспечении защищенности и устойчивого развития личности, общества и государства [14], предполагается, что именно устойчивое развитие позволяет обеспечить сбалансированность интересов личности, общества и государства в различных сферах человеческой деятельности (экономической, внутриполитической, социальной, международной, информационной, военной и др.). Методы и средства реализации и защиты своей национальной безопасности определяются государством на основе своих национальных интересов [8].

Рассмотрим институты личности, общества и государства с точки зрения эффективности их функционирования:

безопасность государства должна обеспечиваться наличием эффективного механизма управления и координации деятельности политических сил и общественных групп, а также институтами защиты;

безопасность общества базируется на наличии и качественном функционировании общественных институтов, норм, развитых форм общественного сознания, позволяющих реализовывать права и свободы всех групп населения и противостоять действиям, ведущим к расколу общества;

безопасность личности обеспечивается формированием комплекса правовых и нравственных норм, общественных институтов и организаций, которые позволили бы ей развивать и реализовывать способности и потребности.

Выделяют различные составляющие национальной безопасности: политическую, социальную, информационную, военную, экономическую, экологическую [15]. Отметим, что для функционирования государства важно сбалансированное обеспечение всех видов безопасности, так как они находятся в тесной взаимосвязи друг с другом.

Необходимо подчеркнуть, что если несколько десятилетий назад в понятие национальной безопасности вкладывался только смысл физической неприкосновенности государства, то есть военной безопасности, то сейчас это понятие существенным образом трансформируется. Содержание национальной безопасности эволюционирует с чисто военных аспектов в сторону расширения толкования самого понятия. Не теряя своего значения, военная безопасность перестает быть единственной заботой государства.

Информационная составляющая международного и внутреннего соперничества с древнейших времен играет важную роль в военном деле. Китайский полководец V века до н. э. Сунь-Цзы, автор одного из древнейших трактатов о военном искусстве, считал, что наивысшее мастерство полководца заключается в том, чтобы победить противника еще до начала открытого столкновения с ним. Первостепенное значение он придавал моральному духу армии, уровню подготовки войск, владению военными руководителями «ситуацией», разведке и т. д., словом всему тому, что сегодня мы связываем с информационной сферой. Вся последующая военная история не раз подтверждала правильность выводов китайского военного теоретика и практика. Свой вклад в развитие информационного компонента военной науки и практики внесли российские полководцы и флотоводцы, такие, как А.В. Суворов, М.И. Кутузов и многие другие.

В третьем тысячелетии значение информационного обеспечения боевых действий еще больше возросло. Эффективность использования электронных и информационных средств была продемонстрирована в двух компаниях США против Ирака, в антиталибской операции в Афганистане и некоторых других. Информационной борьбе в этих операциях отводилась одна из главных ролей.

Информация всегда была важным ресурсом жизнедеятельности отдельных людей, и социального развития в целом, однако ее значение далеко не всегда оценивалось по достоинству. Сегодня информация стала таким же необходимым атрибутом повседневной жизни общества, какими являются природные ресурсы, электроэнергия и финансы. Обострило ситуацию и утверждение права собственности на информацию.

Наконец, информация как таковая осознается все более важным началом бытия человека. Ряд российских ученых (М.А. Марков Г.Н. Дульнев, В.Д. Плыкин и некоторые другие) придают информации статус фундаментальной сущности природы, такой же, как пространство и время, а в отдельных случаях и определяющей их [12].

В настоящее время именно информация в различных ее проявлениях в первую очередь определяет сущность общества. И то, что наиболее развитые, передовые социальные системы сегодня называются информационными – одно из ярких тому подтверждений.

Самые значимые ресурсы жизнедеятельности общества во все времена вызывали к себе повышенный интерес, были причиной непримиримой борьбы, так как обладание ими приближало к вершинам политической власти. Сегодня конкуренция в информационной сфере становится все более напряженной. Возрастают масштабы и жесткость столкновений по поводу информации и с ее использованием. Прочно вошло в лексикон политиков и ученых понятие «информационная война». Участниками информационного противоборства в настоящее время оказались многие субъекты общественной жизни внутри каждого общества и едва ли не все субъекты международных отношений. По мнению российских и зарубежных ученых, информационная война, в отличие от ведения боевых действий вооруженными силами, идет постоянно [13].

