

Національний юридичний університет імені Ярослава Мудрого

Військово-юридичний інститут

Кафедра військового права

ПРОГРАМА

навчальної дисципліни

«Правові основи інформаційної безпеки у воєнній сфері»

Рівень вищої освіти – перший (бакалаврський) рівень

Ступінь вищої освіти – бакалавр

Галузь знань – 26 «Цивільна безпека»

Спеціальність – 262 «Правоохоронна діяльність»

Спеціалізація – «Правоохоронна діяльність»

Статус навчальної дисципліни – обов'язкова

Затверджено на засіданні
Вченої ради,
протокол № 13 від 27 червня 2024 р.

Ректор

Анатолій Гетьман



Харків – 2024

Програма навчальної дисципліни «Правові основи інформаційної безпеки у воєнній сфері» для здобувачів вищої освіти першого (бакалаврського) рівня вищої освіти галузі знань 26 «Цивільна безпека» спеціальності 262 «Правоохоронна діяльність» спеціалізації «Правоохоронна діяльність». Харків: Нац. юрид. ун-т імені Ярослава Мудрого, 2024. 35 с.

Розробники:

**Передерій Олександр Сергійович, кандидат юридичних наук, доцент,
професор кафедри військового права;
Пащенко Євген Миколайович, доктор філософії,
старший викладач кафедри військового права**

**Затверджено на засіданні кафедри військового права
(протокол № 12 від 07 червня 2024 р.)**

Начальник кафедри – Брідня Єгор Олександрович

Зміст

1. Вступ.....	4
2. Опис навчальної дисципліни (навчальні одиниці).....	9
3. Зміст програми навчальної дисципліни.....	9
4. Ресурсне забезпечення навчальної дисципліни.....	12
4.1. Форми організації освітнього процесу та види навчальних занять.....	12
4.2. Самостійна робота здобувачів вищої освіти.....	12
4.3. Освітні технології та методи навчання	13
4.4. Форми педагогічного контролю та система оцінювання якості сформованих компетентностей за результатами засвоєння навчальної дисципліни.....	13
4.5. Навчально-методичне та інформаційне забезпечення навчальної дисципліни.....	22
Додаток 1. Карта предметних компетентностей з навчальної дисципліни	28
Додаток 2. Карта результатів навчання здобувача вищої освіти, сформульованих у термінах компетентностей	32
Додаток 3. Матриця зв'язків модулів навчальної дисципліни, результатів навчання та предметних компетентностей у програмі навчальної дисципліни.....	35

1. Вступ

1.1. Мета та завдання навчальної дисципліни.

Мета навчальної дисципліни полягає у формуванні компетентностей щодо нормативно-правового регулювання застосування заходів забезпечення інформаційної безпеки у воєнній сфері, визначення основних ризиків та загроз в сегменті інформаційної безпеки у кіберпросторі, дієвості нормативних механізмів із забезпечення захисту персональних даних у воєнній сфері.

Завдання:

надання здобувачам вищої освіти системи теоретичних знань щодо основ національної безпеки держави, місця і ролі інформаційної безпеки в системі національної безпеки держави;

засвоєння сутності інформаційних впливів як джерела інформаційних загроз національним інтересам держави, зокрема, у воєнній сфері;

надання знань щодо сутності інформаційної протидії як інструмента забезпечення інформаційної безпеки держави;

формування навичок використання інформаційних технологій в управлінні як об'єкта інформаційної протидії;

надання знань щодо інформаційно-аналітичної діяльності для прийняття управлінських рішень в умовах інформаційної протидії.

1.2. Статус навчальної дисципліни у структурі освітньо-професійної програми: обов'язкова.

1.3. Пререквізити: «Інженерна підготовка», «Організація військового зв'язку», «Основи організації та ведення боротьби в електромагнітному середовищі та кіберпросторі», «Основи військового лідерства», «Розвідувальна підготовка», «Правові засади забезпечення гендерної рівності в оборонній сфері», «Військове право».

1.4. Кореквізити: «Особливості кваліфікації військових кримінальних правопорушень».

1.5. Постреквізити: «Документологія у силах безпеки і оборони», «Лідерство у військовій сфері», «Міжнародне гуманітарне право»,

«Кримінальна відповідальність за воєнні злочини», «Запобігання військовим кримінальним правопорушенням», «Військова адміністрація», «Міжнародне військове співробітництво України».

