НАЦІОНАЛЬНИЙ ЮРИДИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЯРОСЛАВА МУДРОГО

ВІЙСЬКОВО-ЮРИДИЧНИЙ ІНСТИТУТ

Кафедра загальновійськових дисциплін

ЗАТВЕРДЖУЮ
Начальник кафедри
загальновійськових дисциплін
полковник Станіслав КОРОЛЬОВ
« _____ » _____ 20____ р.

ЛЕКЦІЯ № 9
з навчальної дисципліни
«ОРГАНІЗАЦІЯ ВІЙСЬКОВОГО ЗВ'ЯЗКУ»

Модуль 2. Організація зв'язку в механізованому і танковому батальйонах
Змістовий модуль 2.4. Особливості організації зв'язку за досвідом АТО та ООС
Заняття 2.4.1. Особливості організації зв'язку за досвідом АТО та ООС

Харків

Тема: Особливості організації зв'язку за досвідом АТО та ООС

Навчальний потік: 3 курс військово-юридичного інституту

Місце: лекційна аудиторія

Навчальна та виховна мета:

Вивчити:

- особливості побудови системи зв'язку частин (підрозділів) у ході їх застосування в АТО;
- особливості застосування різних родів зв'язку в ході АТО.

Виховувати:

- широкий оперативно-тактичний кругозір;
- зацікавленість щодо вивчення навчальної дисципліни.

Навчальні питання і розподілення часу: (слайд 2)

№ з/п	Зміст занять, навчальні питання	Час, хв.
I	**Вступна частина**	**5**
II	**Основна частина**	**80**
	1. Особливості побудови системи зв'язку частин (підрозділів) у ході їх застосування в АТО та ООС	*30*
	2. Особливості застосування різних родів зв'язку в ході АТО та ООС	*30*
	3. Забезпечення засекреченого зв'язку та безпека зв'язку в ході АТО та ООС	*20*
III	**Заключна частина**	**5**

Навчально-матеріальне забезпечення:

1. Мультимедійний проектор Inphocus;
2. Презентація за темою лекції, підготована за комп'ютерною програмою Microsoft PowerPoint;
3. Схеми за темою лекції.

Навчальна література:

1. Організація військового зв'язку (В.Г. Шолудько, М.Ю. Єсаулов, О.В. Вакуленко, Т.Г. Гурський, М.М. Фомін). Навчальний посібник. – К.: ВІТІ, 2016 р. – 282 с.
2. Організація військового зв'язку. О.О. Лаврут, С.О. Івко, Б.М. Бойчук, С.В. Давіденко, О.М. Манюк. Інтерактивний посібник. – Л: НАСВ, 2016 р. Режим доступу: http://manyukoleksandr.esy.es/.
3. Керівництво з технічного забезпечення зв'язку та автоматизації управління військами Збройних Сил України (КТЗЗ та АУВ ЗСУ – 2002). – К. : Військове видавництво, 2002. – 134 с.
4. Бойовий статут механізованих і танкових військ Сухопутних військ Збройних Сил України. Частина II. Батальйон, рота. – Київ: Командування Сухопутних військ Збройних Сил України, 2016. — 260 с.
5. Стан та перспективи застосування сучасних технологій та засобів радіозв'язку в Збройних Силах України. О.О. Лаврут, О.К. Климович, М.Л. Тарасюк, О.Л. Антонюк. Системи обробки інформації. Х.:ХНУПС, 2017. – № 1 (147),– С. 159 –167.
6. Роман Туровець. «Цифра» в суворих умовах бойових дій. Режим доступу: https://army.unian.ua/.
7. Зв'язок в українській армії. Режим доступу: http://bmpd.livejournal.com.
8. Організація системи зв'язку тактичної ланки. Український мілітарист. Новини військової справи в Україні та світі. Військова наука. Тактика та озброєння. Режим доступу: https://ru-ru.facebook.com/UkrMil.
9. IX науково-практична конференція. «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в АТО». 25 листопада 2016 року. (Доповіді та тези доповідей). – К.: ВІТІ. – 2016. – 212 с.

ЗМІСТ ЛЕКЦІЇ ТА МЕТОДИКА ВИКЛАДЕННЯ

Дана лекція є лекцією інформаційного типу. Вона повинна починатися з короткого вступу, у якому до аудиторії доводиться тема лекції, її значення у системі підготовки військового фахівця, цільова настанова і план лекції. Також необхідно дати стислу характеристику навчальної літератури, яка рекомендується.

В основній частині лекції, при розгляданні кожного питання, доцільно формулювати проблему, яка розглядається, встановлювати її зв'язок із майбутньою діяльністю військового фахівця.