Появление нетрадиционных вызовов в сфере безопасности усложняет само понятие «безопасность». Во-первых, становится сложнее определить, для кого представляет угрозу сложившаяся ситуация, конкретный случай. Когда же речь идет о чисто военном понимании безопасности, определить наличие угрозы и ее объекта можно быстрее и достовернее. Во-вторых, если раньше безопасность понимали в основном как национальную безопасность, теперь проблема безопасности выходит за рамки национальных границ. Безопасность становится многоаспектной, а значит, она становится глобальной [4]. Безопасности суверенного государства теперь может угрожать не только военное вторжение, но и события, происходящие далеко от его границ, на территории других суверенных государств.

Так или иначе, информационная сфера давно стала ареной международного соперничества, а информационные средства – орудием борьбы государств в достижении своих тактических и стратегических целей.

Концепция национальной безопасности России указывает на активизацию усилий ряда государств, направленных на ослабление позиций России в политической, экономической, военной и других областях. Такая ситуация оценивается в Концепции как попытки игнорировать интересы России при решении крупных проблем международных отношений, включая конфликтные ситуации [10]. Это может подорвать международную безопасность и стабильность, затормозить происходящие позитивные изменения в международных отношениях.

Адекватное представление о сущности информационной безопасности осложнено рядом проблем, способных повлечь за собой серьезные ошибки, привести к неверным оценкам в этой области. Иногда информационная безопасность рассматривается в отрыве от безопасности национальной, что во многих случаях не оправдано.

Отметим, что новое понимание безопасности скрывает в себе как новые возможности, так и новые опасности. Высказываются даже мнения, что опасность заключается в том, что под-

вергается сомнению традиционные представления о нерушимости государственного суверенитета [11]. Признание того, что какие-то события, происходящие за рубежом, затрагивают национальную безопасность данного государства, означает по сути дела, возможность как косвенного вмешательства во внутренние дела других стран, так и прямой военной интервенции. Таким образом, признание наличия нетрадиционных угроз безопасности означает полный или частичный отказ от принципов государственного суверенитета и невмешательства во внутренние дела других государств.

В настоящее время зависимость общества от информационных технологий и уязвимость существующих информационных объектов и структур обуславливают риск превращения информационных потоков и средств получения, хранения и передачи информации в потенциальный объект враждебного информационного воздействия [7]. С другой стороны, информация и информационные технологии способны стать средствами воздействия, дезорганизующий эффект от применения которых, может стать сопоставим с эффектом широкомасштабного применения военных средств воздействия.

В современных условиях всеобщей информатизации и развития информационных технологий резко возрастает значение обеспечения национальной безопасности государства в информационной сфере. Информация становится одним из главных рычагов в новом противоборстве между различными странами и социальными силами. Вот почему защита государственного информационного ресурса, который содержит в себе важную политическую, экономическую, научно-техническую и военную информацию, становится одним из приоритетов нашего времени.

Общеизвестно, что информация имеет непосредственное отношение к процессам управления и развития, обеспечивающим устойчивость и выживаемость любых систем. Поэтому понятие информационной безопасности непосредственно связано с устойчивостью любых систем, в том числе социальной, а поскольку отсутствие угроз сегодня недостижимый идеал для международного сообщества, то информационная безопасность определяется возможностями парировать, нейтрализовать опасные информационные воздействия. Исходя из этого, предлагается рассматривать обеспечение информационной безопасности как противодействие враждебному воздействию на государство, общество, граждан и важнейшие информационные системы, а также использованию последних во враждебных и в преступных целях [12].

Глобальные изменения, охватившие современный мир, отчетливо проявляются во всех сферах. Происходит интеграция и трансформация наук, информационных, социальных и технологических, управленческих процессов, резко усиливается их влияние на общественное и индивидуальное сознание.

Включение информационной составляющей в структуру понятия безопасность обусловлено тем, что в современных условиях работа с информацией становится приоритетной во всех сферах функционирования государства, общества и производства. Она пронизывает все сферы и существенным образом трансформирует их. Следовательно, ее защита становится необходимым условием для нормального развития и функционирования общества.