1.6. Перелік предметних компетентностей здобувача вищої освіти:

ПК-1. Здатність характеризувати конституційні положення діяльності Збройних Сил України.

ПК-2. Здатність характеризувати положення нормативно-правових актів, які регулюють діяльність Збройних Сил України в інформаційній сфері.

ПК-3. Здатність демонструвати знання принципів державної політики у сфері інформаційної безпеки України.

ПК-4. Здатність демонструвати знання концепції державної інформаційної політики України.

ПК-5. Здатність характеризувати потенційні загрози національній безпеці України в інформаційній сфері.

ПК-6. Розуміння сутності та основних способів інформаційної протидії.

ПК-7. Здатність тлумачити нормативно-правові акти, які регламентують інформаційну безпеку як функцію забезпечення державної безпеки.

ПК-8. Здатність використовувати правові основи у сфері інформаційної безпеки держави.

ПК-9. Здатність демонструвати знання повноважень суб'єктів національної системи забезпечення інформаційної безпеки.

ПК-10. Здатність демонструвати знання основ правового забезпечення захисту інформації з обмеженим доступом у воєнній сфері.

ПК-11. Здатність демонструвати знання правових механізмів захисту державної таємниці.

ПК-12. Розуміння сутності та основних видів юридичної відповідальності військовослужбовців за правопорушення в інформаційній сфері держави.

ПК-13. Здатність демонструвати знання видів міжнародно-правового співробітництва з державами Північно-атлантичного альянсу (НАТО) в інформаційній сфері.

ПК-14. Здатність працювати з масивами інформації, здійснювати її контент-аналіз і критично-конструктивну оцінку.

ПК-15. Здатність аналізувати, досліджувати та коментувати нормативно-правові акти у сфері інформаційної безпеки.

ПК-16. Здатність до аналізу інструментарію, методології та організації роботи по забезпеченню інформаційної безпеки в умовах бойових дій.

ПК-17. Здатність оцінювати рівень негативного інформаційного впливу противника на морально-психологічний стан особового складу.

ПК-18. Розуміння сутності історії, причин і цілей інформаційного протистояння.

ПК-19. Здатність демонструвати знання алгоритму організації, підготовки та проведення інформаційних кампаній.

ПК-20. Здатність характеризувати місце, роль і обсяг інформаційної складової при плануванні та проведенні військових операцій.

ПК-21. Здатність до аналізу проблем інформаційного забезпечення військової діяльності та формування правових пропозицій щодо їх розв'язання.

ПК-22. Здатність використовувати інформаційні технології в процесі професійної діяльності.

ПК-23. Здатність моделювати та прогнозувати правові ситуації в інформаційній сфері.

ПК-24. Здатність демонструвати знання особливостей інформаційного забезпечення правової діяльності у воєнній сфері.

ПК-25. Здатність до аналізу міжнародного досвіду правової регламентації протидії кібертероризму.

Експлікація загальних і спеціальних компетентностей визначається в карті предметних компетентностей (Додаток 1).

1.7. Перелік результатів навчання здобувача вищої освіти:

РН НД 1.1. Демонструвати розуміння змісту конституційних положень щодо діяльності військових формувань.

РН НД 1.2. Демонструвати розуміння змісту нормативно-правових актів, які регулюють порядок діяльності військових формувань.

РН НД 1.3. Усвідомлювати сутність принципів державної політики у сфері національної безпеки і оборони України.

РН НД 1.4. Тлумачити концепцію державної інформаційної політики.

РН НД 1.5. Пояснювати сутність потенційних загроз національній безпеці України в інформаційній сфері.

РН НД 1.6. Демонструвати розуміння сутності основних способів інформаційного протистояння.

РН НД 1.7. Роз'яснювати сутність нормативно-правових актів, які регламентують інформаційну безпеку як функцію держави.

РН НД 1.8. Використовувати правові знання у сфері інформаційної безпеки.

РН НД 1.9. Характеризувати повноваження суб'єктів національної системи інформаційної безпеки.

РН НД 1.10. Демонструвати розуміння основ правового забезпечення захисту інформації з обмеженим доступом.

РН НД 1.11. Описувати правові механізми захисту державної таємниці.

РН НД 1.12. Характеризувати види юридичної відповідальності військовослужбовців військових формувань за правопорушення в інформаційній сфері.

РН НД 1.13. Аналізувати види міжнародно-правового співробітництва з державами Північно-Атлантичного альянсу (НАТО) в інформаційній сфері.