Розкриття питань лекції, як і її загального змісту, здійснюється шляхом раціонального поєднання методів індукції і дедукції, прийомів викладання від часткового до загального. Лекція повинна формувати у тих, хто навчається, здатності до абстрактного мислення. Викладення матеріалу повинно супроводжуватися демонстрацією слайдів.

Лекція повинна закінчитися формулюванням стислих висновків з матеріалу, який розглядався, викладенням рекомендацій для самостійної роботи, якщо вони не були дані раніше у ході лекції та відповідями викладача на питання курсантів.

ВСТУП

До АТО на території Донецької та Луганської областей Збройні Сили України мали у своєму розпорядженні, успадковані від СРСР засоби зв'язку, які до кінця 2013 року сильно втратили в кількості і якості. Їх намагалися модернізувати силами оборонпрому й приватних компаній, але із-за недоліку фінансування оборонного сектору далі пари виставок і гарних буклетів не пішло. На полігонах та у військах так і використовували старі добрі радіостанції радянських років.

На почату АТО, при спробі розгортання підрозділів почали виявляться всі недоліки забезпечення підрозділів зв'язком: на тій же техніці зв'язок частково працював, але не покривав всіх потреб; засоби зв'язку перебували в незадовільному технічному стані.

Крім цього в гібридній війні найбільш уразливими виявилися системи управління і зв'язку, побудовані за класичними схемами і на великогабаритній автотранспортній базі, з вузлами зв'язку на десятках КШМ з десятками кілометрів польових кабелів. Отже, необхідно було шукати технічне рішення щодо скорочення великогабаритних польових засобів управляння і зв'язку, а також уніфікації їх зовнішніх відмінних ознак, так як в умовах гібридної війни будь-яка автотранспортна одиниця, що має нетипові ознаки, є об'єктом ураження.

Зараз управління військами в зоні антитерористичної операції здійснюється за допомогою сучасних цифрових засобів зв'язку, адже поштовх до стрімкого переходу на «цифру» був продиктований життям.

Сьогоднішня лекція присвячена особливостям організації і забезпечення зв'язку в АТО саме з урахуванням вище приведених факторів.

1. Особливості побудови системи зв'язку частин (підрозділів) у ході їх застосування в АТО та ООС

З початком АТО використання аналогових засобів зв'язку, які передбачали *прив'язку до ліній «Укртелекому»* було відразу відкинуте. Причиною стало те, що практично всі лінії зв'язку цього підприємства проходили через Донецьк та інші міста, що контрольовані терористами.

Застосування радіорелейних та тропосферних станцій було також зведено до мінімуму. По-перше, на їхнє розгортання потрібно багато часу, що впливає на термін готовності пункту управління до роботи. По-друге, підняти високу щоглу з антенами в умовах, коли позиції українських військ і особливо пунктів управління ретельно відслідковувались і піддавалися обстрілам, означало демаскувати і піддати небезпеці місце свого розташування. За тих же причин організатори зв'язку намагались відмовлятись від розгортання вузлів зв'язку, до яких входили *апаратні старого парку*. Великий вузол зв'язку з безліччю машин становить помітну ціль, знищення якої фактично унеможливить процес управління.

Досвід організації зв'язку в ході АТО призвів до *зміни ряду поглядів на способи організації зв'язку та принципи побудови системи зв'язку Збройних сил*:

Система зв'язку у ході застосування Збройних сил України зараз будується на основі стаціонарного компонента, нарощеного польовими засобами. У зв'язку з обмеженою кількістю лінійних засобів зв'язку, особливо цифрових, польова опорна мережа зв'язку ЗС України не розгортається. Польовий компонент системи зв'язку будується на лініях прив'язки вузлів зв'язку пунктів управління до телекомунікаційної мережі загального користування (ТМЗК) та лініях прямого супутникового зв'язку між пунктами управління, зарезервованого на основних напрямках тропосферними засобами зв'язку (рис. 1.1).

