

АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВИТИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И УСЛУГ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Бардашевич А.В.

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

Титков Е.В. – начальник физической подготовки и спорта кафедры ТиОП

Аннотация. Вооруженные Силы играют ключевую роль в обеспечении безопасности и обороноспособности страны, а эффективное использование инфокоммуникационных систем и услуг становится важной частью их деятельности. Военные операции и задачи в современном мире требуют высокоскоростной передачи информации, своевременного обмена данными и согласования действий между различными воинскими подразделениями. Инфокоммуникационные системы и услуги позволяют обеспечить связь между командованием и подразделениями на поле боя, а также между различными уровнями управления.

Современное информационное общество требует непрерывного развития и совершенствования инфокоммуникационных систем и услуг. Вооруженные Силы Республики Беларусь в этом отношении не являются исключением. Развитие инфокоммуникационных систем и услуг в войсках связи играет важную роль в обеспечении эффективной коммуникации, оперативного информационного обмена и поддержания готовности к выполнению задач национальной безопасности.

Первым вопросом является модернизация инфраструктуры связи. С развитием технологий и увеличением объема передаваемой информации возникает необходимость в постоянном совершенствовании инфраструктуры связи. Это включает в себя обновление и модернизацию сетей связи, внедрение более быстрых и надежных каналов передачи данных, а также создание резервных систем связи для обеспечения непрерывности коммуникаций в случае аварий или военных действий. Модернизация инфраструктуры связи позволит Вооруженным Силам Республики Беларусь оперативно реагировать на изменяющиеся условия и эффективно выполнять свои задачи.

Вторым важным вопросом является развитие кибербезопасности. В условиях всеобщей цифровизации и повсеместного использования информационных технологий, вопросы кибербезопасности становятся все более актуальными. Вооруженные Силы Республики Беларусь должны быть готовы к защите своих информационных систем от кибератак, утечки конфиденциальной информации и других угроз. Развитие кибербезопасности в войсках связи включает в себя обучение персонала, внедрение современных технических средств защиты информации, а также разработку стратегий и политик в области кибербезопасности. Это позволит обеспечить конфиденциальность и целостность передаваемой информации, а также сохранить оперативность и надежность связи в военных условиях.

Третьим вопросом является развитие сетей связи нового поколения. Современные вооруженные силы нуждаются в сетях связи, способных обеспечивать высокоскоростной доступ к информации, передачу больших объемов данных и поддержку передовых технологий, таких как облачные вычисления и интернет вещей. Развитие сетей связи нового поколения позволит Вооруженным Силам Республики Беларусь эффективно использовать современные информационные технологии и обеспечивать оперативную коммуникацию и обмен данными как внутри военных структур, так и с внешними партнерами и союзниками. Это также способствует улучшению координации действий, принятию оперативных решений и повышению общей эффективности Вооруженных Сил.

Четвертым вопросом является развитие облачных технологий и цифровизация. Внедрение облачных технологий в войсках связи позволяет обеспечить гибкое хранение, обмен и обработку данных, а также улучшить доступность информации для сотрудников Вооруженных Сил Республики Беларусь в любой точке мира. Цифровизация процессов связи и управления позволяет автоматизировать рутинные операции, ускорить обработку информации и снизить вероятность ошибок. Развитие облачных технологий и цифровизация способствуют повышению оперативности и эффективности деятельности Вооруженных Сил.

Развитие инфокоммуникационных систем в войсках связи Вооруженных Сил Республики Беларусь сопровождается определенными рисками, которые могут повлиять на их функциональность, безопасность и эффективность. Некоторые из этих рисков включают в себя:

1 Кибербезопасность: с развитием сетей связи и передачи данных возрастает вероятность кибератак со стороны злоумышленников и других государств. Атаки могут быть направлены на взлом систем связи, кражу или повреждение данных, а также нарушение работы инфраструктуры связи. Недостаточная защита информационных систем и уязвимости в программном обеспечении могут привести к серьезным последствиям, включая утечку конфиденциальных данных или нарушение важных коммуникаций.

2 Технические сбои: развитие сложных инфокоммуникационных систем может привести к появлению новых технических проблем и сбоев. Неполадки в оборудовании, программных сбоях или неправильной настройке систем могут привести к прерыванию связи, потере данных или недоступности важных сервисов. Такие сбои могут серьезно повлиять на боеспособность и оперативность военных действий.

