**НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ**
**ІМЕНІ БОГДАНА ХМЕЛЬНИЦЬКОГО**

кафедра телекомунікаційних та інформаційних систем факультету забезпечення оперативно-службової діяльності

# СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
# ООК 14 «ОРГАНІЗАЦІЯ ЗВ'ЯЗКУ»
**(обов`язкова освітня компонента)**
# ОПП 262 «Правоохоронна діяльність»

**Рівень вищої освіти:** другий (магістерський)
**Галузь знань:** 26 Цивільна безпека
**Спеціальність:** 262 Правоохоронна діяльність
**Кваліфікація:** магістр правоохоронної діяльності
**Професійна кваліфікація**: офіцер оперативно-тактичного рівня Державної прикордонної служби України
**Форма здобуття освіти:** денна

**АНОТАЦІЯ КУРСУ**

Навчальна дисципліна **«Організація зв'язку»**, входить до обов'язкової освітньої компоненти ОПП «Правоохоронна діяльність» і вивчається на другому (магістерському) рівні у галузі знань 26 Цивільна безпека зі спеціальності 262 Правоохоронна діяльність.

**ТРИВАЛІСТЬ КУРСУ**

**Метою вивчення навчальної дисципліни є** підготовка офіцера-прикордонника за другим (магістерським) рівнем вищої освіти, за спеціальністю 262 «Правоохоронна діяльність», який знає засоби зв'язку і автоматизації тактичного та оперативно-тактичного рівнів управління, вміє технічно грамотно їх експлуатувати, забезпечуючи приховане управління та заходи технічного захисту інформації, що циркулює в інформаційно-телекомунікаційних системах; здійснювати керівництво зв'язком; організовувати зв'язок в повсякденних умовах оперативно-службової діяльності (ОСД), при загострені обстановки, в умовах надзвичайного стану, особливий період, в умовах загрози застосування воєнної сили з боку інших держав, з дотриманням вимог безпеки зв'язку.

**Завданням навчальної дисципліни** є формування у офіцера-прикордонника за другим (магістерським) рівнем вищої освіти, за спеціальністю 262 «Правоохоронна діяльність» відповідних програмних компетентностей, достатніх для виконання функціональних обов'язків за відповідними посадами.

Вивчення навчальної дисципліни забезпечує формування у слухачів наступних **програмних компетентностей**:

**А) загальні компетентності:**

**ЗК 2** Здатність застосовувати знання у практичних ситуаціях в умовах неповної/недостатньої інформації, суперечливих вимог та зміни умов обстановки;

**ЗК 8** Здатність приймати обґрунтовані рішення в складних і непередбачуваних умовах;

**ЗК 10** Здатність оцінювати та забезпечувати якість виконувати робіт у правоохоронній сфері.

**Б) Спеціальні (фахові, предметні) компетентності:**

**СК 6** Здатність керувати самостійною роботою осіб, що навчаються, та бути наставником для молодших колег у процесі набуття і вдосконалення ними професійних навичок;

**СК 9** Здатність обирати оптимальні методи й засоби забезпечення публічної безпеки і порядку;

**СК 10** Здатність аналізувати, оцінювати й застосовувати сучасні інформаційні технології під час вирішення професійних (наукових) завдань, формувати та застосовувати сучасні системи підтримки прийняття рішень;

**СК 11** Здатність взаємодіяти з представниками інших органів виконавчої влади та місцевого самоврядування, громадськістю з питань правоохоронної діяльності та здатність до діяльності в системі інтегрованого управління кордонами;

**СК 12** Здатність до використання технічних приладів та спеціальних засобів, інформаційно-пошукової систем та баз даних, спеціальної техніки, оперативних та оперативно-технічних засобів, організації та здійснення оперативно-розшукової діяльності для

підтримки процесів прийняття рішень щодо запобігання, протидії та нейтралізації загроз прикордонній безпеці на рівні органу охорони державного кордону).

Вивчення навчальної дисципліни забезпечує досягнення слухачами наступних **програмних результатів навчання**:

**ПРН 4** Узагальнювати практичні результати роботи і пропонувати нові рішення, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів;

**ПРН 8** Забезпечувати законність та правопорядок, захист прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов'язків;

**ПРН 9** Використовувати у професійній діяльності сучасні інформаційні технології, бази даних та стандартне і спеціалізоване програмне забезпечення оперативно-службової діяльності органів Державної прикордонної служби України;

**ПРН 10** Користуватися державної системою урядового зв'язку, Національною системою конфіденційного зв'язку, формування та реалізації державної політики у сферах кібербезпеки критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку;

**ПРН 15** Модифікувати основні методи та засоби забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку;

**ПРН 17** Розуміти основи забезпечення національної безпеки, особливості застосування спеціальних засобів (вогнепальної зброї, спеціальний засобів, засобів фізичної сили); технології захисту даних, методи обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (у тому числі міжвідомчі та міжнародні); оперативні та оперативно-технічні засоби, здійснення оперативно-розшукової діяльності) в повсякденних умовах та під час бойових дій.

Досягнення програмних результатів навчання передбачає здатність демонструвати знання, розуміння, застосування, аналіз, синтез та оцінювання його складових.

**ПРН 4** Узагальнювати практичні результати роботи і пропонувати нові рішення, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів;

Знання: практичних результатів роботи і нових рішень, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів.

Розуміння: практичних результатів роботи і нових рішень, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів.

Застосування: практичних результатів роботи і нових рішень, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів.

Аналіз: результатів роботи і нових рішень, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів.

Синтез: нових рішень, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів.

Оцінка: практичних результатів роботи і нових рішень, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів.

**ПРН 8** Забезпечувати законність та правопорядок, захист прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов'язків.

Знання: шляхів забезпечення законності та правопорядку, захисту прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов'язків.

Розуміння: шляхів забезпечення законності та правопорядку, захисту прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов'язків.

Застосування: шляхів забезпечення законності та правопорядку, захисту прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов'язків.

Аналіз: шляхів забезпечення законності та правопорядку, захисту прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов'язків.

Синтез: шляхів забезпечення законності та правопорядку, захисту прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов'язків.

Оцінка: забезпечення законності та правопорядку, захисту прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов'язків.

**ПРН 9** Використовувати у професійній діяльності сучасні інформаційні технології, бази даних та стандартне і спеціалізоване програмне забезпечення оперативно-службової діяльності органів Державної прикордонної служби України.

