

Доктрина зв'язку та кібербезпеки Збройних Сил України

Доктрину розроблено робочою групою офіцерів Командування Військ зв'язку та кібербезпеки ЗС України та погоджено із заінтересованими органами військового управління ЗС України та структурними підрозділами Генерального штабу ЗС України.

У Доктрині враховано погляди керівництва ЗС України на те, якими мають бути сучасні Війська зв'язку та кібербезпеки для протидії викликам та загрозам, досягнення взаємосумісності та взаємодії з країнами – членами НАТО, досвід підготовки та застосування Військ зв'язку та кібербезпеки в ході проведення антитерористичної операції та операції об'єднаних сил на території Донецької та Луганської областей.

Доктрина призначена для органів військового управління, командувань видів, окремих родів військ (сил) ЗС України, командирів (начальників) усіх рівнів виходячи з їх обов'язків щодо організації зв'язку, а також керівного складу та органів управління, частин та підрозділів зв'язку, захисту інформації та кібербезпеки, керівників підрозділів, які відповідають за організацію зв'язку та кібербезпеку у військових частинах.

ДОКТРИНА ВІЙСЬК ЗВ'ЯЗКУ ТА КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ



Видавництво
«Центр учбової літератури»
Київ — 2024

Доктрина зв'язку та кібербезпеки Збройних Сил України. — Київ: «ЦУЛ»,
Д 63 2024. — 48 с.

ISBN 978-611-01-3293-3

Доктрину розроблено робочою групою офіцерів Командування Військ зв'язку та кібербезпеки ЗС України та погоджено із заінтересованими органами військового управління ЗС України та структурними підрозділами Генерального штабу ЗС України.

У Доктрині враховано погляди керівництва ЗС України на те, якими мають бути сучасні Війська зв'язку та кібербезпеки для протидії викликам та загрозам, досягнення взаємосумісності та взаємодії з країнами – членами НАТО, досвід підготовки та застосування Військ зв'язку та кібербезпеки в ході проведення антитерористичної операції та операції об'єднаних сил на території Донецької та Луганської областей.

Доктрина призначена для органів військового управління, командувань видів, окремих родів військ (сил) ЗС України, командирів (начальників) усіх рівнів виходячи з їх обов'язків щодо організації зв'язку, а також керівного складу та органів управління, частин та підрозділів зв'язку, захисту інформації та кібербезпеки, керівників підрозділів, які відповідають за організацію зв'язку та кібербезпеку у військових частинах.

ISBN 978-611-01-3292-3

ЗМІСТ

	ВСТУП	4
	ПОСИЛАННЯ НА ВІЙСЬКОВІ ПУБЛІКАЦІЇ	5
	ОСНОВНІ ТЕРМІНИ ТА ВИЗНАЧЕННЯ	6
	ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ	7
1	ПРИЗНАЧЕННЯ ТА ЗАВДАННЯ ВІЙСЬК ЗВ'ЯЗКУ ТА КІБЕРБЕЗПЕКИ	8
1.1	Війська зв'язку та кібербезпеки ЗС України	8
1.2	Основні завдання Військ зв'язку та кібербезпеки ЗС України	8
2	СТРУКТУРА ТА СКЛАД ВІЙСЬК ЗВ'ЯЗКУ ТА КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ	9
2.1	Загальні положення	9
2.2	Органи військового управління Військ зв'язку та кібербезпеки ЗС України	10
2.3	Військові частини (підрозділи) Військ зв'язку та кібербезпеки ЗС України	22
2.4	Військові навчальні заклади (центри) Військ зв'язку та кібербезпеки ЗС України	35
3	ОРГАНІЗАЦІЯ УПРАВЛІННЯ ВІЙСЬКАМИ ЗВ'ЯЗКУ ТА КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ	35
3.1	Основи організації управління Військами зв'язку та кібербезпеки ЗС України	35
3.2	Організація взаємодії у Військах зв'язку та кібербезпеки ЗС України	39
4	ПІДГОТОВКА ТА ЗАБЕЗПЕЧЕННЯ ВІЙСЬК ЗВ'ЯЗКУ ТА КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ	40
4.1	Підготовка Військ зв'язку та кібербезпеки ЗС України	40
4.2	Логістичне забезпечення Військ зв'язку та кібербезпеки ЗС України	45
4.3	Фінансове та ресурсне забезпечення Військ зв'язку та кібербезпеки ЗС України	46
	ЗАКЛЮЧНА ЧАСТИНА	46
	СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ (ДЖЕРЕЛ)	48