Ввиду достаточной сложности современных информационных технологий и критической зависимости от них человека представляется исключительно важным обеспечить безопасность его взаимодействия с информационной инфраструктурой, повысить его грамотность в вопросах информационной безопасности особенно в условиях преднамеренного информационного воздействия [6].

Следует отметить, что в настоящее время порой не учитывается сложность системы проблем информационной безопасности, в которой можно выделить как минимум два уровня: физический, который в большей степени связан с техническими средствами распространения, хранения, интерпретации информации, и содержательный, отражающий качественную, сущностную сторону вопроса. Если первый в большей степени относится к материальной сфере общества, то второй – к духовной. На самом деле, можно говорить о технологической, организационной и других сторонах данной проблемы. Вместо этого ее иногда сводят лишь к одному

из вопросов; например, довольно часто повышенное внимание уделяется технической стороне проблемы в ущерб остальным ее составляющим.

Далеко не полное перечисление проблем рассматриваемой области указывает на то, что информационная безопасность – сложный комплекс социальных явлений, все аспекты которых играют важную роль в укреплении основ российского общества, обеспечении его устойчивого развития.

Следует заметить, что информационный рост сделал социальную обстановку более ранимой и взрывоопасной, и информационные ресурсы и технологии могут быть использованы как в созидательных и прогрессивных целях, так и в деструктивных. Доступность и концентрация информации в наше время обуславливает возможность ее применения в целях дестабилизации общества.

Таким образом, безопасность, в том числе и как информационное состояние общества, понятие относительное. Поэтому вследствие высокого динамизма процессов социальной среды и многочисленности факторов, действующих в обществе, абсолютного достижения поставленных целей по обеспечению безопасности в данной сфере, чаще всего, не будет. Однако информационную безопасность можно считать обеспеченной, а цели, поставленные в ходе деятельности в этой сфере, достигнутыми, если основное негативное воздействие угроз информационной сферы на личность, общество и государство нейтрализовано, а изучение угроз информационного характера является одним из компонентов деятельности по обеспечению информационной безопасности.

В этой связи целесообразно обратить особое внимание на подготовку военнослужащих в области информационной безопасности. Это обусловлено тем, что в соперничестве и противоборстве государств в мире и в реализации политических планов произошло явное смещение воздействия с открытых силовых (экономических, дипломатических, военных) методов и средств на скрытые, не силовые, а именно информационные методы и средства. Особо отметим, что эта трансформация не ведет к ослаблению борьбы, к меньшей ожесточенности и решительности, а наоборот, под прикрытием риторики о переходе к ненасильственному миру борьба только обостряется [1]. Не акцентируя внимание на техническом аспекте данного вопроса, следует обратить особое внимание на необходимость систематизации, обобщения и формирования подготовки специалиста (военнослужащего) в целом. Следует отметить, что, педагогика, как наука, основываясь на дидактических принципах и методах обучения может, с учетом инновационных технологий, внести весомый вклад в повышение качества такой подготовки.

В содержании военных действий в традиционном их толковании растет удельный вес и значимость информационного противодействия. Информационный прессинг военнослужащих, и населения в целом, может провоцировать растерянность, дезориентацию и даже панику. Превосходство в эфире теперь является непременным условием победы в воздушном, морском и даже сухопутном бою (сражении, операции). Проведение же информационного анализа многовариантных утечек информации, как правило, ведет к неоспоримому преимуществу стороны агрессора. Изучение вопросов информационной безопасности, определение потенциальных угроз и уязвимостей в информационной сфере является в настоящее время для военнослужащих актуальным и сверхважным.

Предлагается рассмотреть более детально вопрос формирования профессиональной компетентности офицерских кадров в области информационной безопасности на уровне отдельного рода войск для понимания состояния проблемы на сегодняшний день в Вооруженных Силах Российской Федерации.

В связи с чем был проведен анализ квалификационных требований к уровню подготовки и минимуму содержания дополнительных профессиональных программ повышения квалификации всех направлений подготовки офицерских кадров, который показал недостаточность формируемых профессиональных компетенций в области информационной безопасности. В результате была рассмотрена возможность создания системы непрерывной подготовки офицерских кадров в области информационной безопасности.