Знання: сучасних інформаційних технологій, баз даних та стандартного і спеціалізованого програмного забезпечення оперативно-службової діяльності органів Державної прикордонної служби України.

Розуміння: сучасних інформаційних технологій, баз даних та стандартного і спеціалізованого програмного забезпечення оперативно-службової діяльності органів Державної прикордонної служби України.

Застосування: – сучасних інформаційних технологій, баз даних та стандартного і спеціалізованого програмного забезпечення оперативно-службової діяльності органів Державної прикордонної служби України.

Аналіз: використання у професійній діяльності сучасних інформаційних технологій, баз даних та стандартного і спеціалізованого програмного забезпечення оперативно-службової діяльності органів Державної прикордонної служби України.

Синтез: напрямків використання у професійній діяльності сучасних інформаційних технологій, баз даних та стандартного і спеціалізованого програмного забезпечення оперативно-службової діяльності органів Державної прикордонної служби України.

Оцінка: ефективності використання у професійній діяльності сучасних інформаційних технологій, баз даних та стандартного і спеціалізованого програмного забезпечення оперативно-службової діяльності органів Державної прикордонної служби України.

**ПРН 10** Користуватися державної системою урядового зв'язку, Національною системою конфіденційного зв'язку, формування та реалізації державної політики у сферах кібербезпеки критичної інформаційної інфраструктури, державних інформаційних ресурсів та

інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку.

Знання: основ користування державною системою урядового зв'язку, Національною системою конфіденційного зв'язку, формування та реалізації державної політики у сферах кібербезпеки критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку.

Розуміння: особливостей користування державною системою урядового зв'язку, Національною системою конфіденційного зв'язку, формування та реалізації державної політики у сферах кібербезпеки критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку.

Застосування: державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кібербезпеки критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку.

Аналіз: шляхів застосування державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кібербезпеки критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку.

Синтез: формування та реалізації державної політики у сферах кібербезпеки критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку.

Оцінка: ефективності застосування державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кібербезпеки критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку.

**ПРН 15** Модифікувати основні методи та засоби забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку.

Знання: основних методів та засобів забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку.

Розуміння: основні методи та засоби забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку.

Застосування: основні методи та засоби забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку.

Аналіз: основні методи та засоби забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку.

Синтез: основні методи та засоби забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку.

Оцінка: ефективності основних методів та засобів забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку.

**ПРН 17** Розуміти основи забезпечення національної безпеки, особливості застосування спеціальних засобів (вогнепальної зброї, спеціальний засобів, засобів фізичної сили); технології захисту даних, методи обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (у тому числі міжвідомчі та міжнародні); оперативні та оперативно-технічні засоби, здійснення оперативно-розшукової діяльності) в повсякденних умовах та під час бойових дій.

Знання: основ забезпечення національної безпеки, особливостей застосування спеціальних засобів (вогнепальної зброї, спеціальний засобів, засобів фізичної сили); технологій захисту даних, методів обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (у тому числі міжвідомчі та міжнародні); оперативних та оперативно-технічних засобів, здійснення оперативно-розшукової діяльності) в повсякденних умовах та під час бойових дій.

Розуміння: основ забезпечення національної безпеки, особливостей застосування спеціальних засобів (вогнепальної зброї, спеціальний засобів, засобів фізичної сили); технологій захисту даних, методів обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (у тому числі міжвідомчі та міжнародні); оперативних та оперативно-технічних засобів, здійснення оперативно-розшукової діяльності) в повсякденних умовах та під час бойових дій.

Застосування: спеціальних засобів (вогнепальної зброї, спеціальний засобів, засобів фізичної сили); технологій захисту даних, методів обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (у тому числі міжвідомчі та міжнародні); оперативних та оперативно-технічних засобів, здійснення оперативно-розшукової діяльності) в повсякденних умовах та під час бойових дій.

Аналіз: особливостей застосування спеціальних засобів (вогнепальної зброї, спеціальний засобів, засобів фізичної сили); технологій захисту даних, методів обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (у тому числі міжвідомчі та міжнародні); оперативних та оперативно-технічних засобів, здійснення оперативно-розшукової діяльності) в повсякденних умовах та під час бойових дій.

Синтез: основ забезпечення національної безпеки, особливостей застосування спеціальних засобів (вогнепальної зброї, спеціальний засобів, засобів фізичної сили); технологій захисту даних, методів обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (у тому числі міжвідомчі та міжнародні); оперативних та оперативно-технічних засобів, здійснення оперативно-розшукової діяльності) в повсякденних умовах та під час бойових дій.

Оцінка: основ забезпечення національної безпеки, особливостей застосування спеціальних засобів (вогнепальної зброї, спеціальний засобів, засобів фізичної сили); технологій захисту даних, методів обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (у тому числі міжвідомчі та міжнародні); оперативних та оперативно-технічних засобів, здійснення оперативно-розшукової діяльності) в повсякденних умовах та під час бойових дій.

**ВИКЛАДАЧІ:**

доцент кафедри телекомунікаційних та інформаційних систем кандидат технічних наук, доцент полковник Євгеній ПРОКОПЕНКО, e-mail: mydocent@gmail.com;

доцент кафедри телекомунікаційних та інформаційних систем кандидат технічних наук, доцент полковник Дмитро МУЛ.

**ПЕРЕДУМОВИ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ.**

Діяльність штабів ДПСУ та ЗСУ, Оперативно-службова діяльність ДПСУ.

**МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ.**

Модернізована спеціальна комплексна інформаційно-телекомунікаційна апаратна «СКІТА -04», рухомий ПТК АПК «Гарт-1/П», мобільний комплект супутникового зв'язку, УКХ радіосистеми сімейства «Mototrbo», УКХ радіоретранслятор «Mototrbo», УКХ та КХ радіосистеми сімейства «Harris», Комутатори П-193м2, телефонні апарати ТА-57.

Програмне забезпечення: Cisco Packet Tracer, Communications Planning Application.