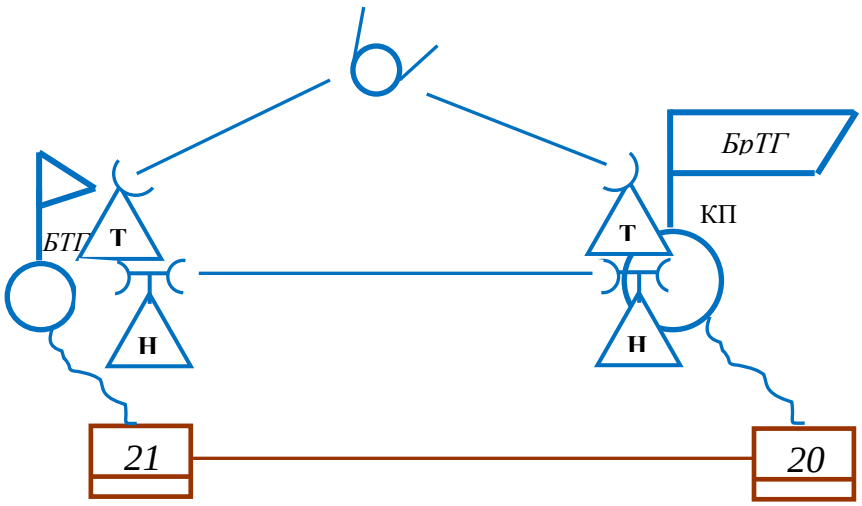

Рис. 1.1. Особливості побудови системи зв'язку в ході АТО (варіант)

Тропосферні лінії зв'язку (ущільнені цифровими модемами) застосовуються не лише для організації прямих зв'язків між пунктами управління, а також для організації ліній прив'язки в місцях, де організація одноінтервальної радіорелейної та проводової прив'язки ускладнена.

Радіорелейні лінії зв'язку на багатоканальних РРС Р-414, навіть ущільнені цифровими модемами, практично не застосовувались внаслідок низької мобільності та демаскувальних ознак (високих антен).

Широкого застосування набули малогабаритні радіорелейні станції широкосмугового доступу (нанобридж і т.д.) (рис. 1.1).

Радіозв'язок УКХ-діапазону, який раніше використовувався лише в тактичній ланці управління, витісняє система транкінгового зв'язку, яка включає в себе всі ланки управління від стратегічної до тактичної. Якщо раніше УКХ-радіозв'язок дозволяв будувати лише локальні мережі та напрямки, зараз завдяки об'єднанню транкінгових мереж супутниковими лініями зв'язку ми маємо можливість використовувати глобальну мережу транкінгового зв'язку від Генерального штабу Збройних сил України до окремих взводних опорних пунктів (рис. 2.1).

Радіозв'язок КХ-діапазону, який практично не використовувався на радіостанціях Р-161А2М внаслідок великої потужності випромінювання, з застосуванням сучасних радіостанцій типу "HARRIS" набув широкого застосування в оперативно-тактичній та стратегічній ланках управління, а також при застосуванні підрозділів спеціального призначення (рис. 2.2).

В ході ведення антитерористичної операції набули вкрай важливого значення мережі радіо-, транкінгового та супутникового зв'язку. Якщо раніше внаслідок їх вузькосмуговості та малоканальності вони використовувалися як лінії прямого зв'язку між командирами та штабами, зараз, наприклад, супутникова мережа є основою транспортної мережі системи зв'язку.

2. Особливості застосування різних родів зв'язку в ході АТО та ООС

Застосування транкінгового зв'язку

Засоби радіозв'язку виробництва радянських часів, які перебувають на озброєнні до цього часу, за своїми тактико-технічними характеристиками не відповідають сучасним вимогам. Засоби радіозв'язку у тактичній ланці управління працюють без забезпечення завадостійкості (псевдовипадкового переналаштування робочих частот), шифрування (захищений режим) переговорів, передачі даних, позиціонування та можливості відображення інформації на робочих місцях посадових осіб.

Також досвід ведення бойових дій показав недоцільність використання КХ радіостанцій середньої потужності (Р-161), які знищувалися ракетно-артилерійським вогнем відразу ж після включення на передачу.

У зв'язку з цим всередині військових формувань почали активно використовуватися транкінгові радіостанції. Звичайно вони не повністю відповідають вимогам до військового радіозв'язку, але ефективність застосування цих засобів пов'язана насамперед з невеликими габаритами і стійкістю до перешкод. Крім того, за потреби ці станції дозволяють зв'язатись з вищими штабами за допомогою спеціальних ретрансляторів.

Засоби цифрового транкінгового радіозв'язку забезпечують маскування мови в УКХ діапазоні, а також можливість інтегрування ретрансляторів в єдину мережу за допомогою технології Ethernet. Система транкінгового зв'язку організована по каналах зв'язку, утворених радіо- та супутниковими засобами з використанням наземних, та за необхідністю, повітряних ретрансляторів (рис. 2.1).