3 Зависимость от внешних поставщиков: развитие инфокоммуникационных систем может привести к увеличению зависимости от внешних поставщиков оборудования, программного обеспечения и услуг связи. Неспособность или задержки со стороны поставщиков могут негативно сказаться на оперативности и доступности систем связи. Более того, зависимость от иностранных поставщиков может вызвать проблемы с безопасностью данных и возможностью несанкционированного доступа к ним.

4 Недостаточная подготовка персонала: развитие инфокоммуникационных систем требует высококвалифицированных специалистов, способных управлять и обслуживать сложное оборудование и программное обеспечение. Недостаточная подготовка и обучение персонала могут стать причиной неэффективного использования систем связи, ошибок в настройке или обслуживании, а также нарушений в области кибербезопасности.

5 Физические угрозы: инфокоммуникационные системы подвержены физическим угрозам, таким как природные катастрофы, технологические аварии или военные действия. Повреждение инфраструктуры связи или потеря доступа к электроэнергии может привести к прерыванию связи и недоступности систем.

Для снижения этих рисков необходимо уделять должное внимание кибербезопасности, проводить регулярные аудиты и испытания систем, обеспечивать надежность и резервирование оборудования, а также обеспечивать надлежащую защиту информации и обучение персонала по вопросам безопасности. Также важно разработать стратегии реагирования на возможные сбои и кибератаки, а также сотрудничать с надежными поставщиками оборудования и услуг связи.

Развитие инфокоммуникационных систем в войсках связи Вооруженных Сил Республики Беларусь будет иметь прямое влияние на обучение курсантов и требования к их подготовке.

С появлением новых технологий и систем связи обновленные программы обучения будут включать изучение новых технических навыков и знаний, необходимых для работы с современным оборудованием и программным обеспечением. Курсанты будут обучаться принципам работы с высокоскоростными сетями, цифровыми технологиями связи, кибербезопасности и другими смежными областями.

Развитие инфокоммуникационных систем потребует проведения практических упражнений и тренировок, чтобы курсанты могли получить практический опыт работы с современным оборудованием и программным обеспечением. Это может включать симуляции сетевых атак, решение проблем связи в реальном времени и выполнение задач с использованием новых технологий. С ростом угроз в области кибербезопасности обучение курсантов будет уделять большое внимание защите информации и предотвращению кибератак. Курсанты могут получить знания о современных методах аутентификации, шифровании данных, обнаружении и реагировании на инциденты безопасности. Развитие инфокоммуникационных систем требует от курсантов развития не только технических навыков, но и коммуникационных навыков. Военные связисты должны быть способными эффективно общаться и сотрудничать в командной среде, координировать свои действия с другими воинскими специальностями и оперативно реагировать на коммуникационные запросы. Системы связи являются ключевым элементом военных операций и тесно связаны с другими военными специальностями. Обучение курсантов будет включать работу в команде с представителями других специальностей, чтобы они могли эффективно интегрировать свои навыки и знания в широкий спектр военных операций.

Общий эффект развития инфокоммуникационных систем на обучение курсантов будет заключаться в более глубоком и широком понимании современных технологий связи, улучшении навыков работы с ними и подготовке курсантов к эффективной работе в современной информационной военной среде.

В заключение, развитие инфокоммуникационных систем и услуг в войсках связи Вооруженных Сил Республики Беларусь является важным аспектом современной военной деятельности. Оно позволяет повысить оперативность, эффективность и безопасность коммуникаций во время выполнения различных задач. Развитие беспилотных систем связи, систем геопозиционирования и навигации, систем связи с высокой пропускной способностью, а также обучение и подготовка персонала являются ключевыми направлениями в этой области.

Список использованных источников:

1. *Современные тенденции развития военного образования [Электронный ресурс]. – Режим доступа <http://elib.bsu.by/handle/123456789/119228/>.*

2. *Интернет-ресурс Министерства обороны РБ.*

3. *Тарасевич А. И. Информационные технологии в системе обеспечения безопасности Республики Беларусь. Минск: БГТУ, 2018. 192 с.*