## ТРИВАЛІСТЬ ТА ОРГАНІЗАЦІЯ КУРСУ

| Курс | Семестр | Кількість кредитів ЄКТС | Кількість годин | | | | | | | | | | | | | | | | | | | | Форми підсумкового контролю | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Загальна | Усього аудиторних занять | Аудиторна робота | | | | | | | | | | | Індивідуальна робота | | | | | | | | Самостійна робота | | | |
| | | | | | лекції | групові заняття | групові вправи | практичні заняття | лабораторні заняття | семінари | рольові ігри | контрольна робота | індивідуальні заняття | модульний контроль | підсумковий контроль | Усього | реферат | конспект з теми | переклад текстів | розрахункове завдання | курсова робота | контрольна робота | модульний контроль | | Екзамен | Диференційований залік | Залік |
| 1 | 2 | 2 | **61** | **34** | 2 | 16 | 2 | 12 | | | | | | | | **5** | | | | 5 | | | | **22** | | | |
| 2 | 3 | 1 | **29** | **16** | | 4 | 2 | 4 | | 4 | | | | | 4 | **5** | 5 | | | | | | | **8** | | + | |
| **Усього за дисципліну** | | **3** | **90** | **50** | **2** | **20** | **4** | **16** | | **4** | | | | | **4** | **10** | **5** | | | **5** | | | | **30** | | **+** | |

**Основні методи навчання:** МН 1.1; МН 1.2; МН 1.4; МН1.5; МН 2.2; МН2.3; МН3.1
**Основні методи контролю навчальних досягнень:** МК1.1; МК1.3; МК2.1; МК2.3; МК2.4; МК2.8; МК3.2; МК4.1; МК4.3; МК4.4

## КОМПЕТЕНТНОСТІ ТА КОНТРОЛЬ РІВНЯ ЇХ ДОСЯГНЕННЯ СЛУХАЧАМИ

| Шифр | Компетентність | Методи контролю |
|---|---|---|
| **Загальні компетентності** | | |
| ЗК-2 | Здатність застосовувати знання у практичних ситуаціях в умовах неповної/недостатньої інформації, суперечливих вимог та зміни умов обстановки. | МК 1.1, МК 1.4, МК 1.6, МК 2.1, МК 2.4, МК 2.6, МК 2.8, МК 2.10, МК 3.2, МК 3.5, МК 4.3, МК 4.5 |
| ЗК-8 | Здатність приймати обґрунтовані рішення в складних і непередбачуваних умовах. | МК 1.1, МК 1.4, МК 1.6, МК 2.1, МК 2.4, МК 2.6, МК 2.8, МК 2.10, МК 3.2, МК 3.5, МК 4.3, МК 4.5 |
| ЗК-10 | Здатність оцінювати та забезпечувати якість виконувати робіт у правоохоронній сфері. | МК 1.1, МК 1.4, МК 1.6, МК 2.1, МК 2.4, МК 2.6, МК 2.8, МК 2.10, МК 3.2, МК 3.5, МК 4.3, МК 4.5 |
| **Спеціальні (фахові, предметні) компетентності** | | |
| СК-6 | Здатність керувати самостійною роботою осіб, що навчаються, та бути наставником для молодших колег у процесі набуття і вдосконалення ними професійних навичок. | МК 1.1, МК 1.4, МК 1.6, МК 2.1, МК 2.4, МК 2.6, МК 2.8, МК 2.10, МК 3.2, МК 3.5, МК 4.3, МК 4.5 |
| СК-9 | Здатність обирати оптимальні методи й засоби забезпечення публічної безпеки і порядку. | МК 1.1, МК 1.4, МК 1.6, МК 2.1, МК 2.4, МК 2.6, МК 2.8, МК 2.10, МК 3.2, МК 3.5, МК 4.3, МК 4.5 |
| СК-10 | Здатність аналізувати, оцінювати й застосовувати сучасні інформаційні технології під час вирішення професійних (наукових) завдань, формувати та застосовувати сучасні системи підтримки прийняття рішень. | МК 1.1, МК 1.4, МК 1.6, МК 2.1, МК 2.4, МК 2.6, МК 2.8, МК 2.10, МК 3.2, МК 3.5, МК 4.3, МК 4.5 |
| СК-11 | Здатність взаємодіяти з представниками інших органів виконавчої влади та місцевого самоврядування, громадськістю з питань правоохоронної діяльності та здатність до діяльності в системі інтегрованого управління кордонами. | МК 1.1, МК 1.4, МК 1.6, МК 2.1, МК 2.4, МК 2.6, МК 2.8, МК 2.10, МК 3.2, МК 3.5, МК 4.3, МК 4.5 |
| СК-12 | Здатність до використання технічних приладів та спеціальних засобів, інформаційно-пошукової систем та баз даних, спеціальної техніки, | МК 1.1, МК 1.4, МК 1.6, МК 2.1, МК 2.4, МК 2.6, МК 2.8, МК 2.10, |

| Шифр | Компетентність | Методи контролю |
|---|---|---|
| | оперативних та оперативно-технічних засобів, організації та здійснення оперативно-розшукової діяльності для підтримки процесів прийняття рішень щодо запобігання, протидії та нейтралізації загроз прикордонній безпеці на рівні органу охорони державного кордону). | МК 3.2, МК 3.5, МК 4.3, МК 4.5 |

## ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ, МЕТОДИ НАВЧАННЯ ТА КОНТРОЛЬ РІВНЯ ЇХ ДОСЯГНЕННЯ СЛУХАЧАМИ

| Шифр | Компетентність | Методи навчання | Оцінювання |
|---|---|---|---|
| ПРН-4 | Узагальнювати практичні результати роботи і пропонувати нові рішення, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів. | МН 1.1, МН.1.2, МН.1.3, МН.1.4, МН.1.5, МН.2.1, МН.2.3, МН.3.1, МН.3.3. | МК 1.1, МК 1.2, МК 1.3, МК 2.1, МК 2.4, МК 2.8, МК 2.10, МК 3.1, МК 3.2, МК 3.5, МК 4.3, МК 4.5 |
| ПРН-8 | Забезпечувати законність та правопорядок, захист прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов’язків. | МН 1.1, МН.1.2, МН.1.3, МН.1.4, МН.1.5, МН.2.1, МН.2.3, МН.3.1, МН.3.3. | МК 1.1, МК 1.2, МК 1.3, МК 2.1, МК 2.4, МК 2.8, МК 2.10, МК 3.1, МК 3.2, МК 3.5, МК 4.3, МК 4.5 |
| ВРН-9 | Використовувати у професійній діяльності сучасні інформаційні технології, бази даних та стандартне і спеціалізоване програмне забезпечення оперативно-службової діяльності органів Державної прикордонної служби України. | МН 1.1, МН.1.2, МН.1.3, МН.1.4, МН.1.5, МН.2.1, МН.2.3, МН.3.1, МН.3.3. | МК 1.1, МК 1.2, МК 1.3, МК 2.1, МК 2.4, МК 2.8, МК 2.10, МК 3.1, МК 3.2, МК 3.5, МК 4.3, МК 4.5 |
| ВРН-10 | Користуватися державної системою урядового зв’язку, Національною системою конфіденційного зв’язку, формування та | МН 1.1, МН.1.2, МН.1.3, МН.1.4, МН.1.5, МН.2.1, МН.2.3, МН.3.1, МН.3.3. | МК 1.1, МК 1.2, МК 1.3, МК 2.1, МК 2.4, МК 2.8, МК 2.10, МК 3.1, МК 3.2, МК 3.5, МК 4.3, МК 4.5 МК 1.1, МК 1.2, МК 1.3, МК 2.1, МК 2.4, МК 2.8, МК |

