4. Макаренко, С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века : моногр. – СПб. : Наукоемкие технологии, 2017. – 546 с.
5. Макаренко, С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки : моногр. – СПб. : Наукоемкие технологии, 2020. – 337 с.
6. Потапчик, Н. Н. Методический подход к оценке стойкости информационного обмена в условиях информационно-технического воздействия противника // Вестн. Воен. акад. Респ. Беларусь – 2024. – № 3 (84). – С. 36–50.
7. Обзор первого квартала 2024: отчет о DDoS-атаках от компании StormWall [Электронный ресурс]. – Режим доступа : https://stormwall.pro/otchet-o-ddos-atakah-2024-perviy-kvartal/. – Дата доступа : 24.01.2025.
8. В Совбезе рассказали о создании системы противодействия опасным DDoS-атакам [Электронный ресурс]. – Режим доступа: https://ria.ru/20240305/ddos-1931151155.html/. – Дата доступа : 25.01.2025.
9. В Куркой области наблюдаются перебои с мобильной связью и интернетом [Электронный ресурс]. – Режим доступа : https://vedomosti.ru/technology/ news/2024/08/09/1054950-na-blyudayutsya-pereboi.html/. – Дата доступа : 28.01.2025.
10. Давыдов, А. Е., Максимов, Р. В., Савицкий, О. К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. – М. : Воентелеком, 2015. – 520 с.

УДК 681.5

к.т.н., доцент Михнёнок Е. И.
к.т.н., доцент Сахарук Д. А.
Сергеенко А. В.
УО «ВА РБ», г. Минск
andrew-sergeenko@mail.ru

ТРЕБОВАНИЯ К СОВРЕМЕННЫМ УСТРОЙСТВАМ ПЕРЕДАЧИ ДАННЫХ ТАКТИЧЕСКОГО УРОВНЯ

Аннотация. В статье проведен краткий анализ организации системы связи и передачи данных на тактическом уровне в ходе проведения специальной военной операции Вооруженных сил Российской Федерации на Украине. Определены основные требования предъявляемые к перспективным устройствам передачи данных, применяемым на тактическом уровне.

Ключевые слова: средства связи, передача данных, тактический уровень.

Проводимая Вооруженными силами Российской Федерации специальная военная операция (СВО) на Украине подтвердила тезис о необходимости повышения устойчивости системы связи и передачи данных при организации и ведении боевых действий, особенно на тактическом уровне. Анализ реализованной системы связи и передачи данных, позволил выделить ряд вопросов, требующих решения для успешного ведения современного общевойскового боя:

- укомплектованность индивидуальными средствами связи в пехотных подразделениях. На начало СВО только в специальных подразделениях индивидуальные средства связи имелись у каждого военнослужащего, в обычных механизированных подразделениях такие средства связи появлялись у командиров начиная от командира отделения. Современные условия ведения общевойскового боя требуют наличия индивидуальны средств связи у каждого бойца;

- повышение пропускной способности штатных средств связи. Широкое применение средств разведки, в первую очередь оптических, размещенных на беспилотных летательных аппаратах, повлекло за собой необходимость передачи больших объемов информации (в том числе и видеопотока) на командные пункты подразделений;

- слабые горизонтальные связи внутри подразделений и практически полное отсутствие горизонтальных связей между взаимодействующими подразделениями;

- низкая обученность личного состава по вопросам использования и эксплуатации средств связи;

- устойчивость к системам радиоэлектронной разведки (РЭР) и радиоэлектронной борьбы (РЭБ).

В решении данных вопросов активное участие помимо Министерства обороны Российской Федерации принимают волонтерские движения. Так, команда «ZOVКарты» активно предоставляет в подразделения собственные устройства передачи данных «Квант», внешний вид представлен на рисунке 1 а.

Для обеспечения работы устройств передачи данных необходимо средство автоматизации (СА) с установленным специальным программным обеспечением (СПО) «Квант» и «ZOV Карты». Устройства передачи данных построены на базе LoRa-модемов, что позволяет обеспечивать связь на удалении нескольких километров, а использование реализованных в СПО протоколов построения mesh-сетей, позволяет увеличить дальность работы устройств до нескольких десятков километров, а также обеспечить построение горизонтальных связей как внутри подразделения, так и с взаимодействующими подразделениями. Относительно малая мощность излучения позволяет уменьшить вероятность обнаружения средствами РЭР.

Аналогичные устройства передачи данных поставляет в подразделения команда «Гроза/Глаз», внешний вид представлен на рисунке 1 б.

а) б)

а) – внешний вид устройства передачи данных «Квант»;
б) – внешний вид устройства передачи данных СПО «Гроза/Глаз»
Рисунок 1 – Внешний вид устройств передачи данных на базе LoRa-модемов

При этом, также, как и в устройстве передачи данных «Квант», для работы необходимо СА с установленным СПО «Гроза».

Помимо этого, существует множество инициативных групп, поставляющих в подразделения гражданские радиостанции от производителей «Motorola», «Hytera», «TYT» и др. Среди таких инициативных групп следует выделить команду «Веда» которая выполняет прошивку радиостанций типа «TYT MD-UV390» собственным СПО, которое обеспечивает повышенную криптографическую защиту передаваемых данных.

Благодаря работе волонтерских и инициативных команд, были частично решены проблемы с недостаточной укомплектованностью индивидуальными средствами связи. В подразделениях появились новые средства связи позволяющие обеспечить передачу больших объемов данных. Однако это породило новые проблемы:

- низкая унификация средств связи. Например, аккумуляторные батареи одного производителя могут требовать использование разных зарядных станций;
- отсутствие возможности обмена данными между разнотипными радиостанциями с использованием технических средств маскирования и криптографических средств защиты информации. Например, устройства передачи данных, поставляемые командами «ZOVКарты» и «Гроза/Глаз», хоть и имеют единую техническую основу, не могу обеспечить обмен данными между собой, а также сопряжение СА с установленным СПО «ZOVКарты» и «Гроза».

Таким образом, можно выделить следующие основные требования предъявляемые к устройствам передачи данных, применяемым на тактическом уровне:

- возможность сопряжения с автоматизированными рабочими местами (АРМ) (ноутбуки, планшеты, смартфоны и т.п.) по наиболее распространенным интерфейсам передачи данных (USB, Bluetooth, Wi-Fi, Ethernet и т.п.);
- единые протоколы обмена данными с АРМ;
- возможность дистанционного управления непосредственно с АРМ;
- возможность регулирования выходной мощности;
- в режимах фиксированной рабочей частоты, при отсутствии противодействия противника обеспечение дальности связи от 2 до 8 км;
- в режимах псевдослучайной перестройки рабочей частоты, при отсутствии противодействия противника обеспечение дальности связи от 2 до 5 км;
- применение стандартизированных единых методов криптографической защиты информации;
- обеспечение канальной скорости передачи данных не менее 19,2 кбит/с;
- возможность построения mesh-сетей;
- возможность сканирования нескольких заданных каналов;
- высокая степень унификации по зарядным устройствам, аккумуляторным батареям, антенным устройствам, гарнитуре.

Список используемых источников и литературы

1. Иванов, В. Г. Перспектива развития автоматизированных систем управления специального назначения в интересах управления войсками / В. Г. Иванов, Г. А. Тучин, Е. Ю. Русаков, А. Н. Назаров // САПР и графика. - 2024. - N1. - С. 58-64.