Рассматривая общую статистику утечки информации по данным агентства InfoWatch 2017-2018 года количественный рост утечки конфиденциальной информации составил 12 %, внешние атаки только за 1 полугодие 2018 года стали причиной 35,5% утечек данных, в то время как 64,5% произошли под воздействием внутреннего нарушителя. В 53,5% случаев виновными в утечке информации оказались штатные сотрудники, причем в более чем 2% случаев ими оказались высшие руководители.

По данным того же агентства распределение утечек по типам данных за первые кварталы 2017 и 2018 годов соответственно (рис. 1). Распределение внутренних утечек по характеру умысла за эти же периоды (рис. 2). Распределение по возможным каналам утечек (рис. 3).

Рисунок 1 – Распределение утечек по типам данных

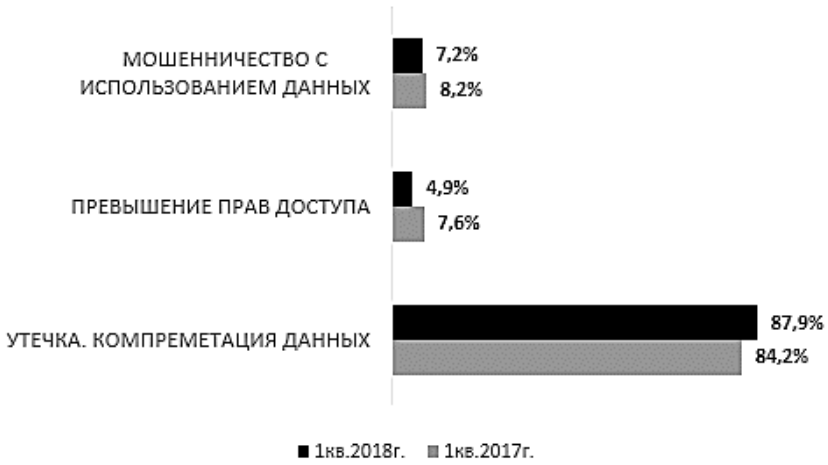

Рисунок 2 – Распределение внутренних утечек по характеру умысла

Рисунок 3 – Каналы утечки

Распределение числа утечек и объема скомпрометированных данных по данным за первые кварталы 2017 и 2018 годов составляет для государственного сектора 75,7% и 79,7% соответственно.

Доля умышленных утечек данных от общего числа утечек данных по отраслям в 2018 году представлена на графике (рис. 4).

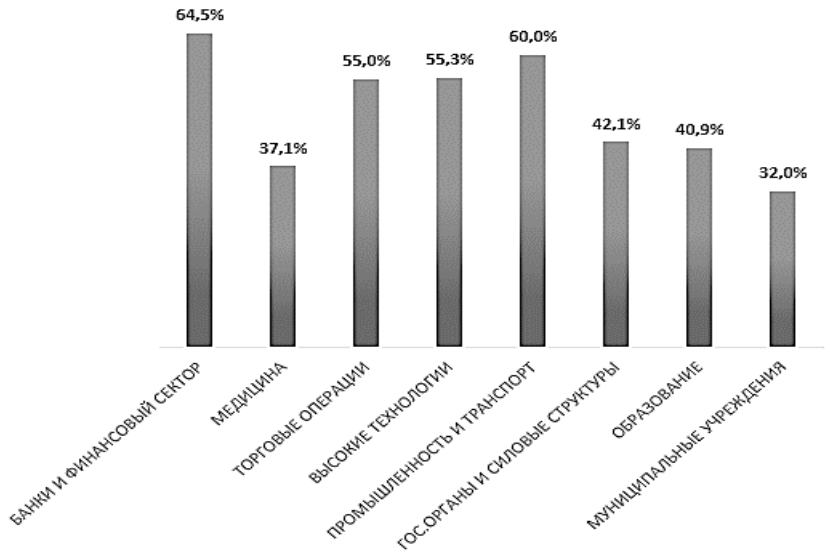

Рисунок 4 – Доля умышленных утечек данных от общего числа уточек данных по отраслям

Изученная статистика инцидентов и нарушений в информационной сфере за период 2018 г. – I-й квартал 2020 года, представленная, как по данным центра мониторинга информационной безопасности Российской Федерации, так и в отчетных данных органов военного управления подтверждают рост числа правонарушений и других инцидентов в информационной сфере.