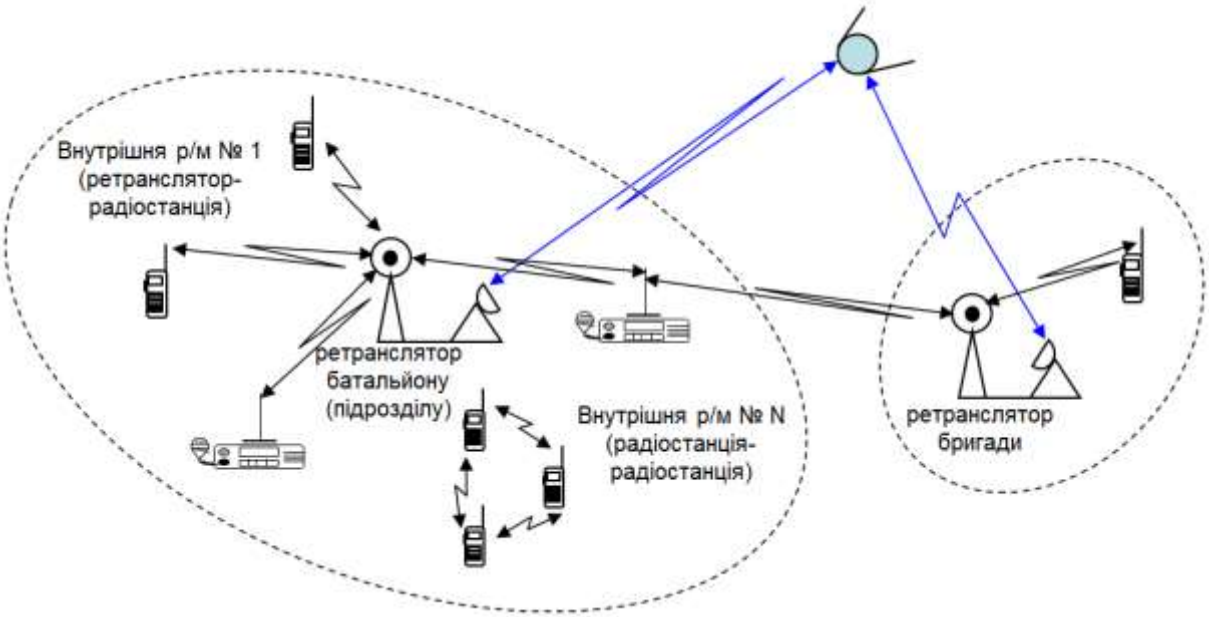

Рис. 2.1. Варіант організації транкінгового і супутникового зв'язку в ланці бригада – батальйон

В системі транкінгового зв'язку передбачено можливість безпосереднього управління визначеними військовими частинами та підрозділами шляхом включення відповідних абонентів в глобальний канал транкінгового зв'язку або входження старшого начальника в мережі транкінгового зв'язку угрупувань військ (секторів).

Для забезпечення взаємодії між військовими частинами та підрозділами, у кожному підрозділі до ротної тактичної групи включно, передбачено автомобільні радіостанції транкінгового зв'язку, налаштовані для роботи через повітряний ретранслятор. При цьому другий канал повітряного ретранслятора використовується для надання можливості самостійної організації зв'язку взаємодії між військовими частинами та підрозділами. Також передбачено загальні канали взаємодії в мережах транкінгового зв'язку. Застосування цифрового транкінгового радіозв'язку у військах дозволило забезпечити нагальні потреби управління у тактичній ланці.

Застосування радіо- та супутникового зв'язку

На початку АТО радіостанції, які дозволяють зв'язуватись на великих відстанях (Р-161А2М, Р-140М) із-за відсутності перешкодостійких режимів піддавалися потужному впливу систем радіоелектронної боротьби противника, що діяли проти українських військових з території Російської Федерації. Були ситуації, коли неможливо було зв'язатись по радіо на коротких хвилях на відстані до 60 кілометрів. І це радіостанціями, які дозволяють тримати зв'язок на відстані до тисячі кілометрів! Ефір був настільки «забитий» засобами РЕБ, що практично на кожній частоті була потужна перешкода.

Тому в даний час для забезпечення *УКХ і КХ радіозв'язку* в ланці бригада – батальйон і вище використовуються сучасні іноземні засоби радіозв'язку військового призначення Harris (рис. 2.2).

Для забезпечення потреб ЗС України у сучасних засобах радіозв'язку пропонується налагодити виробництво іноземних засобів радіозв'язку військового призначення на території України, або провести закупівлю, лізинг чи отримання у

якості допомоги КХ, УКХ радіостанцій закордонних виробників (виробів компаній Harris, разом з програмним забезпеченням типу Falcon Command та шифрування стандарту AES 128, 256 біт або Citadel 128, 256 біт).

Не останнє значення мало й те, що для охорони системи зв'язку (ліній, станцій та вузлів), побудованої старими аналоговими засобами, необхідно було залучати певну кількість особового складу. А в умовах бойових дій, де кожен боєць важливий, командири дозволити собі таку розкіш не могли.

Саме тому військові зв'язківці віддавали перевагу здебільшого застосуванню сучасних малогабаритних станцій супутникового і транкінгового зв'язку.