РН НД 1.14. Працювати з масивами інформації, здійснювати її контент-аналіз і критично-конструктивну оцінку.

РН НД 2.1. Демонструвати уміння ведення науково-дослідницької роботи в інформаційній сфері.

РН НД 2.2. Володіти інструментарієм, методологією та навичками організації роботи у військових формуваннях по забезпеченню інформаційної безпеки в умовах бойових дій.

РН НД 2.3. Проводити оцінювання рівня негативного інформаційного впливу противника на морально-психологічний стан особового складу.

РН НД 2.4. Демонструвати розуміння сутності історії, причин і цілей інформаційних війн сучасності.

РН НД 2.5. Усвідомлювати зміст алгоритмів організації, підготовки та проведення інформаційних кампаній.

РН НД 2.6. Інтегрувати знання про місце, роль і обсяг інформаційної складової при плануванні та проведенні військових операцій.

РН НД 2.7. Досліджувати проблеми інформаційного забезпечення військової діяльності та надавати правові пропозиції щодо їх розв'язання.

РН НД 2.8. Характеризувати інформаційні технології в процесі професійної діяльності.

РН НД 2.9. Прогнозувати правові ситуації в інформаційній сфері.

РН НД 2.10. Пояснювати особливості інформаційного забезпечення правової діяльності у воєнній сфері.

РН НД 2.11. Використовувати міжнародний досвід правової регламентації боротьби з кібертероризмом.

Експлікація результатів освоєння навчальної дисципліни та результатів навчання за спеціальністю і спеціалізацією визначається в карті результатів навчання, сформульованих у термінах компетентностей (Додаток 2).

1.8. Модулі програми навчальної дисципліни.

Модуль 1. Концептуальні засади інформаційної безпеки у воєнній сфері.

Модуль 2. Організаційно-правові засади забезпечення інформаційної безпеки України у воєнній сфері.

Експлікація модулів компетентнісно-орієнтованої програми навчальної дисципліни визначається у матриці зв'язків між модулями навчальної дисципліни, результатами навчання та предметними компетентностями (Додаток 3).

2. Опис навчальної дисципліни (навчальні одиниці)

Найменування показників	Рівень освіти, галузь знань, спеціальність, спеціалізація	Дидактична структура та кількість годин
Кількість кредитів ЄКТС: 4,0 Кількість модулів: 2 Загальна кількість годин: 120 Тижневих годин: аудиторних – 2-4, самостійної роботи здобувача вищої освіти – 2-4	Рівень освіти – перший (бакалаврський) Галузь знань – 26 «Цивільна безпека» Спеціальність – 262 «Правоохоронна діяльність» Спеціалізація – «Правоохоронна діяльність»	Модуль 1 Лекції: 10 Семінарські заняття: 18 Самостійна робота: 26 Модуль 2 Лекції: 10 Семінарські заняття: 22 Самостійна робота: 34 Види контролю: поточний контроль; підсумковий контроль знань (диференційований залік)

3. Зміст програми навчальної дисципліни

Модуль 1. Концептуальні засади інформаційної безпеки у военній сфері.

Основи державної політики у сфері забезпечення інформаційної безпеки України. Основи національної безпеки України. Інформаційна безпека як складова національної безпеки держави. Місце і роль інформаційної безпеки в системі національної безпеки України. Загрози і виклики національній безпеці України в сучасних умовах. Основні напрямки державної політики у сегменті національної безпеки України. Принципи національної безпеки в інформаційній сфері. Партнерство з НАТО як гарантія стабільності та безпеки України.

Інформаційна безпека України в умовах геополітичного інформаційного протиборства. Поняття і сутність інформаційної безпеки держави, суспільства та особи. Суб'єкти, об'єкти та основні принципи інформаційних відносин. Основи національної безпеки в інформаційній сфері. Виклики і загрози національній безпеці держави в інформаційному просторі. Напрями забезпечення інформаційної безпеки України. Співвідношення безпеки держави, суспільства та особи в інформаційній сфері. Тенденції ключових геополітичних змін у сучасній світовій інформаційній сфері. Характеристика актуальних проблем інформаційної безпеки України.