| Шифр | Компетентність | Методи навчання | Оцінювання |
|---|---|---|---|
| | реалізації державної політики у сферах кібербезпеки критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку | | 2.10, МК 3.1, МК 3.2, МК 3.5, МК 4.3, МК 4.5 |
| ВРН-15 | Модифікувати основні методи та засоби забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку | МН 1.1, МН.1.2, МН.1.3, МН.1.4, МН.1.5, МН.2.1, МН.2.3, МН.3.1, МН.3.3. | МК 1.1, МК 1.2, МК 1.3, МК 2.1, МК 2.4, МК 2.8, МК 2.10, МК 3.1, МК 3.2, МК 3.5, МК 4.3, МК 4.5 |
| ВРН-17 | Розуміти основи забезпечення національної безпеки, особливості застосування спеціальних засобів (вогнепальної зброї, спеціальний засобів, засобів фізичної сили); технології захисту даних, методи обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (у тому числі міжвідомчі та міжнародні); оперативні та оперативно-технічні засоби, здійснення оперативно-розшукової діяльності) в повсякденних умовах та під час бойових дій | МН 1.1, МН.1.2, МН.1.3, МН.1.4, МН.1.5, МН.2.1, МН.2.3, МН.3.1, МН.3.3. | МК 1.1, МК 1.2, МК 1.3, МК 2.1, МК 2.4, МК 2.8, МК 2.10, МК 3.1, МК 3.2, МК 3.5, МК 4.3, МК 4.5 |

## ОРГАНІЗАЦІЯ НАВЧАННЯ

| № теми | Найменування тем | Кількість годин | Номери, вид занять та кількість годин | | | | | | | | | | Місяць | Номери тем, занять, вид занять, кількість годин | Кіль-кість годин |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | | |
| 1. | Зв’язок, як основа управління | **8** | **Л2** | **Гз2** | **Пз4** | | | | | | | | **1 курс** | | |
| | | | | | | | | | | | | | ***2семестр*** | | |
| | | | | | | | | | | | | | 01 | 1/1Л(2); 2/1Гз(2); 2/2Пз(4) | 8 |
| 2. | Зв’язок в органі охорони державного кордону | **10** | **Гз2** | **Гз2** | **Гз2** | **Гз2** | **Гв2** | | | | | | 02 | 3/1Гз(2); 3/2Гз(2); 3/3Гз(2), | 6 |
| 3. | Зв’язок в загальновійськових з’єднаннях | **6** | **Гз2** | **Гз2** | **Гв2** | | | | | | | | 04 | 3/4Гз(2); 3/5Гв(2), 4/1Гз(2), 4/2Пз(4); | 10 |
| | | | | | | | | | | | | | 05 | 4/3Пз(4); 5/1Гз(2), 5/2Пз(2) | 8 |
| 4. | Інформаційно-телекомунікаційні системи | **4** | **Гз2** | **Пз2** | | | | | | | | | 06 | 6/1Гз(2) | 2 |
| | | | | | | | | | | | | | ***Разом за 3 семестр*** | | **34** |
| 5. | Безпека зв’язку та захист інформації в інформаційних системах | **18** | **Гз2** | **Пз4** | **Гз2** | **Пз6** | **Сз** | | | | | | 09 | 5/3Гз(2), | 2 |
| | | | | | | | | | | | | | 10 | 5/4Пз(6), | 6 |
| | | | | | | | | | | | | | 11 | 5/5Сз(4) | 4 |
| | | | | | | | | | | | | | 12 | Дз(4) | 4 |
| Диференційований залік | | **4** | | | | | | | | | | | | | |
| | | | | | | | | | | | | | ***Разом за 3 семестр*** | | **16** |
| | | | | | | | | | | | | | ***Всього за дисципліну*** | | **50** |

## ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

| № теми | № заняття | Види навчальних занять, завдань | Кількість годин | Найменування теми і навчальні питання | Література |
|---|---|---|---|---|---|
| **1 курс** | | | | | |
| **2 семестр** | | | | | |
| **1** | | | **16** | **ЗВ’ЯЗОК, ЯК ОСНОВА УПРАВЛІННЯ** | |
| | 1 | лекція | 2 | ***Введення в навчальну дисципліну «Організація зв’язку»***<br>1. Мета і завдання дисципліни.<br>2. Основні поняття та терміни в галузі зв’язку.<br>3. Класифікація засобів і комплексів зв'язку, що використовуються у ДПСУ та їх характеристика. Основні поняття системи зв’язку. | [1.1] [1.2] [1.3] [1.8] [2.1]с.5-25 [2.2]с.4-7 |

