РАЗВИТИЯ МОБИЛЬНЫХ КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ЭФФЕКТИВНОСТИ ВОЕННЫХ ОПЕРАЦИЙ

Долганов Д.А.

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

Федоренко В.А.

Аннотация. В докладе рассмотрены перспективы и преимущества развития мобильных коммуникационных технологий в военных операциях, а также выделены основные проблемы и уязвимости, связанные с их использованием.

В наше время мобильные коммуникационные технологии играют решающую роль в обеспечении высокой оперативности и связи на поле боя. Современные военные операции требуют надежной, быстрой и защищенной связи для координации действий, передачи информации и принятия оперативных решений.

Развитие мобильных коммуникационных технологий имеет целый ряд важных аспектов. Во-первых, это обеспечение защищенности передаваемой информации, что является критически важным аспектом для успешного проведения военных операций. Во-вторых, современные коммуникационные технологии позволяют обеспечить бесперебойную связь на различных типах территории и в условиях жестких климатических условий. Наконец, развитие мобильных коммуникационных технологий способствует улучшению координации действий военных подразделений и оперативности принятия решений. Проводя плановые мероприятия по переходу на современную технику связи, войска связи становятся более компактными и мобильными, при этом боевые возможности воинских частей и подразделений связи увеличились на порядок. Для продолжения совершенствования войск связи проводятся мероприятия по разработке и внедрению мобильных средств связи.

Мобильные средства связи – это средства, предназначенные для передачи информации по беспроводным каналам связи. Эти устройства обеспечивают возможность связи на перемещающихся объектах, таких как автомобили, поезда, корабли, а также у мобильных пользователей, например, в рамках сотовой связи.

Технологически мобильные средства связи базируются на использовании радиоволн для передачи звука, данных и другой информации. Они включают в себя различные типы устройств, такие как мобильные телефоны, смартфоны, планшеты, носимые устройства и даже навигационные приборы.

Мобильные средства связи используют различные технологии, включая стандарты сотовой связи (например, GSM, CDMA, LTE), беспроводные локальные сети (Wi-Fi, Bluetooth), спутниковую связь и прочие методы передачи данных. В современном мире мобильные средства связи стали неотъемлемой частью нашей повседневной жизни, обеспечивая мобильную связь, доступ в интернет, навигацию, передачу сообщений и многие другие функции.

Важной особенностью мобильных средств связи является их мобильность и доступность в различных местах, что позволяет людям оставаться на связи в любое время и в любой точке планеты.

Таким образом, мобильные средства связи представляют собой широкий спектр технологий и устройств, обеспечивающих возможность беспроводной связи на перемещающихся объектах и для мобильных пользователей, играющих важную роль в современном информационном обществе.

Войска связи являются самостоятельными специальными войсками, входят в состав военной организации государства и выступают как средство обеспечения его вооруженной защиты.

Тенденции изменения содержания вооруженной борьбы, опыт локальных войн и вооруженных конфликтов последнего десятилетия свидетельствуют, что требования к современной системе связи существенно повысились:

– автоматизация работы должностных лиц значительно увеличила объемы передаваемых сообщений и сократила время их обработки для получения достоверной информации, необходимой для принятия решений;

– быстрое изменение обстановки требует ведения информационного обмена в реальном масштабе времени;

– высокая подвижность объектов и субъектов управления в боевом пространстве обязывает устанавливать связь абонентам преимущественно в движении и с коротких остановок.

Проводя плановые мероприятия по переходу на современную технику связи, войска связи становятся более компактными и мобильными, при этом боевые возможности воинских частей и подразделений связи увеличились на порядок. Для продолжения совершенствования войск связи проводятся мероприятия по разработке и внедрению мобильных средств связи.

В настоящее время мобильные технологии стали неотъемлемой частью жизни людей, а также сферы бизнеса и государственного управления. В войсках связи РБ также активно используются мобильные технологии для обеспечения связи и передачи данных в режиме реального времени.

Одним из примеров использования мобильных технологий в войсках связи РБ является создание специализированных приложений для мобильных устройств, которые позволяют быстро и эффективно передавать информацию между подразделениями, координировать действия военнослужащих и контролировать выполнение задач.