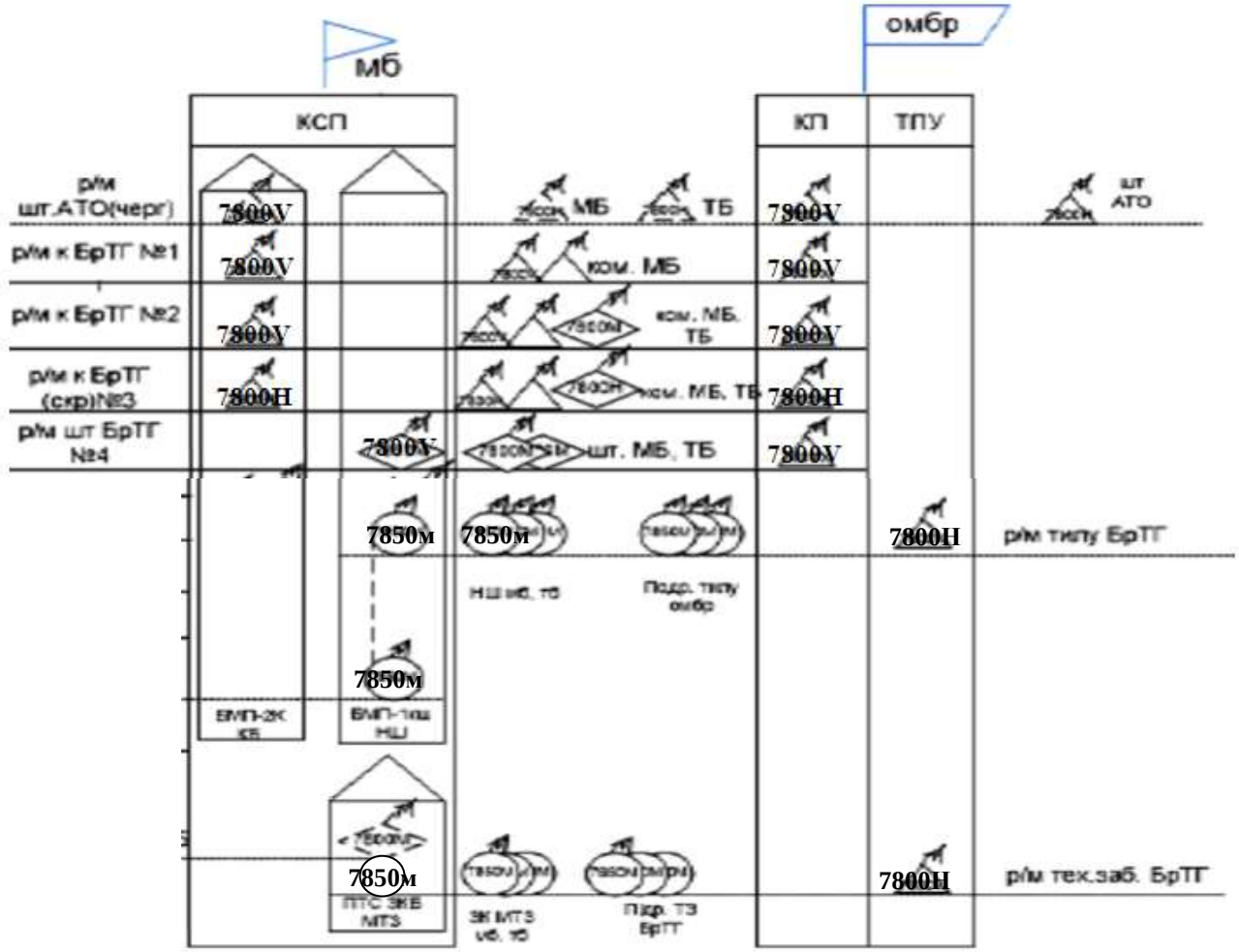

Рис. 2.2. Організація радіозв'язку командира і штабу омбр з командиром і штабом мб

Основним зв'язком між пунктами управління штабів, військових частин та окремих підрозділів, що діють у зоні АТО, став *супутниковий*. Компактні станції легко транспортуються й досить швидко встановлюються та налаштовуються. При цьому якість зв'язку, яку вони забезпечують, є високою. По зашифрованих супутникових каналах військові організували як телефонний зв'язок, так і передачу документованих повідомлень (рис. 2.1).

Через відсутність національного супутника зв'язку, станцій супутникового зв'язку та портативних терміналів супутникового зв'язку військового призначення було прийнято рішення на використання станцій супутникового зв'язку комерційного призначення. На цей час розгорнута повнозв'язна підсистема

супутникового зв’язку, яка доведена до окремих батальйонних та ротних тактичних груп, ротних та окремих взводних опорних пунктів. Крім цього вона використовується для створення багатосайтової мережі транкінгового зв’язку. З метою підвищення живучості системи супутникового зв’язку розглядається рішення щодо нарощування системи засобами Ku-діапазону (10,7 — 12,75 ГГц).

