Единственный способ завоевания и сохранения авторитета среди подчиненных – постоянное и непрерывное подтверждение своих лучших качеств, результатами своей практической управленческой и другой деятельности.

Но авторитет можно и потерять попытками подавления подчиненных силой командирского положения, отсутствием взаимосвязи между командиром и подчиненными, высокомерием, педантизмом, резонерством, беспринципностью, снижением требований и др.

Авторитет командира является динамическим явлением. Он может укрепляться, повышаться, и в определенных ситуациях снижаться или утрачивать всю свою силу. Правдой является то, что утраченный авторитет сложнее вернуть, чем укрепить или повысить сложившийся.

Авторитет является важной чертой командира, которую нужно усиливать и поддерживать, иначе военно-социальное управление не будет столь качественным и полноценным.

ЛИТЕРАТУРА

1. Авторитет и доверия в структуре военного управления и военной мысли. Э.Б. Осипенко, А.В. Сальников, М.В. Барановский // Социология. 2020, № 6. С. 76-83.

2. Мерецков К.А. На службе народу. Страницы воспоминаний. М.: Политиздат, 1970. С. 122.

УДК 356.11

Студ. И.С. Супрунович
Науч. рук. преп. С.М. Савицкий (военная кафедра, БГТУ)

ПРИМЕНЕНИЕ СРЕДСТВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ССО

Гибридные способы ведения современных войн делают крайне важным обеспечение информационной безопасности вооруженных сил. 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.

Создание глобального пространства существенно усилило угрозы применения стратегическим противником или мировым

терроризмом мер информационного характера как при разворачивании отдельных военно-политических операций, так и для развития своего стратегического потенциала в целом.

Защиту от угроз подобного характера требуют и сами вооруженные силы, и их личный состав, работа с которым средствами гибридной войны ведется в первую очередь.

Повышается и ценность информации. Степень ее защиты от преступных посягательств становится все выше, а возможностей по ее получению – все больше. Умение правильно управлять информационными массивами и их использованием становится важнейшей задачей, стоящей перед военнослужащими.

Информационная безопасность вооруженных сил как важнейшего государственного института является и гарантией безопасности самого государства. Защита информационных ресурсов войск должна стать приоритетной задачей для специалистов по безопасности. Чтобы нейтрализовать угрозы наилучшим способом, необходимо их выявить и классифицировать по происхождению, характеру воздействия, степени опасности. Специалисты подразделяют виды источников угроз на две группы: внутренние и внешние.

Иногда в одном явлении можно обнаружить и внешние, и внутренние источники угроз. Это может происходить в случае, когда направленное воздействие, имеющее внешний источник происхождения, транслируется через операторов, находящихся в стране. Сегодня такие подразделения имеют в своем распоряжении серьезные электронные средства распространения информационных потоков, иногда они привлекают к работе и профессиональных хакеров, и волонтеров из числа граждан.

На практике обеспечение информационной безопасности фирмы осуществляется с помощью следующих средств:

- моральных;
- правовых;
- организационных;
- физических;
- аппаратных;
- программных;
- технических;
- криптографических.

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, а также 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.

УДК 614.841

Студ. И.А. Старовойтов
Науч. рук. нач. кафедры полковник А.В. Зеленкевич
(военная кафедра, БГТУ)

ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ В ПРОЦЕССЕ ВОЕННО-ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВОЙСК

В современном мире вопросы экологической безопасности становятся все более актуальными. Это касается и военной сферы, где