

БЕЗОПАСНОСТИ СВЯЗИ КАК КЛЮЧЕВОЙ АСПЕКТ ИНФОРМАЦИОННОЙ УСТОЙЧИВОСТИ ВОЙСК СВЯЗИ

Сацута К.В., Семёнов Е.В.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Сидоров С.В.

Аннотация. Данный тезис показывает важность безопасности связи в войсках связи.

В современном мире, где доминирующую роль в управлении и ведении боевых действий играет информация, безопасность связи в войсках связи приобретает первостепенное значение. Надёжная и устойчивая система связи становится краеугольным камнем эффективного функционирования всех звеньев военного управления. Малейшая уязвимость в канале передачи данных может обернуться масштабными последствиями — от срыва координации до утраты инициативы на оперативном или стратегическом уровне. Именно поэтому защита информации, её сохранность и недопустимость утечки являются приоритетом при организации систем связи в вооружённых силах.

Современные конфликты всё чаще сопровождаются активным применением средств радиоэлектронной борьбы, кибервоздействий и других форм информационного давления. На этом фоне особую значимость приобретает не только разработка, но и своевременное внедрение современных технологических решений, позволяющих обеспечить максимальную защищённость каналов связи от внешнего вмешательства. Технологии, используемые в сфере инфокоммуникаций, меняются с поразительной скоростью, а вместе с ними совершенствуются и методы информационного воздействия со стороны вероятного противника. Это порождает необходимость постоянного перевооружения технической базы войск связи и поддержания её в полной боевой готовности. Только находясь на передовой технического прогресса, можно гарантировать надёжную информационную устойчивость в условиях высокотехнологичного противоборства.

Поддержание технических средств связи в актуальном и боеспособном состоянии — это не разовая задача, а долгосрочный, планомерный и ресурсозатратный процесс, который должен быть интегрирован в систему оборонного планирования. Устаревшие или физически изношенные средства связи становятся слабым звеном, независимо от уровня подготовки личного состава. Именно поэтому важна не только защита информации как таковая, но и комплексное развитие всей системы связи — от канальных и абонентских устройств до средств автоматизированного управления, встроенных в единую информационную структуру войск.

Нельзя не отметить и глобальный контекст — проблема информационной безопасности и защиты каналов связи не ограничивается национальными рамками. Это международный вызов, находящийся в центре внимания как государств, так и крупных транснациональных акторов. Постоянное появление новых векторов угроз, таких как искусственный интеллект в сфере кибершпионажа, автоматизация атакующих алгоритмов и развитие нейросетевых методов анализа данных, делают сферу информационной безопасности одной из самых динамичных и наукоёмких. Игнорировать эти процессы — значит осознанно уступать инициативу и подвергать риску устойчивость национальной обороны.

Особую роль в системе обеспечения безопасности связи играет подготовка квалифицированных специалистов. Эффективная защита каналов передачи информации невозможна без наличия кадров, способных оперативно реагировать на нестандартные ситуации, разрабатывать и внедрять инновационные решения, а также грамотно управлять существующими средствами защиты. Такие задачи требуют глубоких знаний, системного мышления, постоянного саморазвития и, что особенно важно, профильного высшего образования. Только на его основе возможно сформировать специалистов, обладающих не только техническими, но и аналитическими компетенциями, способными быть на шаг впереди потенциальных угроз.

Таким образом, обеспечение безопасности связи в войсках связи — это неотъемлемая часть общей стратегии обороны, требующая скоординированных усилий в научной, технической и кадровой сферах. Это тема, не теряющая своей актуальности вне зависимости от политической конъюнктуры или внешних обстоятельств. Это вечно развивающееся направление, следить за которым — значит сохранять стратегическую устойчивость, обеспечивать победу в информационном противоборстве и гарантировать безопасность государства в условиях стремительно меняющейся реальности.