Також пропонується розпочати роботи щодо відновлення державної програми із запуску національного супутника зв’язку та створення вітчизняного виробництва станцій супутникового зв’язку військового призначення з можливістю організації зв’язку (обміну інформацією), як в стаціонарному виконанні так і в русі. У разі відсутності достатнього фінансування пропонується розглянути можливість закупівлі чи лізингу станцій супутникового зв’язку військового призначення у закордонного виробника.

Застосування тропосферного, проводового та радіорелейного зв’язку

Засоби тропосферного, проводового та радіорелейного зв’язку виробництва СРСР в більшості, являються аналоговими, морально та технічно застарілими, мають низьку пропускну спроможність та велику енергоємність.

Та все ж повністю відмовитись від техніки старого парку в зоні АТО на початку бойових дій не змогли. Це стосується вже згаданих радіорелейних та тропосферних станцій, які застосовуються для побудови резервних ліній зв’язку. Їх просто нічим було замінити. Але використовувалися вони обмежено і тільки там, де дозволяла безпекова обстановка.

Як уже було сказано раніше,тропосферні лінії зв’язку (ущільнені цифровими модемами) зараз застосовуються не лише для організації прямих зв’язків між пунктами управління, а також для організації ліній прив’язки в місцях, де організація одноінтервальної радіорелейної та проводової прив’язки ускладнена.

Проводові засоби використовуються для, як правило, для побудови ліній прив’язки вузлів зв’язку пунктів управління до телекомунікаційної мережі загального користування (ТМЗК) (рис. 1.1).

Радіорелейні лінії зв’язку на багатоканальних РРС Р-414, навіть ущільнені цифровими модемами, практично не застосовувались внаслідок низької мобільності та демаскувальних ознак (високих антен).

Широкого застосування набули малогабаритні радіорелейні станції широкосмугового доступу (нанобридж і т.д.) (рис. 1.1).

Застосування інформаційних систем

Основу АСУ “Дніпро” складають інформаційно-телекомунікаційні вузли, які розгорнуті на стаціонарних вузлах зв’язку пунктів управління в стратегічній та оперативній ланках управління. На польових пунктах управління батальйонних (ротних) тактичних груп, окремих ротних опорних пунктів та взводних опорних пунктів розгорнуті АРМ АСУ “Дніпро” з використанням супутникових каналів зв’язку;

В переважній більшості АСУ “Дніпро” використовується для обміну відкритими документальними повідомленнями з використанням електронної пошти. Для обміну інформацією великих об’ємів (розміром в десятки та сотні мегабайт) розгорнуто ftp-сервер.

Продовжуються роботи щодо розробки спеціального програмного забезпечення для планшетів артилериста (з вбудованими балістичними калькуляторами та іншими допоміжними програмами) з метою обміну

інформацією в артилерійських підрозділах через радіостанції типу Motorola.

Заплановано впровадження програмного забезпечення для централізованого налагодження радіостанцій транкінгового зв'язку.

3. Забезпечення засекреченого зв'язку та безпека зв'язку в ході АТО та ООС

Забезпечення засекреченого зв'язку

На момент початку АТО система засекреченого зв'язку ЗС України знаходилась у процесі поступової заміни апаратури ЗАЗ виробництва колишнього СРСР на сучасну апаратуру IP-шифрування вітчизняного виробництва. Телефонна апаратура ЗАЗ тимчасової стійкості була знята з озброєння, також була заборонена передача інформації з обмеженим доступом по апаратурі телеграфного засекречування, проте нових засобів ЗАЗ взамін старих поставлено не було. Принципи організації засекреченого зв'язку на нових засобах були у процесі розробки. Апаратурою криптографічного захисту інформації (далі – КЗІ) були забезпечені лише стаціонарні інформаційно-телекомунікаційні вузли (ІТВ) органів військового управління стратегічної та оперативної ланок та набуто певного досвіду щодо використання зазначеної апаратури на рухомих пунктах управління.

У ході проведення АТО були розгорнута та постійно нарощувалася мережа обміну службовою інформацією (далі – МОСІ) Збройних сил України, проводилося нарощування захищеної системи обміну інформацією (далі – ЗСОІ) Збройних сил України. На цей час, МОСІ доведена до батальйонної ланки, ЗСОІ – до оперативної ланки (вид ЗС, ОК) польовими засобами та до штабів бригад – стаціонарними. До кінця 2015 року було проведено нарощування цих систем та доведення: МОСІ – до батальйонної тактичної групи, мотопіхотного батальйону, роти, ЗСОІ – до бригади, полку.