ВСТУП

В умовах збройної агресії з боку Російської Федерації проти нашої держави та реалізації стратегічного курсу держави на приєднання до європейської спільноти, її безпекових структур ЗС України потрібні військові частини (підрозділи), спроможні виконувати завдання із захисту держави, діяти спільно з підрозділами держав – членів НАТО.

Сучасні виклики, які зумовлені переходом провідних країн світу до концепції ведення мережецентричних війн, перенесенням театру воєнних дій у площину кіберпростору, все більше і більше вимагають від особового складу Військ зв'язку та кібербезпеки ЗС України опанування та впровадження новітніх засобів зв'язку та технологій, надання сервісів зв'язку для забезпечення функціонування єдиного інформаційного середовища ЗС України та досягнення оперативної й технічної взаємосумісності з іншими складовими сил оборони та державами – членами НАТО.

Розвиток та широке впровадження систем і комплексів зв'язку з використанням інноваційних інформаційних та телекомунікаційних технологій сприяли появі у 2013 році у військах зв'язку додаткових завдань щодо забезпечення кібербезпеки в інформаційно-телекомунікаційних системах та створення відповідних підрозділів кібербезпеки, які виконують завдання в цій сфері.

Прийнятий керівництвом держави євроатлантичний вектор розвитку спричинив реорганізацію структури управління ЗС України, яка не оминула й Війська зв'язку та кібербезпеки, розділивши функції планування, застосування та генерування сил між Генеральним штабом ЗС України та органами військового управління ЗС України.

Доктрина містить загальні поняття про основні завдання, склад та організацію Військ зв'язку та кібербезпеки ЗС України, особливості їх підготовки, застосування та покликана сформулювати загальне уявлення про Війська зв'язку та кібербезпеки ЗС України серед особового складу ЗС України та інших складових сил оборони.

ПОСИЛАННЯ НА ВІЙСЬКОВІ ПУБЛІКАЦІЇ

Позначка військової публікації	Повне найменування військової публікації
1	2
	Тимчасова доктрина застосування сил оборони держави, затверджена та введена в дію наказом Генерального штабу Збройних Сил України від 31.03.2020 № 124/ДСК
ВКДП 1-003(03).01	Тимчасовий порядок оформлення військових публікацій у Збройних Силах України, затверджений наказом Генерального штабу Збройних Сил України від 26.12.2018 № 460
ВД 7-05(03).01	Доктрина розвитку військових публікацій у Збройних Силах України, затверджена начальником Генерального штабу Збройних Сил України 29.05.2020
ВКП 6-00(01).01	Доктрина “Зв’язок та інформаційні системи”, затверджена Головнокомандувачем Збройних Сил України 01.07.2020
ВКП 7-00(01).01	Доктрина підготовки сил оборони держави, затверджена наказом Генерального штабу Збройних Сил України від 21.01.2020 № 18
ВКДП 6-00(03).01	Доктрина операцій в кіберпросторі, затверджена начальником Генерального штабу ЗС України 30.09.2020, реєстраційний № 198/нвгш/дск
АJP-3.20	Доктрина операцій в кіберпросторі (Allied Joint Doctrine for Cyberspace Operation)
АJP-3.10.2	Доктрина безпеки операцій та приховування (Allied Joint Doctrine for Operations Security and Deception)
SH/CCD J6/SM FCIS/394/15-305978	Deployable Communications and Information Systems Concept of Operations (DCIS CONOPS)
ВСТ 01.112.004 – 2017 (01)	Військовий зв’язок та інформаційні системи. Словник НАТО з систем зв’язку та інформаційних систем (AAP-31 (Edition 3), IDT)
	Опис типових носіїв спроможностей “Спроможності центрів захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах Збройних Сил України щодо дій під час кібероборони України”, затверджений начальником Генерального штабу Збройних Сил України 30.11.2020, реєстраційний № 2812/С/дск

ОСНОВНІ ТЕРМІНИ ТА ВИЗНАЧЕННЯ

Нарощування системи зв'язку та інформаційних систем – заходи, спрямовані на збільшення спроможностей (можливостей) системи зв'язку та інформаційних систем для покращення показників стійкості та живучості системи управління, а також забезпечення послугами зв'язку підрозділів, які розгортаються для виконання завдань за призначенням згідно із ситуацією, що склалася.