Загрози національній безпеці держави в інформаційній сфері. Поняття, види та класифікація загроз безпеці держави в інформаційній сфері. Наукові підходи до визначення видів загроз інформаційній безпеці. Гібридні війни сучасності: сутність та специфіка. Гібридна війна РФ проти України. Кібервійна – ключовий елемент інформаційної війни. Інформаційна війна як джерело загрози національній безпеці держави. Сутність, зміст та особливості ведення інформаційних війн. Технології та методи інформаційних війн. Збройні Сили України як головний об'єкт інформаційного ураження противником.

Основи забезпечення інформаційної безпеки у воєнній сфері. Напрями та особливості забезпечення інформаційної безпеки у військових формуваннях України. Аналіз складових інформаційної безпеки. Стан та перспективи розвитку інформаційної безпеки в Україні. Роль і завдання інформаційного захисту у вітчизняній оборонній сфері. Актуальні проблеми інформаційного захисту в секторі безпеки і оборони. Інформаційна складова у діяльності військових формувань України. Забезпечення інформаційної безпеки як функція держави. Роль інформаційної безпеки у системі функцій держави. Кібертероризм як глобальна загроза життєдіяльності держави.

Забезпечення інформаційної безпеки держави у воєнній сфері при запобіганні і стримуванні воєнного конфлікту. Інформаційне протистояння: сутність, зміст та завдання. Особливості визначення ефективності системи забезпечення інформаційної безпеки держави. Критерії ефективності системи забезпечення інформаційної безпеки держави. Інформаційна боротьба як феномен сучасного геополітичного протистояння. Ознаки і особливості деструктивної інформаційної кампанії проти України. Завдання Збройних Сил України у сфері інформаційної безпеки.

Модуль 2. Організаційно-правові засади забезпечення інформаційної безпеки України у воєнній сфері.

Система суб'єктів забезпечення інформаційної безпеки. Військові та правоохоронні органи у системі забезпечення інформаційної безпеки України.

Національна система інформаційної безпеки і кібербезпеки. Принципи та пріоритетні напрямки діяльності національної системи інформаційної безпеки і кібербезпеки. Основні суб'єкти національної системи інформаційної безпеки та їх функції. Повноваження суб'єктів сектору безпеки і оборони в системі забезпечення інформаційної безпеки держави. Особливості діяльності військових формувань та правоохоронних органів у сфері забезпечення інформаційної безпеки. Місце і роль військових формувань у забезпеченні інформаційного захисту воєнної сфери.

Основні напрями нормативно-правового забезпечення інформаційної безпеки України у воєнній сфері. Правове підґрунтя діяльності суб'єктів сектору безпеки і оборони України в інформаційній сфері. Передумови формування нормативно-правового забезпечення інформаційної безпеки України. Рівні нормативних актів, орієнтованих на забезпечення національної безпеки в інформаційній сфері. Базові нормативно-правові акти забезпечення інформаційної безпеки у воєнній сфері. Принципи функціонування системи забезпечення інформаційної безпеки України. Роль нормативно-правової складової у системі забезпечення інформаційної безпеки держави.

Нормативні акти конститутивного рівня та центральних органів виконавчої влади України з питань інформаційної безпеки у воєнній сфері. Нормативні акти, що регулюють питання інформаційної безпеки в Україні. Порівняльний аналіз європейського та вітчизняного законодавства у сфері протидії кіберзлочинності. Нормативно-розпорядчі акти органів державної влади з питань забезпечення інформаційної безпеки. Нормативно-правове регулювання як інструмент захисту інформації у воєнній сфері. Інформаційна безпека в інформаційному суспільстві: стан і шляхи забезпечення.

Захист інформації з обмеженим доступом як складова інформаційної безпеки держави. Поняття, зміст та види інформації з обмеженим доступом. Організаційно-правові та технічні заходи захисту інформації з обмеженим доступом. Контроль за забезпеченням охорони державної таємниці та нагляд за додержанням законодавства про державну таємницю. Порядок доступу до

публічної, конфіденційної, службової і таємної інформації за законодавством України. Правила поводження з інформацією з обмеженим доступом. Допуск і доступ до державної таємниці.

Юридична відповідальність за правопорушення в інформаційній сфері.
Загальна характеристика правопорушень в інформаційній сфері. Суб'єкти та об'єкти правопорушень. Види юридичної відповідальності за правопорушення в інформаційній сфері. Кримінальна та адміністративна відповідальність за правопорушення в інформаційній сфері.

Напрями вдосконалення кримінального та адміністративного законодавства України у сфері забезпечення інформаційної безпеки. Фактори, що ідентифікують інформаційні правопорушення.

