I International Scientific Practical Conference of graduate and postgraduate students, lecturers
«APPLIED ISSUES OF EXACT SCIENCES»
19-20October 2018, Armavir

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ВООРУЖЕННЫХ СИЛАХ РОССИЙСКОЙ ФЕДЕРАЦИИ

В.Л. Гашевский[1)], Ю.В. Назаров[2)], В.Л. Артемук[3)]

1) преподаватель 4-го авиационного факультета (дальней и военно-транспортной авиации) (г. Балашов) Краснодарского высшего военного училища лётчиков им. Героя Советского Союза А.К. Серова, г. Балашов, Россия, GashekVL@mail.ru;
2) старший преподаватель 4-го авиационного факультета (дальней и военно-транспортной авиации) (г. Балашов) Краснодарского высшего военного училища лётчиков им. Героя Советского Союза А.К. Серова, г. Балашов, Россия;
3) преподаватель 4-го авиационного факультета (дальней и военно-транспортной авиации) (г. Балашов) Краснодарского высшего военного училища лётчиков им. Героя Советского Союза А.К. Серова, г. Балашов, Россия.

Аннотация: рассматривается проблемы информационной безопасности в Вооруженных силах РФ, методы защиты информации и некоторые меры по обеспечению информационной безопасности.

Ключевые слова: информационная безопасность, угрозы и меры защиты информации.

INFORMATION SECURITY IN THE ARMED FORCES OF THE RUSSIAN FEDERATION

Vladimir L. Gashevsky[1)], Yuri V. Nazarov[2)], Vladimir L. Artemuk[3)]

1) lecturer of 4 aviation faculty (long and military transport aviation) (Balashov), Krasnodar Air Force Institute for Pilots named after Hero of the Soviet Union A. K. Serov, Balashov, Russia, GashekVL@mail.ru
2) senior lecturer of 41 departments of tactics and all-war disciplines of 4 aviation faculty (long and military transport aviation) (Balashov), candidate of Biological Sciences, Krasnodar Air Force Institute for Pilots named after Hero of the Soviet Union A. K. Serov, Balashov, Russia.
3) lecturer of 41 departments of tactics and all-war disciplines of 4 aviation faculty (long and military transport aviation) (Balashov), Krasnodar Air Force Institute for Pilots named after Hero of the Soviet Union A. K. Serov, Balashov, Russia.

Annotation: the problems of information security in the Armed Forces of the Russian Federation, methods of information protection and some measures to ensure information security are considered.

Keywords: information security, threats and measures to protect information.

Высокие темпы формирования глобального информационного пространства и информатизация большинства государств в конце XX - начале XXI веков создали предпосылки для интенсивного использования информационной сферы при разрешении межгосударственных противоречий, что привело к обострению межгосударственного информационного противоборства на качественно новом уровне.

Вооруженные Силы РФ становятся объектом информационного воздействия со стороны вероятного противника. В этих условиях они должны обеспечивать на достаточном уровне собственную информационную безопасность, которая является залогом успешного решения задач по нейтрализации угроз в информационной сфере государства в целом.

В Указе Президента РФ «О концепции национальной безопасности Российской Федерации» от 10.01.2000 г. № 24 интересы России в информационной сфере впервые были упомянуты как составная часть национальной безопасности.

Но наиболее полно понятие информационной безопасности отражено в Доктрине информационной безопасности РФ от 09.09.2000 г. № Пр-1895, развивающей основные положения Концепции национальной безопасности РФ применительно к информационной сфере.

Информационная безопасность вооруженных сил как важнейшего государственного института является и гарантией безопасности самого государства. На смену войне горячего типа, предусматривающей прямые военные столкновения, приходит война гибридного характера, имеющая своей основной целью развитие гражданских войн и создание управляемого информационного хаоса на территории противника. Для этого используются все возможности – от хакерских атак на важнейшие системы жизнеобеспечения государства до целенаправленной работы СМИ.

Внутренние угрозы

Одним из основных источников угроз информационного характера является дестабилизация социальной и политической обстановки в местах дислокации воинских частей. Создание искусственно накаленной атмосферы, провокация конфликтов личного состава с местным населением, иногда даже беспорядки, вызванные направленным

информационным воздействием, становятся серьезными угрозами стабильности ситуации в военной части и в войсках в целом. Такие ситуации происходили и происходят на Кавказе, на российских базах, находящихся в странах СНГ, в других регионах. Противостоять им можно, только проводя целенаправленную психологическую и воспитательную работу с личным составом.

Важной угрозой является направленное воздействие на моральный дух войск путем фальсификации фактов военной истории, усиления социального напряжения, попытка задействовать личный состав в развитии политических конфликтов. Виновником возникновения таких угроз информационного характера наиболее часто становятся средства массовой информации, нацеленные на создание напряженной обстановки.

Иногда мерами подобного воздействия достигаются психологические срывы у военнослужащих, приводящие к воинским правонарушениям. Серьезной угрозой информационной безопасности армии может стать и распространение радикального исламизма. Военнослужащий, прошедший специальную психологическую обработку, относит себя к религиозной общине, и выполняет не приказы командования, а советы своих учителей. Такой боец становится серьезной угрозой информационной безопасности воинских частей, особенно находящихся в регионах с преимущественно мусульманским населением.

Технические угрозы информационного характера включают в себя системы управления и сохранности конфиденциальной информации, передаваемой по каналам военной связи. Виды технических угроз деятельности Вооруженных сил могут носить различный характер: от намеренного повреждения систем и похищения информации до халатности отдельных сотрудников. Мерами защиты в этом случае станут и повышение уровня защищенности систем автоматизированного управления, тщательный отбор личного состава и его обучение необходимым требованиям, связанным с защитой информации.