Проведенный опрос, проходящих переподготовку военнослужащих, также показывает необходимость сосредоточения усилий по усовершенствованию подготовки в области информационной безопасности. Сами респонденты по данным личной оценки своего уровня при использовании информационных технологий отметили недостаточность подготовки (рис. 5, 6).

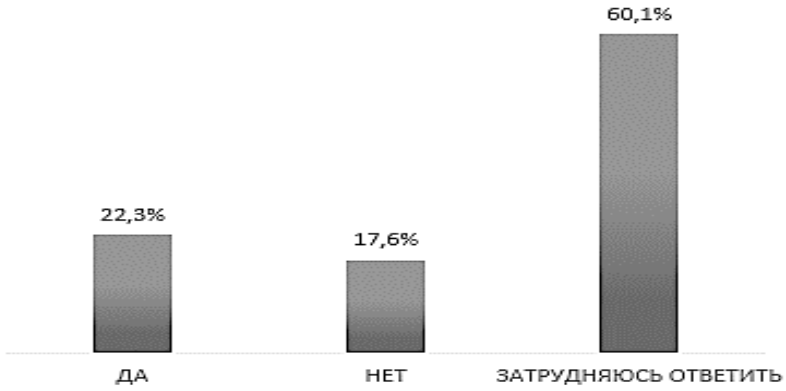

Рисунок 5 – Недостаточность знаний в области информационной безопасности при использовании информационных технологий (по субъективной оценке опрашиваемого)

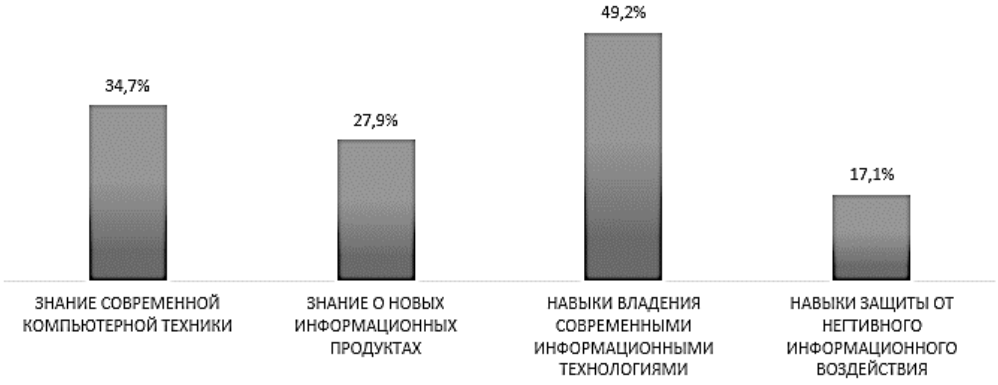

Рисунок 6 – Недостаточность знаний и навыков в области информационной безопасности (по субъективной оценке опрашиваемого)

Данные объективной оценки, ввиду ограниченности доступа к таковым, в данной статье не приведены.

Необходимо отметить, что некоторые затруднения в ответах респондентов, личное мнение о недостаточности подготовки в области информационной безопасности и проведенная оценка позволяют сделать вывод о целесообразности организации дополнительной подготовки военнослужащих. Также при проведении опроса было отмечено, что уровень подготовки руководящих кадров оказался выше.

По мере развития и активизации средств массовой информации, информационной техники и технологий противодействие в информационной сфере все чаще используются государствами для достижения политических целей. Изменяется характер вооруженного противостояния. И в мирное, в традиционном понимании, время происходит постоянное информационное

противоборство, о чем свидетельствует информационная борьба, происходящая в компьютерных сетях [5]. Обмен информационными воздействиями становится все опаснее и глобальнее, поскольку их эффективность растет из года в год, а выявлять источники таких воздействий крайне трудно. В нынешних условиях следует учитывать невозможность рассмотрения личности офицера в отрыве от семьи, друзей и близких. В этой связи, представляется актуальным изучение вопросов реализации воздействий как злоумышленных, направленных на получение информации и дестабилизирующее разрушающее воздействие на личность, так и разъяснительно-позитивных, дозированных, направленных на окружение с целью нормализации обстановки, предотвращения неумышленного нарушения информационной безопасности. Отметим, что во многом этому будет способствовать овладения соответствующими знаниями, умениями и навыками не только в области психологии и социальной инженерии, но и информационной безопасности в части работы в глобальной сети и осуществлении инфокоммуникации.