В ланці бригада – батальйон для закриття каналів зв'язку або групових цифрових потоків використовується АПК "Г" (апаратура криптозахисту).

Для організації мережі обміну службовою інформацією (МОСІ) в мб (БТГр) використовується В-271. Так при організації супутникового зв'язку на напрямку зв'язку КСП мб – КП мбр можливо забезпечити 1-2 ТФ канали для організації МОСІ (ДСК).

В подальшому планується використання для побудови перспективних інформаційно-телекомунікаційних систем новітніх засобів IP-шифрування, розроблених за замовленням ЗС України;

Здійснення обміну інформацією в стратегічній ланці управління з грифом секретності до "цілком таємно", "таємно" – до бригади включно, "ДСК" – до роти включно, також на рівні батальйон-рота-взвод використовувати засоби маскування мови для засобів зв'язку;

Взаємодію з іншими держаними органами та іншими силовими структурами України здійснювати через ГІТВ ГШ ЗС України по Захищеній мережі передачі даних Державної служби спеціального зв'язку та захисту інформації України.

Кібернетична безпека

З початком агресії Російської Федерації на території України зафіксоване значне зростання інтенсивності кібернетичних атак, направлених на порушення функціонування інформаційно-телекомунікаційних систем Міністерства оборони України та Збройних сил України.

Більшість епізодів загострення військово-політичної обстановки, таких як референдум в АР Крим, захоплення кораблів ВМС України, псевдовибори в так званих ЛНР та ДНР, проведення антитерористичної операції на Сході України супроводжувалися потужними кібератаками на ІТС МО та ЗС України, в тому числі і на офіційний веб-портал Міністерства оборони України.

Форми і методи реалізації кібернетичних атак постійно змінюються і ускладнюються.

Майже всі кібератаки здійснювались з території Російської Федерації. Кібератаки з території інших держав з високою ймовірністю здійснювались з використанням бот-мереж підконтрольних спецслужбам Російської Федерації.

З метою недопущення деструктивного впливу на інформаційно-телекомунікаційні системи Міністерства оборони України та Збройних сил України розгорнута та набирає бойових можливостей система кібернетичної безпеки в ІТС Збройних сил України, яка може:

− здійснювати контроль (моніторинг) стану кібернетичної безпеки елементів ІТС, інформаційних ресурсів та надавати рекомендації щодо підвищення рівня їх захищеності;

− здійснювати дистанційно оцінку (контроль) ефективності програмних та програмно-апаратних засобів захисту інформації;

− здійснювати виявлення уразливостей апаратного та програмного забезпечення об’єктів критичної інформаційної інфраструктури, оновлення бази даних ідентифікованих уразливостей;

− забезпечити своєчасне оновлення програмного забезпечення елементів ІТС, антивірусних програмних засобів та іншого програмного забезпечення;

− блокувати джерела деструктивного програмно - математичного впливу на ІТС Збройних сил України;

− виконувати заходи щодо усунення наслідків впливу кібератак.

Існує багато проблемних питань, які успішно вирішуються.

Основні шляхи вирішення проблемних питань:

− розробка нормативно-правових актів у сфері кібернетичної безпеки в шестимісячний термін після прийняття загальнодержавних законодавчих актів у цій сфері;

− навчання фахівців з кібернетичної безпеки на спеціалізованих курсах;

− проведення спеціалізованих навчань з кібердій у кіберпросторі Збройних сил України;

− проведення тренувань особового складу кібернетичної безпеки під час проведення навчань (тренувань) Збройних сил України;

− участь у міжнародних навчаннях з кібероборони;

− забезпечення закупівлі засобів для створення системи захисту інформації та кібербезпеки за найвищим пріоритетом.

Забезпечення безпеки інформації

Безпека інформації у відкритих інформаційно-телекомунікаційних системах Збройних сил України здійснюється шляхом застосування організаційних і технічних рішень з захисту інформації (впровадженням комплексних систем захисту інформації в АСУ ЗС України “Дніпро”, ІСД-Інтернет, використанням вбудованих конструктивних і схемотехнічних рішень автоматичних телефонних

станцій єдиної автоматизованої мережі ЗС України, обмеженням роботи на передачу радіозасобів та використання переговорних таблиць в КХ-радіомережах, використанням вбудованих засобів шифрування засобів цифрового транкінгового зв'язку з довжиною ключів 256 та 40 біт, застосуванням технологій VPN при використанні супутникових каналів зв'язку, впровадженням організаційних заходів щодо обмеження використання засобів стільникового зв'язку), кібернетичної безпеки та заходів контролю (моніторингу) безпеки інформації.