Органи управління системою зв'язку та інформаційних систем – сукупність постійних (штатних) і тимчасово створюваних (позаштатних) структурних підрозділів з відповідними повноваженнями щодо організації (управління) зв'язку (-ом), які організаційно і функціонально об'єднані для виконання покладених на них завдань.

Пункт управління системою зв'язку та інформаційних систем – сукупність робочих місць, які розташовані в захищених спорудах, будівлях, тимчасових спорудах або на рухомій базі (командно-штабні (штабні) машини) і призначені для роботи оперативного складу органів управління зв'язком.

Система зв'язку та інформаційних систем Збройних Сил України – одна зі складових системи управління ЗС України, яка становить собою інтегровану сукупність взаємопов'язаних та узгоджених за завданнями телекомунікаційних мереж, інформаційно та інформаційно-телекомунікаційних систем, систем захисту інформації та кібербезпеки, спеціального зв'язку, технічного і криптографічного захисту інформації в інформаційно-телекомунікаційних системах МО України та ЗС України, мережі фельд'єгерсько-поштового зв'язку та системи технічного забезпечення зв'язку та інформаційних систем ЗС України, які розгортаються в МО України та ЗС України з метою забезпечення обміну інформацією в системі управління.

Спроможність (оперативна, бойова, спеціальна) – здатність структурної одиниці (елемента) Збройних Сил (сил оборони) або сукупності сил і засобів виконувати певні завдання (забезпечувати реалізацію визначених військових цілей) за певних умов обстановки, ресурсного забезпечення та відповідно до встановлених стандартів.

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

Скорочення та умовні позначення	Повне словосполучення та поняття, що скорочуються
1	2
МО України	Міністерство оборони України
ГШ ЗС України	Генеральний штаб Збройних Сил України
ЗС України	Збройні Сили України
СВ ЗС України	Сухопутні війська Збройних Сил України
ПС ЗС України	Повітряні Сили Збройних Сил України
ВМС ЗС України	Військово-Морські Сили Збройних Сил України
ССО ЗС України	Сили спеціальних операцій Збройних Сил України
ДШВ ЗС України	Десантно-штурмові війська Збройних Сил України
ВЗ та КБ ЗС України	Війська зв'язку та кібербезпеки Збройних Сил України
ЦУЗ та ІС ГШ ЗС України	Центральне управління зв'язку та інформаційних систем (J6) Генерального штабу Збройних Сил України
ОВУ	Орган військового управління
ОУСЗ та ІС	Орган управління системою зв'язку та інформаційних систем
КВЗ та КБ ЗС України	Командування Військ зв'язку та кібербезпеки Збройних Сил України
ІТС	Інформаційно-телекомунікаційні системи
ГІТВ	Головний інформаційно-телекомунікаційний вузол
ІТВ	Інформаційно-телекомунікаційний вузол
ПУЗ та КБ	Пункт управління зв'язком та кібербезпекою
ФПЗ	Фельд'єгерсько-поштовий зв'язок
СУ	Система управління
ОВТ	Озброєння та військова техніка
РТЗ	Радіотехнічне забезпечення
METL	“Mission-essentialtasklist”. Перелік навчально-бойових завдань
MET	“Mission-essentialtask” Каталог завдань

1. ПРИЗНАЧЕННЯ ТА ЗАВДАННЯ ВІЙСЬК ЗВ'ЯЗКУ ТА КІБЕРБЕЗПЕКИ

1.1. Війська зв'язку та кібербезпеки ЗС України

ВЗ та КБ ЗС України – спеціальні війська, призначені для планування та забезпечення розгортання, згортання, функціонування системи зв'язку та інформаційних систем, систем бойового управління та оповіщення, їх нарощування в мирний час, в особливий період, в умовах надзвичайного та воєнного стану з метою вирішення завдань забезпечення управління військами (силами) ЗС України, а також здійснення заходів з функціонування національної системи кібербезпеки та відбиття воєнної агресії у кіберпросторі (кібероборони). Частини та підрозділи ВЗ та КБ ЗС України входять до складу всіх видів та окремих родів військ, сил ЗС України.