Таким образом, военнослужащие, являясь активными участниками и потребителями как официальных новостных информационных сообщений, так и прочих источников, должны иметь определенный запас актуальных знаний в области информационной безопасности как в части ее воздействия на человека, так и в части предотвращения возможных информационных утечек как лично, так и в кругу своего общения.

Комплексная система защиты информации – это совокупность организационно-правовых и инженерно-технических мероприятий, направленных на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа [3].

Основными задачами, решаемыми посредством организации комплексной системы защиты информации, являются: управление доступом пользователей к ресурсам с целью исключения неправомерного случайного или умышленного вмешательства в работу системы и несанкционированного (например, с превышением предоставленных полномочий) доступа к ее информационным, программным и аппаратным ресурсам со стороны персонала или посторонних лиц; защита данных, передаваемых по каналам связи; регистрация, сбор, хранение, обработка и предоставление сведений обо всех событиях, происходящих в системе и имеющих отношение к ее безопасности; контроль работы пользователей системы и оперативное оповещение о попытках несанкционированного доступа к ее ресурсам; контроль и поддержание целостности критичных ресурсов системы защиты и среды исполнения прикладных программ; обеспечение замкнутой среды проверенного программного обеспечения с целью защиты от внедрения в систему потенциально опасных программ и распространения компьютерных вирусов; управление средствами системы защиты [3].

В связи с вышесказанным, целесообразно было бы полагать, что в рамках подготовки, переподготовки и повышения квалификации военнослужащих целесообразно уделить внимание следующим направлениям:

правового регулирования защиты информации в Российской Федерации, включающее вопросы обозначения актуальности проблемы обеспечения безопасности информации, организационно-правовых основ обеспечения защиты информации в РФ, деятельности государственной системы защиты информации, законодательной базы обеспечения информационной безопасности, лицензирования деятельности по технической защите конфиденциальной информации, ответственности за правонарушения в области защиты информации;

комплексной системы защиты информации в организации, содержащее организацию и внедрение комплексной системы защиты информации, факторы, воздействующие на защищаемую информацию, методы и способы защиты конфиденциальной информации и информации, содержащей государственную тайну, угрозы безопасности информации, уязвимости систем;

защиты информации от утечки по техническим каналам, включающее вопросы изучения основных видов утечек информации, основ организации технической защиты информации в ВС РФ, классификации технических каналов утечки информации, мероприятий и средств защиты информации от утечки по техническим каналам на объектах информатизации, оценки эффективности методов и средств технической защиты информации;

защиты информации от несанкционированного доступа с изучением возможных угроз безопасности информации в случае несанкционированного доступа к ней, защиты информации от несанкционированного доступа и от программно-математических воздействий, построения системы защиты информационной системы от несанкционированного доступа;

криптографической защиты информации с точки зрения теоретических основ криптографических методов защиты информации и защиты автоматизированных систем организации с использованием средств криптографической защиты;

психологической защиты военнослужащего от информационного воздействия, включая критическую оценку информационных потоков средств массовой информации.

Стоит оговориться, что данные направления являются системообразующими для подготовки отдельных категорий военнослужащих, но авторами предлагается рассматривать основы данных направлений в совокупности именно для формирования профессиональной компетентности всех категорий военнослужащих в области информационной безопасности. Причем такая подготовка ни в коем случае не должна ограничиваться подготовкой в военном вузе, а должна органично продолжиться в войсках. В тоже время коррективы могут быть внесены в программы дополнительного профессионального образования в военных вузах и в планы подготовки в периодах обучения в войсках с учетом современных вызовов и угроз в сфере информационной безопасности.