Кібернетична безпека системи зв'язку ЗС України забезпечується організаційними заходами та технічними засобами. На АРМ користувачів здійснюється розмежування прав доступу шляхом впровадження засобів захисту інформації, а також застосовується антивірусне програмне забезпечення. На транспортному рівні впроваджено захист за допомогою налаштування безпеки серверів, маршрутизаторів, загороджувальних серверів та програмних міжмережних екранів. Проте такі заходи лише частково захищають систему зв'язку ЗС України від деструктивного кібернетичного впливу, тому розпочато розгортання апаратних засобів кібернетичної безпеки на основних елементах системи зв'язку ЗС України.

Контроль (моніторинг) безпеки інформації здійснюється у відкритих телефонних мережах Збройних сил України, в автоматизованій системі управління Збройними силами України "Дніпро", в інформаційній системі з доступом до мережі Інтернет, а також у радіомережах Збройних сил України та радіомережах Генерального штабу Збройних сил України.

Результати контролю свідчать про низький рівень дотримання правил прихованого управління військами в усіх ланках управління при застосуванні відкритих інформаційно-телекомунікаційних систем.

Так у радіомережах КХ/УКХ діапазону, незважаючи на фактично запроваджений режим радіомовчання, за час проведення антитерористичної операції на сході України було зафіксовано багато прошень другої та третьої категорій. У відкритих телефонних мережах Збройних сил України також зафіксовані порушення безпеки інформації. В АСУ ЗС України "Дніпро" також зафіксовані порушення різних категорій.

Іншим проблемним питанням є те, що, незважаючи на численні розпорядження Генерального штабу, особовий склад у зоні проведення АТО продовжує користуватися особистими мобільними телефонами, у тому числі й на пунктах управління. Це створює реальну загрозу як витоку інформації з обмеженим доступом, так і визначення місць розміщення пунктів управління та скупчення військ.

Висновок:

Запропоновані підходи до вирішення проблемних питань дозволять:

− забезпечити потреби службових осіб органів управління ЗС України у наданні сучасних якісних інформаційних та телекомунікаційних послуг (сервісів);

− забезпечити взаємне використання ресурсів систем зв'язку усіх телекомунікаційних мереж Сектора безпеки і оборони України при виконанні спільних завдань у мирний та воєнний час;

− здійснити повний перехід системи зв'язку Збройних сил України з аналогових на цифрові телекомунікаційні засоби, створити єдиний

телекомунікаційний простір для забезпечення функціонування елементів Єдиної автоматизованої системи управління Збройних сил України;

− забезпечити виконання вимог щодо своєчасності, достовірності та скритності зв'язку на основі широкого впровадження новітніх інформаційно-телекомунікаційних технологій, перспективних цифрових засобів (систем, комплексів) зв'язку і автоматизації;

− забезпечити захист інформації та кібернетичну безпеку в інформаційно-телекомунікаційних системах Збройних сил України;

− створити сприятливі умови для подальшої розробки і впровадження сучасних засобів зв'язку та інформатизації.

Принцип випереджаючої готовності системи зв'язку і військ зв'язку, щодо готовності органів управління військами диктує потребу підготовки висококваліфікованих фахівців зв'язку, які відповідають сучасним потребам розвитку у галузях телекомунікації, інформатизації, захисту інформації та кібернетичної безпеки і приведення змісту підготовки фахівців зв'язку до потреб сьогодення.

ЗАКЛЮЧЕННЯ

Необхідність стрімкого переходу на нові засоби зв'язку була продиктована передусім обстановкою, що склалась у зоні АТО. На Херсонщині було можливе застосовування аналогового обладнання, адже територія, на якій розгорталась система зв'язку, була повністю під контролем наших військ. Проте під час заходу до зони АТО використання старих систем зв'язку припинялось, адже в тих умовах це було недоцільним та неможливим з позицій безпеки, мобільності й оперативності системи управління військами.

У підсумку є всі підстави стверджувати, що дії зв'язківців у зоні АТО дали позитивний результат. Адже з початку проведення антитерористичної операції вони практично не мали фактів знищення засобів зв'язку під час артилерійських обстрілів, зокрема з систем залпового вогню. Фахівці зв'язку ніколи не забувають кілька важливих понять, що характеризують функціонування систем зв'язку, такі як «безпека», «стійкість», «живучість», «надійність». При цьому роблять акцент саме на надійності, адже добре розуміють значення надійного зв'язку в системі управління військами в сучасних умовах.

Лекцію розробив
Старший викладач
кафедри загальновійськових дисциплін Геннадій ЗМІЇВСЬКИЙ

Лекція обговорена і схвалена
на засіданні кафедри,
протокол №_____
від «_____» _____20___ р.