1.2. Основні завдання Військ зв'язку та кібербезпеки ЗС України

Основними завданнями ВЗ та КБ ЗС України є:

- організація планування розгортання та нарощування, забезпечення функціонування системи зв'язку та інформаційних систем, систем бойового управління та оповіщення в мирний час, в особливий період, в умовах надзвичайного та воєнного стану;

- організація взаємодії з іншими складовими сил оборони, Національним центром оперативно-технічного управління телекомунікаційними мережами України та операторами електронних комунікацій (операторами зв'язку) з питань забезпечення зв'язком у ході виконання спільних завдань з оборони держави;

- створення (розгортання) єдиного інформаційного середовища ЗС України з використанням сервісно-орієнтованої архітектури;

- надання сервісів зв'язку для забезпечення функціонування єдиного інформаційного середовища ЗС України та досягнення оперативної й технічної взаємосумісності з іншими складовими сил оборони та держав – членів НАТО;

- забезпечення обміну інформацією в єдиному інформаційному середовищі ЗС України;

- надання оперативному складу пунктів управління ЗС України, а також іншим складовим сил оборони базових та функціональних сервісів через їх відповідні точки присутності;

- здійснення заходів з функціонування національної системи кібербезпеки; участь у заходах з кібероборони;

- ведення та/або участь у кіберопераціях, ведення кібердій;

- організація та керівництво технічним забезпеченням зв'язку у ЗС України;

- здійснення військової співпраці зі збройними силами країн – членів НАТО щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз;

- впровадження заходів із забезпечення кіберзахисту критичної

участь у заходах міжнародного співробітництва та миротворчих операціях.
При виконанні завдань із забезпечення функціонування системи зв'язку та інформаційних систем ураховуються такі принципи та підходи:

єдиначальності та персональної відповідальності начальників зв'язку, командирів військових частин (підрозділів) зв'язку, кібербезпеки за результати виконання поставлених завдань;

централізації управління з наданням підлеглим розумної ініціативи та самостійності у визначенні способів виконання поставлених завдань;

твердості та наполегливості в ході реалізації замислів і планів;

чіткого розподілу функцій, завдань, повноважень і відповідальності між структурними підрозділами органів військового управління, що здійснюють управління системою зв'язку та інформаційних систем, та ВЗ та КБ ЗС України;

реальності визначених завдань військовим частинам (підрозділам) зв'язку, кібербезпеки та відповідності їх можливостям;

урахування та раціонального використання наявних сил і засобів, комплексів зв'язку;

єдності і комплексності замислів і планів під час їх розробки, виконання та контролю;

раціональності, гнучкості та адаптивності планів.

2. СТРУКТУРА ТА СКЛАД ВІЙСЬК ЗВ'ЯЗКУ ТА КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

2.1. Загальні положення

2.1.1. Суб'єктами ВЗ та КБ ЗС України є: ОВУ, структурні підрозділи ОВУ, військові частини (підрозділи), військові навчальні заклади. Чисельність ВЗ та КБ ЗС України визначається Головнокомандувачем ЗС України та утримується в межах чисельності ЗС України.