Выводы

Таким образом, в настоящее время информационная безопасность проявляется не только как самостоятельный вид безопасности, но и как аспект, срез экономической, политической, научно-технической, военной, духовно-культурной безопасности.

Она является приоритетным направлением национальной безопасности, и в условиях общемировой интеграции необходимо осознание всех потенциальных угроз. Обеспечение информационной безопасности должно занимать приоритетное место в политике (в том числе и военной) практически каждого государства мирового сообщества. В этой связи целесообразно введение в военных образовательных организациях на всех уровнях военной подготовки как целых дисциплин, так и отдельных разделов по информационной безопасности. Особо следует подчеркнуть актуальность регулярного обновления данных курсов в связи с появлением новых информационных угроз, совершенствованием техники и технологий и выявлением все новых их уязвимостей. Достаточный уровень информационной грамотности военнослужащих в данных вопросах будет способствовать безопасности нашего общества и государства в целом.

Заключение

Организация системы подготовки военных кадров в области информационной безопасности, независимо от профиля подготовки, на сегодняшний день является достаточно актуальной задачей. Ее реализация призвана повысить уровень защищенности личности, общества и государства от внутренних и внешних информационных угроз, повысить обороноспособность и безопасность государства.

Библиография

1. Акимов В.А. Безопасность России. Национальная и международная безопасность. – М.: Знание, 2012. – 497 с.

2. Анненков В.И. Безопасность и противоборство в информационной сфере. – М.: РУСАВИА, 2010. – 447 с.

3. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации. – СПб: НИУ ИТМО, 2011. – 112 с.

4. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова, – Ст. Оскол: ТНТ, 2017. – 384 с.

5. Грушо А.А. Теоретические основы компьютерной безопасности. – М.: Academia, 2016. – 448 с.

6. Ефимова Н.С. Основы психологической безопасности. – М.: Форум, 2018. – 286 с.

7. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 – Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская, – М.: ГЛТ, 2017. – 536 с.

8. Зеленков М.Ю. Основы теории национальной безопасности. – М.: Юнити, 2017. – 384 с.

9. Кушников В.А. Модель для оценки состояния национальной безопасности России на основе теории системной динамики: моногр. – М.: Синергия, 2017. – 964 с.

10. Литвинов В.А. Основы национальной безопасности России. – М.: Ленанд, 2018. – 320 с.

11. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – М.: ГЛТ, 2016. – 280 с.

12. Новиков В.К., Галушкин И.Б., Аксенов С.В. Информационная безопасность и защита информации. – М.: Горячая линия – Телеком, 2019.

13. Новиков В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации). – М.: Горячая линия – Телеком, 2015. – 176 с.

14. Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 31.12.2015 года № 683.

15. Цаликов Р.Х., Панков Н.А., Конашенков И.Е. Организация информационного обеспечения Вооруженных Сил Российской Федерации. – М.: Редакционно-издательский центр Министерства обороны Российской Федерации, 2018.

Останина Елена Анатольевна. E-mail: neka1818@mail.ru

Самойлов Александр Владимирович. E-mail: aleksandr.samojlov.84@mail.ru

THE RELEVANCE OF THE TRAINING OF MILITARY SERVANTS IN THE FIELD OF INFORMATION SECURITY AS A COMPONENT OF NATIONAL SECURITY OF THE STATE

DOI: 10.25629/HC.2020.09.06

Elena A. Ostanina[1,2], Alexander V. Samoilov[2]

[1]Moscow Aviation Institute (National Research University)

Moscow, Russia

[2]Military Academy of Strategic Missile Forces named after Peter the Great

Balashikha, Russia

Abstract. Over the past decade, attention to information security problems has become widespread throughout the world, including in the Russian Federation. Efforts to ensure information security have become an integral part of the activities of almost any state. The article provides an analysis of the category of "information security", reflects the current state of the general competence of officers in the field of information security in one of the military branches. Its place and role in the armed forces and in the national security system as a whole is revealed. The origin of the phenomenon of information security, its essence and structure is considered.

In this connection, questions are raised of ensuring the information security of the state strike as a whole and the guarantor of national security – the armed forces. The main task is to prepare a serviceman for action in conditions of informational impact and the ability to counter it. The solution of particular tasks indicated in the article is intended to contribute to the formation of professional competence of officer personnel in the field of information security.