| | | | | | |
|---|---|---|---|---|---|
| | *самостійна робота* | | *2* | *1. Основні поняття телекомунікацій та інформатизації.*<br>*2. Компоненти і функції телекомунікаційної мережі ДПСУ.* | *[2.2]с.7-22*<br>*[3.14]с.4-5* |
| | 2 | групове заняття | 2 | ***Спеціальні комплексні інформаційно-телекомунікаційні апаратні***<br>1. Призначення та можливості СКІТА по забезпеченню управління.<br>2. Складові «СКІТА-04»(«СКІТА-02»).<br>3. Розгортання польового вузла зв'язку ООДК. | [1.23]<br>[2.1]с.79-94<br>[Х: 1.13] |
| | 3 | практичне заняття | 4 | ***Практичне розгортання елементів польового вузла зв'язку ООДК***<br>1. Розгортання «СКІТА-04»(«СКІТА-02»).<br>2. Розгортання мобільного комплексу «Гарт-1/П».<br>3. Здійснення інформаційного обміну. | [1.19]<br>[2.1]с.95-185<br>[3.3] |
| | *самостійна робота* | | *2* | *1. Правила встановлення зв'язку і ведення радіотелефонного обміну по відкритим каналам з використанням документів прихованого управління.*<br>*2. Порядок ведення обміну інформацією щодо обстановки на державному кордоні з використанням засобів радіозв'язку.* | [1.19] [1.20]<br>[2.1]с.95-106<br>[Х: 1.10] |
| | *самостійна робота* | | *2* | *1. Призначення, склад основного обладнання, ТТХ і можливості по забезпеченню інформаційного обміну «СКІТА-04»(«СКІТА-02»).* | 2.1]с.153-166, 176-183<br>[3.3], [Х: 1.13] |
| | *самостійна робота* | | *2* | *1. Порядок та культура ведення телефонних переговорів засобами проводового зв'язку.*<br>*2. Порядок використання засобів стільникового зв'язку.* | [1.19] [1.20]<br>[2.1]с.95-106<br>[Х: 1.10] |
| **2** | | | **16** | **ЗВ'ЯЗОК В ОРГАНІ ОХОРОНИ ДЕРЖАВНОГО КОРДОНУ** | |
| | 1 | групове заняття | 2 | ***Організація зв'язку у відділі прикордонної служби***<br>1. Організація зв'язку на ділянці *впс*.<br>2. Задачі зв'язку і можливості *впс* по забезпеченню управління.<br>3. Система зв'язку і характеристика її елементів. | [1.8] [1.20]<br>[2.1]с.284-292<br>[3.5] [3.11] |
| | 2 | групове заняття | 2 | ***Організація зв'язку на ділянці прикордонного загону***<br>1. Організація зв'язку на ділянці ООДК. Особливості організації зв'язку в оперативно-бойових підрозділах.<br>2. Задачі зв'язку і можливості ООДК по забезпеченню управління.<br>3. Система зв'язку і характеристика її елементів. | [1.8] [1.20]<br>[2.1]с.284-292<br>[3.5] [3.11] |
| | 3 | групове заняття Т | 2 | ***Вузли зв'язку пунктів управління прикордонного загону***<br>1. Призначення вузлів зв'язку пунктів управління. Склад сил та засобів зв'язку, що залучаються для їх розгортання.<br>2. Організація переміщення та охорони вузлів зв'язку пунктів управління.<br>3. Порядок перевірки та оцінки стану ВЗ пунктів управління. | [1.14]<br>[3.5] [3.11] |

| | | | | | |
|---|---|---|---|---|---|
| | 4 | групове заняття Т | 2 | ***Зміст роботи начальника штабу ООДК щодо організації зв'язку в охороні державного кордону***<br>1. Обов'язки та методика роботи НШ ООДК щодо оформлення пропозицій та постановки завдань з організації зв'язку.<br>2. Зміст вказівок начальнику зв'язку на забезпечення зв'язку в ОДК та порядок їх відпрацювання.<br>3. Зміст та порядок оформлення документів плану зв'язку. | [1.6] [1.8] [3.5] [3.11] |
| | 5 | групова вправа Т | 2 | ***Робота начальника штабу ООДК щодо організації зв'язку на період охорони державного кордону в різних умовах оперативно-службової діяльності***<br>1. Заслуховування пропозицій начальника зв'язку на організацію зв'язку в охороні державного кордону.<br>2. Розробка та постановка завдань начальником штабу ООДК начальнику зв'язку на організацію і забезпечення зв'язку у період охорони державного кордону в різних умовах оперативно-службової діяльності.<br>3. Розгляд начальником штабу ООДК документів плану зв'язку. Затвердження плану зв'язку начальником ООДК. | [1.6] [3.5] [3.11] |
| | *самостійна робота* | | *4* | *1. Організація зв'язку в регіональному управлінні. Сили та засоби зв'язку регіонального управління.*<br>*2. Особливості організації зв'язку на ділянці регіонального управління в різних умовах.* | [1.20] [3.7] [3.16] |
| | *самостійна робота* | | *2* | *1. Оперативно-технічна служба на вузлах зв'язку.*<br>*2. Організація чергування на вузлах зв'язку.*<br>*3. Цифрова телекомунікаційна мережа ДПСУ. Правила надання телефонних послуг.* | [1.14] |
| **3** | | | **10** | **ЗВ'ЯЗОК В ЗАГАЛЬНОВІЙСЬКОВИХ З'ЄДНАННЯХ** | |
| | 1 | групове заняття Т | 2 | ***Організація зв'язку в загальновійськовому з'єднанні***<br>1. Роль і місце системи зв'язку в системі управління окремої механізованої (танкової) бригади.<br>2. Основи організації зв'язку у різних видах бою бригади.<br>3. Потреби управління та можливості сил і засобів зв'язку окремої механізованої (танкової) бригади в обороні. | [3.1] [3.4] [3.8] [3.11] [3.15] |
| | 2 | групове заняття Т | 2 | ***Організація зв'язку в оборонному та наступальному бою омбр***<br>1. Організація зв'язку в омбр в наступальному бою.<br>2. Організація зв'язку в омбр в оборонному бою. | [3.1] [3.4] [3.8] [3.11] [3.15] |
| | *самостійна робота* | | *2* | *1. Командно-штабні машини окремої механізованої (танкової) бригади* | [3.1] [3.4] [3.8] [3.11] [3.15] |
| | *самостійна робота* | | *2* | 1. Особливості організації фельд'єгерсько-поштового зв'язку в різних видах бою | [3.9] [3.10] [Х: 1.15] |