Органи управління ВЗ та КБ ЗС України мають таку загальну структуру:

ЦУЗ та ІС ГШ ЗС України;

КВЗ та КБ ЗС України з підпорядкованими йому військовими частинами та військовими навчальними закладами;

центр зв'язку та інформаційних систем Командування об'єднаних сил ЗС України;

управління зв'язку та інформаційних систем штабу Командування СВ ЗС України з підпорядкованими управліннями зв'язку та інформаційних систем оперативних командувань, командування територіальної оборони, військовими частинами (підрозділами) зв'язку;

управління зв'язку та інформаційних систем штабу Командування ПС ЗС України з підпорядкованими відділами зв'язку та інформаційних систем повітряних командувань, військовими частинами (підрозділами) зв'язку та радіотехнічного забезпечення;

управління зв'язку та інформаційних систем штабу Командування ВМС ЗС України з підпорядкованими відділами зв'язку та інформаційних систем командування морської піхоти та морського командування, військовими частинами (підрозділами) зв'язку;

управління зв'язку та інформаційних систем штабу Командування ДШВ ЗС України з підпорядкованими військовими частинами (підрозділами) зв'язку;

управління зв'язку та інформаційних систем штабу Командування ССО ЗС України з підпорядкованими військовими частинами (підрозділами) зв'язку;

група зв'язку та інформаційних систем штабу Командування Сил підтримки ЗС України з підпорядкованими військовими частинами (підрозділами) зв'язку;

управління зв'язку та інформаційних систем штабу Командування Сил логістики ЗС України з підпорядкованими військовими частинами (підрозділами) зв'язку;

відділ зв'язку медичних інформаційних систем та кібербезпеки штабу Командування Медичних сил ЗС України з підпорядкованими підрозділами зв'язку.

2.1.2. ОВУ (структурні підрозділи ОВУ), військові частини (підрозділи), військові навчальні заклади дислокуються на території держави або тимчасово за її межами відповідно до завдань оборони, стратегічного плану застосування і завдань ЗС України з урахуванням військово-адміністративного поділу території України.

2.2. Органи військового управління Військ зв'язку та кібербезпеки ЗС України

2.2.1. ОВУ (структурні підрозділи ОВУ) ВЗ та КБ ЗС України наділені відокремленими повноваженнями щодо виконання функцій планування застосування наявних сил і засобів зв'язку в операціях (бойових діях), застосування частин та підрозділів ВЗ та КБ ЗС України, їх підготовки та генерації.

2.2.2. Функції стратегічного планування застосування ВЗ та КБ ЗС України та інших складових сил оборони за напрямом “зв'язок та інформаційні системи” відповідно до сценаріїв виникнення та розвитку ситуацій воєнного характеру, планування кібероборони держави, планування та контролю функціонування системи захисту інформації та кібербезпеки в ІТС МО України та ЗС України покладено на Центральне управління зв'язку та інформаційних систем (ІБ), яке є структурним підрозділом Генерального штабу ЗС України.

Крім цього, на ЦУЗ та ІС ГШ ЗС України покладено такі основні функції: планування, організація розгортання та забезпечення функціонування системи управління військами та зв'язку згідно зі Стратегічним планом застосування ЗС України та інших складових сил оборони:

організація забезпечення інформаційної безпеки та захисту в інформаційних технічних системах;

розроблення доктрин, наказів, концепцій, інших нормативно-правових актів та документів з питань організації та функціонування комунікаційних та інформаційних систем у ЗС України;

організація прихованого управління військами (силами).

Реалізація завдань з планування зв'язку у ході стратегічного планування застосування ЗС України досягається виконанням базових, основних та додаткових вимог, що ставляться до носія спроможностей за унікальним кодом CIS-1.1.1, а з питань планування кібербезпеки та кіберзахисту у ході стратегічного планування застосування ЗС України досягається виконанням базових, основних та додаткових вимог, що ставляться до носія спроможностей за унікальним кодом CIS-1.9.1. Крім цього, реалізація завдань з регулювання і розподілу радіочастотного ресурсу в інтересах ЗС України, інших спеціальних користувачів досягається виконанням базових, основних та додаткових вимог, що ставляться до носія спроможностей за унікальним кодом CIS-1.3.1.

Центральне управління зв'язку та інформаційних систем (J6) Генерального штабу ЗС України підпорядковується начальнику Генерального штабу ЗС України.