Keywords: national security, information, information security, information impact, information warfare, state, society, personality, military man, information protection, training directions, information leakage, threats, methods and means of protection, information technology.

References

1. Akimov V.A. *Bezopasnost' Rossii. Natsional'naya i mezhdunarodnaya bezopasnost'* [The security of Russia. National and international security]. Moscow: Znanie, 2012. 497 p.

2. Annenkov V.I. *Bezopasnost' i protivoborstvo v informatsionnoi sfere* [Security and confrontation in the information sphere]. Moscow: RUSAVIA, 2010. 447 p.

3. Gatchin Yu.A., Klimova E.V. *Vvedenie v kompleksnuyu zashchitu ob"ektov informatizatsii* [Introduction to comprehensive protection of informatization objects]. Saint Petersburg: NIU ITMO, 2011. 112 p.

4. Gromov Yu.Yu., Drachev V.O., Ivanova O.G. *Informatsionnaya bezopasnost' i zashchita informatsii: Uchebnoe posobie* [Information Security and Information Protection: A Training Manual]. St. Oskol: TNT, 2017. 384 p.

5. Grusho A.A. *Teoreticheskie osnovy komp'yuternoi bezopasnosti* [Theoretical Foundations of Computer Security]. Moscow: Academia, 2016. 448 p.

6. Efimova N.S. *Osnovy psikhologicheskoi bezopasnosti* [Psychological Safety Basics]. Moscow: Forum, 2018. 286 p.

7. Zapechnikov S.V., Miloslavskaya N.G. *Informatsionnaya bezopasnost' otkrytykh sistem. V 2-kh t. T.1. Ugrozy, uyazvimosti, ataki i podkhody k zashchite* [Information security of open systems. In 2 vol. V.1 Threats, vulnerabilities, attacks and approaches to protection]. Moscow: GLT, 2017. 536 p.

8. Zelenkov M.Yu. *Osnovy teorii natsional'noi bezopasnosti* [Fundamentals of the theory of national security]. Moscow: Yuniti, 2017. 384 p.

9. Kushnikov V.A. *Model' dlya otsenki sostoyaniya natsional'noi bezopasnosti Rossii na osnove teorii sistemnoi dinamiki* [A model for assessing the state of national security of Russia based on the theory of system dynamics]. Moscow: Sinergiya, 2017. 964 p.

10. Litvinov V.A. *Osnovy natsional'noi bezopasnosti Rossii* [Fundamentals of Russian national security]. Moscow: Lenand, 2018. 320 p.

11. Malyuk A.A. Informatsionnaya bezopasnost': kontseptual'nye i metodologicheskie osnovy zashchity informatsii [Information security: conceptual and methodological foundations of information security]. Moscow: GLT, 2016. 280 p.

12. Novikov V.K., Galushkin I.B., Aksenov S.V. *Informatsionnaya bezopasnost' i zashchita informatsii* [Information security and information protection]. Moscow: Goryachaya liniya – Telekom, 2019.

13. Novikov V.K. *Organizatsionno-pravovye osnovy informatsionnoi bezopasnosti (zashchity informatsii). Yuridicheskaya otvetstvennost' za pravonarusheniya v oblasti informatsionnoi bezopasnosti (zashchity informatsii)* [Organizational and legal foundations of information security (protection of information). Legal liability for offenses in the field of information security (information protection)]. Moscow: Goryachaya liniya – Telekom, 2015. 176 p.

14. National Security Strategy of the Russian Federation. Approved by Decree of the President of the Russian Federation of December 31, 2015 No. 683.

15. Tsalikov R.Kh., Pankov N.A., Konashenkov I.E. *Organizatsiya informatsionnogo obespecheniya Vooruzhennykh Sil Rossiiskoi Federatsii* [Organization of information support for the Armed Forces of the Russian Federation]. Moscow: Editorial and Publishing Center of the Ministry of Defense of the Russian Federation, 2018.

Ostanina Elena Anatolyevna. E-mail: neka1818@mail.ru

Samoilov Alexander Vladimirovich. E-mail: aleksandr.samojlov.84@mail.ru