| | | | | | |
|---|---|---|---|---|---|
| | 3 | групова вправа Т | 2 | ***Робота командира та начальника штабу омбр щодо керівництва і організації зв'язку в наступі***<br>1. Організація зв'язку в *омбр* в наступі.<br>2. Відпрацювання плануючих і розпорядчих документів зі зв'язку. | [3.1] [3.4] [3.8] [3.11] [3.15] |
| **4** | | | **22** | **ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ** | |
| | 1 | групове заняття | 2 | ***Інтегрована інформаційно-телекоммунікаційна система ДПСУ «Гарт»***<br>1. Концепція інформатизації оперативно-службової діяльності ДПСУ.<br>2. Структура та функції ІІТС «Гарт».<br>3. Сучасний стан розвитку ІІТС «Гарт». | [1.34] [1.35] [2.2]с.23-35, 170-172<br>[Х: 1.11] |
| | 2 | практичне заняття | 2 | ***Використання інформаційних ресурсів ІІТС «Гарт»***<br>1. Практичне використання інформаційних ресурсів ІТС «Гарт-3».<br>2. Практичне використання інформаційних ресурсів ІТС «Гарт-5».<br>3. Практичне використання інформаційних ресурсів ІТС «Гарт-12», ПС «Ризик», ІТС «Гарт-НПД» | [1.34] [1.35] [1.36] [1.39] |
| | *самостійна робота* | | *2* | *Концепція функціонування ІТС «Гарт-1».* | [1.34] [1.35] [1.36] [1.39] [2.2]с.207-271 |
| | *самостійна робота* | | *2* | *Реєстрація подій з оперативно-службової діяльності в ІТС «Гарт-2» та «Гарт-5».* | [1.34] [1.35] [1.36] [1.39] [2.2]с.207-271 |
| | *самостійна робота* | | *2* | *Організація інформаційного обміну в мережах документального електрозв'язку* | [1.34] [1.35] [1.36] [1.39] [2.2]с.207-271 |
| | *самостійна робота* | | *2* | *Застосування геоінформаційних систем при плануванні оперативно-службової діяльності* | [1.12] [1.13] [3.2] [Х: 1.13] |
| | *індивідуальне завдання (реферат)* | | *10* | Виконання реферату за заданою тематикою | [2.2] [Х: 1.13] |
| **5** | | | **6** | **БЕЗПЕКА ЗВ'ЯЗКУ ТА ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ** | |
| | 1 | групове заняття | 2 | ***Забезпечення безпеки зв'язку в системі зв'язку ООДК***<br>1. Загальні положення із забезпечення безпеки зв'язку.<br>2. Нормативні документи щодо забезпечення безпеки зв'язку в ООДК<br>3. Заходи зі забезпечення безпеки зв'язку в ООДК. | [1.4]; [1.6]; [1.22]; [2.1.]с.314-321<br>[3.17] с. 22-24, 106-114 |
| | 2 | практичне заняття | 4 | ***Робота посадових осіб щодо забезпечення безпеки зв'язку в системі зв'язку ООДК***<br>1. Відпрацювання плануючих документів щодо забезпечення безпеки зв'язку.<br>2. Здійснення управління з робочих місць посадових осіб.<br>4. Обмін інформацією про обстановку на державному кордоні в умовах радіозавад. | [1.4]; [1.6]; [1.22]; [2.1.]с.314-321<br>[3.17] с. 22-24, 106-114 |
| **Разом за ІІ семестр** | | | **70** | | |
| **Разом за 1-й курс** | | | **70** | | |

| | | | | | |
|---|---|---|---|---|---|
| **2-й курс** | | | | | |
| **III семестр** | | | | | |
| **5** | | | **16** | **БЕЗПЕКА ЗВ'ЯЗКУ ТА ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ (продовження)** | |
| | 3 | групове заняття | 2 | ***Основи захисту інформації в інформаційних системах ДПСУ***<br>1. Базові визначення та поняття.<br>2. Загрози безпеці інформації.<br>3. Класифікація загроз. | [1.2] [1.3] [1.6] [1.24] [1.25] [1.32] [2.3]с.18-50;78-98 |
| | 4 | практичне заняття | 6 | ***Робота керівника щодо розгляду та затвердження моделі загроз для інформації на об'єкті інформаційної діяльності***<br>1. Категоріювання ОІД для побудови моделі загроз.<br>2. Оформлення моделі загроз для інформації та її структурних елементів. | [1.25] [1.28] [1.29] [1.30] [2.3] с.512-543 |
| | 5 | семінар | 4 | ***Сили і засоби інформаційної боротьби провідних країн НАТО та суміжних держав***<br>1. Система забезпечення інформаційної безпеки України в ході проведення заходів інформаційної боротьби.<br>2. Вплив інформаційно-телекомунікаційної системи на можливості інформаційної боротьби.<br>3. Системи інформаційної боротьби в провідних країнах світу та суміжних з Україною державах. | [1.5] [2.3] с.142-158 [3.13] с.101-155 [Х: 1.14, 1.16] |
| | *самостійна робота* | | *2* | *1. Основні поняття та визначення технічної розвідки. Загальні відомості про види технічної розвідки.*<br>*2. Організація та забезпечення діяльності з протидії технічній розвідці.* | [1.3]; [1.33]; [Х: 1.16] |
| | *самостійна робота* | | *2* | *1. Державна таємниця. Віднесення інформації до державної таємниці.*<br>*2. Матеріальний носій інформації. Основні заходи щодо охорони державної таємниці.* | [1.3] [1.4] [1.22] |
| Диференційований залік | | | 4 | | |
| **Разом за III семестр** | | | **20** | | |
| **Разом за 2 курс** | | | **20** | | |
| **Усього за дисципліну** | | | **90** | | |

## ІНФОРМАЦІЙНІ РЕСУРСИ

### 1. Нормативно-правові акти

1.1. Закон України «Про Державну прикордонну службу України».
1.2. Закон України «Про телекомунікації».
1.3. Закон України «Про інформацію».

1.4. Закон України «Про державну таємницю».

1.5. Закон України «Про основи національної безпеки України».

1.6. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

1.7. Указ Президента України від 12 червня 2014 року «Про Доктрину інформаційної безпеки України» /проект/.

1.8. ДСТУ В 3265-95 Зв'язок військовий. Терміни та визначення.

1.9. Положення про матеріальну відповідальність військовослужбовців за шкоду, заподіяну Державі, затверджене Постановою Верховної Ради України від 23.06.1995 року № 243/95-ВР.

1.10. Перелік військового майна, нестача або розкрадання якого відшкодовується винним особами у кратному співвідношенні до його вартості, затверджений Постановою Кабінету Міністрів України від 2.11.1995 року № 880.

1.11. Порядок визначення розміру збитків від розкрадання, нестачі, знищення (псування) матеріальних цінностей, затверджений Постановою Кабінету Міністрів України від 22.01.1996 року № 116.

1.12. Концепція переоснащення польових вузлів зв'язку Державної прикордонної служби України сучасними технічними інформаційно-телекомунікаційними засобами, затверджена наказом Адміністрації Держприкордонслужби від 24.12.2009 року № 1025.