2.2.3. Функції з підготовки та генерації ВЗ та КБ здійснює Командування Військ зв'язку та кібербезпеки ЗС України, яке є органом військового управління ЗС України і призначене для:

реалізації завдань з організації та забезпечення функціонування стаціонарної телекомунікаційної системи зв'язку, на базі якої функціонують інформаційні системи ЗС України та системи стаціонарних інформаційно-телекомунікаційних вузлів, поєднаних між собою каналами зв'язку, їх нарощування в мирний час та особливий період, в умовах надзвичайного та воєнного стану;

підготовки та підтримання в готовності до виконання покладених завдань польової системи зв'язку;

підтримання в постійній бойовій і мобілізаційній готовності частин та підрозділів ВЗ та КБ безпосереднього підпорядкування;

виконання заходів з підготовки держави до оборони та відбиття воєнної загрози в кіберпросторі (кібероборони).

Крім цього, КВЗ та КБ ЗС України формує вимоги до:

підготовки ВЗ та КБ;

розвитку ВЗ та КБ, визначає найбільш оптимальну за критерієм “ефективність – вартість” перспективну модель ВЗ та КБ, їх технічне оснащення та всебічне забезпечення;

необхідних (критичних) спроможностей ВЗ та КБ ЗС України.

КВЗ та КБ ЗС України реалізовує завдання щодо:

забезпечення взаємусумісності ІТС у рамках виконання базових, основних та додаткових вимог, що ставляться до носія спроможностей за унікальним

забезпечення кібербезпеки в інформаційно-телекомунікаційних системах ЗС України у рамках виконання базових, основних та додаткових вимог, що ставляться до носіїв спроможностей за унікальним кодом CIS-1.2.5;

організації фельд'єгерсько-поштового зв'язку ЗС України в рамках виконання базових, основних та додаткових вимог, що ставляться до носіїв спроможностей за унікальним кодом CIS-1.4.1;

здійснення кіберрозвідки, аналізу, прогнозування та оцінки обстановки в кіберпросторі, кібердорозвідки в рамках виконання базових, основних та додаткових вимог, що ставляться до носіїв спроможностей за унікальним кодом Е-3.3.1;

здійснення підготовки та проведення заходів кібербезпеки та кіберзахисту в ІТС МО України та ЗС України в рамках виконання базових, основних та додаткових вимог, що ставляться до носіїв спроможностей за унікальним кодом Е-3.3.2;

здійснення підготовки та проведення кібердій і кібервпливів в ІТС противника в рамках виконання базових, основних та додаткових вимог, що ставляться до носіїв спроможностей за унікальним кодом Е-3.3.3.

Крім цього, КВЗ та КБ ЗС України здійснює заходи щодо:

забезпечення функціонування стаціонарної телекомунікаційної системи зв'язку ЗС України, систем спеціального зв'язку, системи центрального бойового управління та оповіщення, системи захисту інформації та кібербезпеки в ІТС ЗС України, їх нарощування в мирний час та особливий період, в умовах надзвичайного та воєнного стану;

взаємодії з Національним центром оперативно-технічного управління телекомунікаційними мережами України та операторами електронних комунікацій (операторами зв'язку) з питань забезпечення послугами зв'язку у повсякденній діяльності ЗС України, планування послуг зв'язку на особливий період та формування мобілізаційного завдання операторам електронних комунікацій (операторам зв'язку);

моніторингу стану та управління системою зв'язку та інформаційних систем, систем спеціального зв'язку, системи захисту інформації та кібербезпеки;

короткострокового оборонного планування системи зв'язку та інформаційних систем ЗС України на основі спроможностей ВЗ та КБ ЗС України;

участі у здійсненні заходів з кібероборони держави;

організації технічного забезпечення зв'язку у ЗС України.

Командування Військ зв'язку та кібербезпеки ЗС України підпорядковується Головнокомандувачу ЗС України.

2.2.4. Функції планування застосування переданих в оперативне підпорядкування комплекту ВЗ та КБ у найбільш ефективний спосіб та уточнення вимог до наявних спроможностей, а також управління частинами (підрозділами) зв'язку, що входить до складу мікророзвідки, мінімізацію

Книги, які можуть вас зацікавити



Виконання заходів радіо-, радіотехнічного контролю окремим спеціальним центром радіоелектронної боротьби (окремим вузлом радіоелектронної боротьби)...



Бойова робота підрозділів оптичної та оптико-електронної розвідки ракетних військ і артилерії Збройних Сил України



[Перейти на сайт](#) →