Развитие мобильных коммуникационных технологий связано с использованием различных типов устройств, таких как планшеты, ноутбуки, смарт-часы, умные очки и др. Данные устройства повышают мобильность и удобство использования программного обеспечения, а также могут применяться для сбора и анализа данных, а также для более эффективного управления операциями.

При создании приложений для мобильных средств передачи информации, необходимо учитывать специфику военных операций и создавать мобильные приложения, которые могут быть использованы в различных ситуациях. Например, мобильные приложения для навигации, обмена сообщениями и мониторинга состояния оборудования и оружия могут значительно повысить эффективность военных операций [1].

Однако, внедрение сети 5G в вооруженные силы также вызывает вопросы безопасности и защиты данных. В связи с этим, необходимо уделять особое внимание аспектам кибербезопасности и разработке защищенных коммуникационных систем для предотвращения утечек информации и кибератак.

Таким образом, внедрение сети 5G в вооруженные силы открывает новые перспективы для повышения эффективности операций, обеспечивая быструю передачу данных, интеграцию современных технологий и создание устойчивых коммуникационных сетей в военной сфере.

Кибербезопасность - это область информационной безопасности, которая охватывает меры, технологии и практики, направленные на защиту информационных систем, сетей, данных и устройств от киберугроз, кибератак и несанкционированного доступа.

Основная цель кибербезопасности -это обеспечение надежности, конфиденциальности, целостности и доступности информации в условиях информационных технологий, сетевой связи и цифровых платформ. Кибербезопасность включает в себя как технические меры защиты - такие как шифрование данных, многоуровневые системы защиты, брандмауэры и системы мониторинга, так и организационные и управленческие меры, включая политику безопасности, обучение персонала, аудит безопасности и процедуры реагирования на инциденты.

Современные вооруженные силы сталкиваются с ростом угроз в киберпространстве, что делает кибербезопасность ключевым аспектом в поддержании и обеспечении безопасности информационных систем и коммуникаций. Кибербезопасность в вооруженных силах включает в себя не только защиту от кибератак, но и обеспечение надежности, целостности и конфиденциальности важной информации, поддержание работоспособности коммуникационной инфраструктуры и защиту от утечек данных.

Одной из основных задач кибербезопасности вооруженных сил является защита командно-управляющих систем, систем связи, информационных ресурсов, военно-промышленных комплексов и других объектов от кибератак. В свете растущих угроз кибернетической войны и кибершпионажа, важно обеспечить непрерывность функционирования информационных систем, а также предотвратить несанкционированный доступ к конфиденциальной информации.

Кроме того, кибербезопасность включает в себя разработку и внедрение современных методов аутентификации, шифрования данных, систем мониторинга и обнаружения инцидентов, а также проактивные меры по предотвращению утечек информации. Технические и организационные меры безопасности важны для защиты важных данных и обеспечения надежности коммуникационной инфраструктуры [2].

Наконец, важным аспектом кибербезопасности в вооруженных силах является сотрудничество и взаимодействие на международном уровне. В условиях глобальных киберугроз важно осуществлять обмен информацией и опытом, разрабатывать и внедрять совместные меры защиты и совместные проекты по кибербезопасности.

Таким образом, кибербезопасность в вооруженных силах представляет собой комплексный и многомерный набор мер, технологий и практик, направленных на защиту от киберугроз, обеспечение оперативности и непрерывности коммуникаций, а также на сохранение конфиденциальности и целостности информации. Эффективная кибербезопасность становится неотъемлемой частью современных вооруженных сил в условиях информационного противостояния и растущих киберугроз. Что показывает необходимость в развитии мобильных инфокоммуникационных технологиях для специалистов связи.

Список использованных источников:

1. Военный информационный портал Министерства обороны Республики Беларусь [Электронный ресурс] - Режим доступа: https://www.mil.by/ru/forces/special/us/history/

2. https://russiandrone.ru/publications/metody-obnaruzheniya-malorazmernykh-bespilotnykh-letatelnykh-apparatov-na-osnove-analiza-elektromagn/.