1.13. Програма переоснащення польових вузлів зв'язку Державної прикордонної служби України сучасними технічними інформаційно-телекомунікаційними засобами, затверджена наказом Адміністрації Держприкордонслужби від 25.12.2009 року № 1030.

1.14. Настанова з організації оперативно-технічної служби на вузлах зв'язку ДПСУ, затверджена наказом Адміністрації Держприкордонслужби України від 26.11.2004 року № 878.

1.15. Проект Порадника з технічного забезпечення зв'язку та автоматизації Прикордонних військ України, затверджений наказом Держкомкордону України від 28.07.1999 року № 364.

1.16. Положення, затверджене наказом Адміністрації Держприкордонслужби України від 22.02.2011 року № 4т. інв. 513т.

1.17. Інструкція про порядок списання військового майна в Держприкордонслужбі України, затверджена наказом Адміністрації Держприкордонслужби України від 20.05.2005 року № 404.

1.18. РР-ДПСУ-2016. інв. 691/т.

1.19. Керівництво по радіозв'язку в Збройних силах України. Частина 2. Правила радіозв'язку., інв. 525 (ДСК).

1.20. Наказ Адміністрації Держприкордонслужби України від 19.12.2008 року № 1068 «Про документи щодо забезпечення функціонування телекомунікаційної мережі Держприкордонслужби України».

1.21. Наказ Адміністрації Держприкордонслужби України від 11.12.2003 року № 347 «Про затвердження строків служби засобів зв'язку, автоматизації та радіотехніки».

1.22. Наказ Адміністрації Держприкордонслужби України від 07.07.2011 року № 501 «Про затвердження Переліку відомостей, що становлять службову інформацію у Державній прикордонній службі України та Інструкції із захисту публічної інформації у Державній прикордонній службі України».

1.23. Розпорядження Адміністрації Держприкордонслужби України від 14.02.2005 року № 111 «Про організацію супутникового зв'язку ДПСУ».

1.24. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

1.25. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

1.26. НД ТЗІ1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

1.27. НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

1.28. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

1.29. НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

1.30. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

1.31. НД ТЗІ 1.5-001-2000. Радіовиявляючі. Класифікація. Загальні технічні вимоги.

1.32. ТР ЕОТ-95. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок.

1.33. НД ТЗІ 3.6-002-01 «Технічний захист інформації щодо озброєнь та військової техніки. Інструкції з протидії технічним розвідкам під час створення зразків озброєнь та військової техніки. Методичні вказівки».

1.34. Положення про інформаційно-телекомунікаційну систему прикордонного контролю «Гарт-1» Держприкордонслужби України, затверджене наказом Адміністрації Держприкордонслужби України від 30.09.2008 року № 810, який зареєстрований в Міністерстві юстиції України 7.11.2008 року за № 1086/15777.

1.35. Положення про інформаційно-телекомунікаційну систему прикордонної служби «Гарт-3» Держприкордонслужби України, затверджене наказом Адміністрації Держприкордонслужби України від 9.12.2009 року № 949.

1.36. Порядок функціонування, застосування та використання Інтранет-мережі Держприкордонслужби України, затверджений наказом Адміністрації Держприкордонслужби України від 10.09.2004 року № 663.

1.37. Інструкція про порядок застосування АРМ «Порушник» в оперативно-службовій діяльності, затверджена наказом Адміністрації Держприкордонслужби України від 18.05.2007 року № 348.

1.38. Наказ Адміністрації Держприкордонслужби України від 14.03.2005 року № 184 «Про призначення комісії для проведення приймально-здавальних випробувань ПТК АПК ІТС «Гарт-1» у регіональних управліннях та органах охорони державного кордону Держприкордонслужби України».

1.39. Наказ Адміністрації Держприкордонслужби України від 6.05.2010 року № 325 «Про упорядкування питань використання автоматизованого робочого місця «Користувач»».

1.40. Наказ Адміністрації Держприкордонслужби України від 19.01.2007 року № 33 «Про затвердження та введення в дію Порядку користування мережами документального електрозв'язку ДПСУ».

1.41. Наказ Адміністрації Держприкордонслужби України, Державної митної служби України, Державної податкової адміністрації України, Міністерства внутрішніх справ України, Міністерства закордонних справ України, Міністерства праці та соціальної політики України, Служби безпеки України, Служби зовнішньої розвідки України від 3.04.2008 року № 284/287/214/150/64/175/266/75, зареєстрований в Міністерстві юстиції України 12.05.2008 року за № 396/15087 «Про затвердження Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон».

1.42. Інструкція, затверджена наказом Міністерства оборони України та Адміністрації Державної прикордонної служби України від 16.10.2012 року № 05/49т. – інв. 1454.

**2. Базова**

2.1. Желдак А.А. Основи зв'язку підрозділів охорони кордону. Хм.: 2005.

2.2. Катеринчук І.С., Мул Д.А., Рачок Р.В., Волинець Д.О., Прокопенко Є.В. Програмно-технічні комплекси підрозділів охорони кордону. – Хм.: В-во НАДПСУ, 2011.

2.3. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009.-608 с.: іл.

**1. Допоміжна**

1.1. Управління військами. інв. 2093-в.

1.2. Технічний опис та інструкції з експлуатації: Р-140М, Р-409, Р-419, П-240, П-241, СКІТА, PES-5000.

1.3. Комбинирование радиостанция Р-142Н, інв. 93 (ДСК)

1.4. Организация связи в бою и операции. 1994 г., інв. 291 (ДСК).

1.5. Задача 1-ДПС. Основне тактичне завдання.

1.6. Задача 2-ДПС. Основне тактичне завдання.

1.7. Задача 3-ДПС. Основне оперативно-тактичне завдання.

1.8. Бойовий статут Сухопутних військ. інв. 2017-в

1.9. Безопасность связи. інв. 1588.

1.10. Основы РЭБ, защита и безопасность связи и АСУ. інв. 1119.

1.11. Наставление по связи Сухопутных войск. інв. 376-в.

1.12. Розпорядження по зв'язку. інв. 747т

1.13. Забезпечення інформаційної безпеки як функція сучасної держави : моногр. / О. О. Тихомиров ; заг. ред. Р. А. Калюжний. − Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. – 196 с.

1.14. Катеринчук І.С., Мул Д.А., Рачок Р.В., Прокопенко Є.В. Основи будови телекомунікаційних систем. – Хм.: В-во НАДПСУ, 2014.

1.15. Альбом схем з дисципліни «ЗДК». інв. 1887-в.