4. Ресурсне забезпечення навчальної дисципліни

4.1. Форми організації освітнього процесу та види навчальних занять:

- форми організації освітнього процесу: навчальні заняття; самостійна робота; контрольні заходи;
- види навчальних занять: лекції, семінарські заняття, консультації.

4.2. Самостійна робота здобувачів вищої освіти

Самостійна робота здобувача вищої освіти є основним способом засвоєння навчального матеріалу у вільний від аудиторних занять час.

Зміст самостійної роботи здобувачів вищої освіти над конкретною навчальною дисципліною визначається відповідною програмою, методичними матеріалами, завданнями та настановами викладача. Самостійна робота забезпечується системою навчально-методичних засобів, передбачених програмою навчальної дисципліни: навчальними та методичними посібниками, матеріалами лекцій, методичними рекомендаціями з організації самостійної роботи здобувачів освіти.

Мета самостійної роботи – надати здобувачам вищої освіти комплексні знання щодо правових основ інформаційної безпеки у воєнній сфері.

Самостійна робота здобувачів вищої освіти здійснюється у таких формах: підбір та аналітичне дослідження нової наукової та навчальної літератури, рекомендованої спеціальної літератури, а також тематичного законодавства і практики його застосування правоохоронними органами; опрацювання матеріалів лекцій; виконання індивідуальних робіт; підготовка до семінарських занять; самотестування; підготовка до контрольних заходів під час поточного контролю та диференційованого заліку.

Види індивідуальних робіт, вимоги до виконання та критерії їх оцінювання закріплені у Положенні про види та критерії оцінювання індивідуальних робіт здобувачів вищої освіти кафедри військового права.

4.3. Освітні технології та методи навчання

- освітні технології: аудіовізуальні технології тощо;
- методи навчання: поєднання словесних, наочних і практичних методів, метод проблемного викладання, метод дискусії та ін.

4.4. Форми педагогічного контролю та система оцінювання якості сформованих компетентностей за результатами засвоєння навчальної дисципліни

Формами контролю знань здобувачів вищої освіти є поточний та підсумковий контроль.

Поточний контроль знань включає:

контроль якості засвоєння здобувачами вищої освіти програмного матеріалу навчальної дисципліни *на семінарських заняттях* із застосуванням таких засобів: усне, письмове або експрес-опитування, захист есе чи реферату за ініціативи здобувача освіти. У ході семінарського заняття здобувач може отримати оцінку за п'ятибальною шкалою (0; 0,25; 0,5; 0,75; 1);

контроль якості засвоєння здобувачами вищої освіти програмного матеріалу навчальної дисципліни, що проводиться наприкінці модулів у формі

виконання тестових завдань. Поточний контроль має на меті перевірку рівня підготовки здобувача у вивченні поточного матеріалу.

Впродовж семестру здобувачі вищої освіти виконують самостійну роботу, в тому числі, у формі підготовки *індивідуальної роботи*. Максимальна кількість балів за індивідуальну роботу – 10 балів.

Формою *підсумкового контролю* знань здобувачів вищої освіти з навчальної дисципліни є *диференційований залік*. Мінімальна оцінка результатів поточного контролю та індивідуальної роботи, за якої здобувач освіти допускається до складання диференційованого заліку, становить 25 балів. Максимальна кількість балів, яку здобувач вищої освіти може отримати за результатами підсумкового контролю, становить 60 балів.

*Розподіл балів між формами організації освітнього процесу
і видами контрольних заходів навчальної дисципліни
«Правові основи інформаційної безпеки у воєнній сфері»
при підсумковому контролі у формі диференційованого заліку:*

Поточний контроль				Індивідуальна робота здобувачів	Підсумковий контроль (диференційований залік)	Підсумкова оцінка знань
Модуль № 1		Модуль № 2				
Семінарські заняття	Тестове завдання	Семінарські заняття	Тестове завдання			
max 9	max 5	max 11	max 5	max 10	max 60	max 100

Критерії оцінювання (диференційований залік):

Вид контролю	Кількість балів	Критерії (за кожною з оцінок)
Поточний контроль на семінарському занятті	Max 1	Відмінне засвоєння навчального матеріалу з теми, можливі окремі несуттєві недоліки.
	0,75	Добре засвоєння матеріалу з теми, але є окремі помилки.
	0,5	Задовільний рівень засвоєння матеріалу, значна кількість помилок.
	0,25	Прогалини в знаннях, здобувач вищої освіти слабо володіє матеріалом.
	Min 0	Незадовільний рівень засвоєння матеріалу.