В рамках этого типа атак может быть рассмотрено и намеренное повреждение оборудования и линий связи, иногда возникающее и по вине личного состава, и по вине местного населения, и в результате направленной деятельности противника. Контроль над сохранностью воинского оборудования – одна из важнейших задач, стоящая перед ответственными сотрудниками войск. Особенно серьезными могут быть проблемы с информационными системами на объектах военно-космических войск, относящихся войскам ПВО, к ядерным силам. Нарушение систем управления из-за внедренного в программный продукт ложного кода часто приводит не только к финансовым потерям, но и к нарушению целостности системы безопасности страны. По одной из

версий, высказанных на госкомиссии, крушение аппарата «Фобос-Грунт» было вызвано именно вторжением в системы управления.

Серьезной проблемой на сегодняшний день является и недостаточная разработка нормативно-правовой базы, касающейся защиты информации. Большое количество явлений информационного пространства еще не было классифицировано и отражено в нормативных актах, в связи с чем затруднено применение мер ответственности за реализацию каких-либо действий или организацию деятельности, которая может нанести урон информационной безопасности вооруженных сил и военнослужащих.

Но эти направления развиваются, принимаются нормативно-правовые акты, законодательно регламентирующие допустимость применения той или иной техники иностранного производства, например, чипов, в оборудовании, которое поставляется в войска.

Внешние угрозы

Достаточно реальной угрозой становится использование новых видов информационного оружия, часть из которых направлена на выведение из строя информационных систем, а часть – на прямое психологическое воздействие на личный состав. При этом механизм действия такого оружия, по данным аналитиков, основан на применении ультразвука, электромагнитных полей, микроволн различного характера. Не исключено и использование медицинских и химических средств, которые помогут целенаправленно действовать на поведение военнослужащих в мирной и боевой обстановке. Такие средства ведения психологических операций могут быть применены в тех местах, где вооруженные силы России участвуют в текущих конфликтах.

В составе вооруженных сил стратегического противника или организаций мирового терроризма есть специальные подразделения информационно-психологического воздействия. Их деятельность изучается на уровне специализированных НИИ, и меры борьбы с новыми угрозами разрабатываются и активно внедряются в практику.

Часто применение целенаправленного информационного воздействия заранее тщательно подготавливается работой средств массовой информации. Серьезнейшей проблемой для безопасности становятся социальные сети, с помощью которых военнослужащие могут случайно выдать важную информацию. Одной из основных задач по защите безопасности государства должно стать выявление таких угроз и своевременное их устранение.

Меры по обеспечению информационной безопасности

Меры, которые могут быть применены в целях защиты информации и обеспечения безопасности, также делятся на две группы:

- защита информационных систем от повреждения и информации от утечки и перехвата;
- защита психики личного состава от намеренного информационно-психологического воздействия.

Эти меры должны приниматься в совокупности, опираясь на все новейшие научные разработки и программные продукты.

Первая группа мер:

- защита объектов дислокации войск и расположенных в них АСУ и элементов компьютерной техники от огневого поражения или иного намеренного выведения из строя;
- защита систем от удаленного проникновения в них противника, в частности с установлением программных продуктов, обеспечивающих полную защиту периметра от проникновений, например, DLP-систем и SIEM-систем;
- защита информации, носящей характер государственной или военной тайны, от утечек или намеренного похищения;
- радиоэлектронная защита;
- использование защищенных моделей компьютеров и программных средств, которые не могут быть повреждены заранее созданными проблемами в их кодах;
- развитие средств электронной разведки;
- использование социальных сетей для намеренного дезинформационного воздействия на противника;
- защита систем связи.

Ко второй группе мер относится:

- предохранение психики войск от намеренного психологического воздействия;
- корректировка информации, транслируемой потенциальным противником.

Для разработки и реализации комплекса этих мер необходимо создание отдельных подразделений, действующих в сфере информационной безопасности.

Дополнительно следует учитывать, что меры защиты военной информации проблематично применять при формировании документации на базе транспортных компаний, научных институтов, сервисных служб. Отсутствие должного контроля над поставщиками и подрядчиками приводит к тому, что в войска поставляется оборудование, которое допускает удаленный доступ со стороны потенциального противника. В ряде случаев использование таких устройств запрещено законодательно, но пока не все техническое оснащение армии было модернизировано.

Серьезная уязвимость систем АСУ армии возникает и из-за передачи информации закрытого характера по открытым линиям связи. Угрозы возникают и при распространении частными лицами случайно полученных ими сведений в социальных сетях. Такие риски блокируются только разъяснительной работой с населением, так как ситуации с возбуждением уголовных дел по статье «Государственная измена» за пост в Сети не являются достойной превентивной мерой.

Комплексный подход к обеспечению информационной безопасности Вооруженных сил и личного состава должен обеспечить укрепление обороноспособности России. Опираясь на Доктрину информационной безопасности, можно разрабатывать новые комплексные способы борьбы с нарастающими угрозами

Список использованных источников:

1. Поздняков А. Информационная безопасность страны и вооруженные силы: сущность, структура, актуальные проблемы обеспечения. Вестник МГУ, Серия 12- 2004. - №2

2. Организация информационно-психологической защиты войск (сил) (проект), ГУВР, 2003.

3. Цифровой спецназ Шойгу. Чему противостоят Войска информационных операций? Еженедельник «Аргументы и факты» №9 01/03/2017