1.16. Оперативне командування. інв. 2088-в (2090-в).

## X. ІНФОРМАЦІЙНІ РЕСУРСИ.

1. Сайт адміністрації ДПСУ IP: http://10.241.1.3/
2. Сайт НАДПСУ http://nadpsu.edu.ua/
3. Електронна бібліотека академії IP: http://10.241.24.195/
4. Система дистанційного навчання кафедри IP: http://10.241.24.24
5. Модульне середовище навчання http://10.241.24.9
6. Цент дослідження комп'ютерної злочинності: http://www.crime-research.ru/

**ОЦІНЮВАННЯ**

Поточне рубіжне та підсумкове оцінювання здійснюється відповідно до положення https://nadpsu.edu.ua/wp-content/uploads/2020/01/polozh-otsinka-2020-_12.01.-.pdf.

**ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)**

Середовище в аудиторії є творчим, відкритим до конструктивної критики.

Усі завдання, передбачені програмою, мають бути виконані у встановлені терміни. Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона відпрацьовують навчальні питання та завдання в часи самостійної підготовки та у встановлені викладачем терміни обов'язково звітують про опанування ними навчального матеріалу. Слухачі, які пропустили більше 30% з тих занять, де було передбачено оцінювання, одержали середньоарифметичну з поточних оцінок нижче 2,60, тобто менше 70% позитивних оцінок від загальної кількості, не відзвітували за індивідуальну та самостійну роботу, до диференційованого заліку не допускаються.

У разі коли слухач не виконав умови допуску до складання диференційованого заліку, завчасно, але не пізніше трьох робочих днів до складання диференційованого заліку, рішенням кафедри йому встановлюється індивідуальний термін ліквідації заборгованості. Якщо слухач (слухач, студент) не ліквідовує заборгованість у визначений кафедрою термін, то він вважається таким, що не виконав вимоги робочої програми навчальної дисципліни і в відомості обліку успішності, в графі «підсумкова оцінка», йому виставляється оцінка «незадовільно» за національною шкалою, 50 балів за 100-бальною шкалою і FX – за шкалою ЄКТС. При повній відсутності позитивних поточних оцінок, за визначені звітності, і не ліквідації заборгованості у визначений кафедрою термін, слухачу (слухачу, студенту) курс з навчальної дисципліни не зараховується і в графі «підсумкова оцінка», йому виставляється оцінка «недопущений» за національною шкалою, 17 балів за 100-бальною шкалою і F за шкалою ЄКТС. В такому випадку слухач (слухач, студент) представляється на засідання Вченої ради факультету, академії і йому пропонується пройти повний курс повторно. У разі відмови розглядається питання про його відрахування з академії.

**Дотримання академічної доброчесності**

Під час навчання учасники освітнього процесу зобов'язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності науково-педагогічним складом передбачає:

- посилання на джерела інформації у разі використання ідей, тверджень, відомостей;
- дотримання норм законодавства про авторське право;
- надання достовірної інформації про результати досліджень та власну педагогічну (науково-педагогічну, творчу) діяльність;
- контроль за дотриманням академічної доброчесності здобувачами освіти.

Дотримання академічної доброчесності здобувачами освіти передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей);

- посилання на джерела інформації у разі використання ідей, тверджень, відомостей;
- дотримання норм законодавства про авторське право;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

За порушення академічної доброчесності учасники освітнього процесу закладу вищої освіти можуть бути притягнені до відповідальності.

Нормативно-правове забезпечення: https://nadpsu.edu.ua/osvita/normatyvno-pravove-zabezpechennia/.

**Додаток А**

**Методи навчання та методи контролю навчальних досягнень**

| Шифр | Метод навчання |
|---|---|
| **1. Традиційні методи навчання** | |
| МН.1.1. | Усне викладення навчального матеріалу (*розповідь, пояснення, лекція*) |
| МН.1.2. | Обговорення матеріалу, що вивчається (*бесіда, дискусія, брифінг, диспут*) |
| МН.1.3. | Наочні методи (*ілюстрація, демонстрація*) |
| МН.1.4. | Практичні методи (*лабораторна робота, практична робота, пробні вправи, творчі вправи, усні вправи, практичні вправи, графічні вправи, технічні вправи*) |
| МН.1.5. | Методи самостійного та індивідуального навчання (*рецептивний, репродуктивний, евристичний, дослідницький*) |
| **2. Активні методи навчання** | |
| МН.2.1. | Ігрові (*професійні ігри, професійний тренінг*) |
| МН.2.2. | Неігрові (*аналіз конкретної ситуації, круглий стіл, навчання через науково-дослідну роботу*) |
| МН.2.3. | Неімітаційні (*групова дискусія, індивідуальні практикуми, метод «ХОБО», активні види лекційних і семінарських занять*) |
| **3. Інтерактивні методи навчання** | |
| МН.3.1. | Інтерактивні методи в малих групах |
| МН.3.2. | Інтерактивні методи в великих групах |
| МН.3.3. | Інтерактивні методи під час самостійної роботи |

| Шифр | Метод контролю навчальних досягнень |
|---|---|
| **1. Попередній контроль** | |
| МК 1.1 | Вибірковий усний |
| МК 1.2 | Фронтальний письмовий |
| МК 1.3 | Фронтальний тестовий |
| МК 1.4 | Фронтальний проблемний |
| МК 1.5 | Виконання нормативу |
| МК 1.6 | Виконання вправи |
| **2. Поточний контроль** | |
| МК 2.1 | Вибірковий усний |
| МК 2.2 | Колоквіум |
| МК 2.3 | Контрольна робота |
| МК 2.4 | Тестування |
| МК 2.5 | Захист звіту з лабораторної роботи |
| МК 2.6 | Захист звіту з практичної роботи |
| МК 2.7 | Індивідуальна розрахункова робота |
| МК 2.8 | Реферат |
| МК 2.9 | Виконання нормативу |
| МК 2.10 | Виконання вправи |
| **3. Рубіжний контроль** | |
| МК 3.1 | Фронтальний письмовий |
| МК 3.2 | Фронтальний тестовий |
| МК 3.3 | Фронтальний проблемний |
| МК 3.4 | Виконання нормативу |
| МК 3.5 | Виконання вправи |
| **4. Підсумковий контроль** | |
| МК 4.1 | Усний |
| МК 4.2 | Письмовий |
| МК 4.3 | Тестовий |
| МК 4.4 | Проблемний |
| МК 4.5 | Практичний |