Тестове завдання	Max 5	Результати опрацювання матеріалу високі, можлива незначна кількість несуттєвих помилок.
	4	Добре засвоєння матеріалу з тем, але є окремі помилки.
	3	Задовільний рівень засвоєння матеріалу, значна кількість несуттєвих помилок.
	2	Задовільний рівень засвоєння матеріалу, значна кількість суттєвих помилок.
	1	Прогалини в знаннях, здобувач вищої освіти слабо володіє матеріалом.
	Min 0	Незадовільний рівень засвоєння матеріалу.
Оцінка індивідуальної роботи здобувачів вищої освіти: Наукова доповідь	Max 10	Послідовно, систематизовано, логічно, грамотно, повно викладені результати проведеного наукового дослідження за певною темою. Ґрунтовно вивчена сучасна вітчизняна та зарубіжна наукова література, нормативні джерела, судова практика, практика органів охорони правопорядку, офіційна статистика. Проведено соціологічне дослідження – опитування, анкетування тощо. Наведені посилання на використані джерела. Обрана тема є актуальною як з практичної, так і з теоретичної точок зору. Робота правильно структурована, має вступ (обґрунтування актуальності дослідження, постановка його мети та завдання), повно висвітлено стан наукової розробленості проблеми, наведено узагальнення наукової літератури, законодавства та інших джерел. Окрім викладення матеріалу робота містить власний авторський підхід до вирішення розглядуваної проблеми та висновки. Наукова доповідь ілюструється за допомогою презентації.
	8	Послідовно, систематизовано, логічно, грамотно викладені результати проведеного наукового дослідження за певною темою. Автор використав основні сучасні вітчизняні та зарубіжні наукові літературні джерела, законодавство, релевантну правозастосовну практику. В роботі наведені посилання на використані інформаційні джерела. Обрана тема є актуальною як з практичної, так і з теоретичної точок зору. Робота добре структурована, має обґрунтування актуальності дослідження; висвітлюється загальний стан наукової розробленості проблеми. Окрім викладення матеріалу робота містить аргументовані авторські висновки. Наукова доповідь ілюструється за допомогою презентації.

	6	<p>Послідовно та грамотно викладені результати проведеного наукового дослідження за певною темою. Автор використав незначну кількість сучасних вітчизняних та зарубіжних наукових літературних джерел, законодавство, правозастосовну практику. В роботі наведені посилання на використані джерела.</p> <p>Обрана тема є актуальною як з практичної, так і з теоретичної точок зору. Робота структурована, має обґрунтування актуальності дослідження, висвітлюється стан наукової розробленості проблеми. Окрім викладення матеріалу робота містить окремі авторські висновки.</p>
	4	<p>Робота недостатньо структурована, не має послідовності та логічності викладення матеріалу. Автор використав сучасні вітчизняні джерела. Наявна незначна кількість посилань на судову та / або правозастосовну практику. Представлена робота не повністю відповідає вимогам, які висуваються до робіт такого рівня, не містить достатнього обсягу, який би дозволив усвідомити сутність питання чи проблеми, задля розкриття яких вона виконувалася. Обрана тема є актуальною, але відсутній авторський підхід при дослідженні більшості питань.</p>
	2	<p>Робота недостатньо структурована, не має змістовної логічності у викладенні матеріалу. Автор використав сучасні вітчизняні джерела, але не звернувся до правозастосовної практики. Представлена робота не в повній мірі відповідає вимогам, які висуваються до робіт такого рівня, виконана неакуратно, не містить достатнього обсягу, який би дозволив усвідомити сутність питання чи проблеми, задля розкриття яких вона виконувалася; відсутні авторські висновки.</p>
	Min 0	<p>Представлена робота не відповідає вимогам, які висуваються до робіт такого рівня; містить ознаки академічної недоброчесності.</p>
Реферат	Max 10	<p>Питання плану реферату висвітлені повно. Проаналізовані представлені в навчальній та науковій літературі погляди щодо предмета дослідження; на основі їх порівняльної оцінки висловлене особисте ставлення автора до кожного з них, а також надана власна оцінка запропонованим у літературі пропозиціям стосовно шляхів вирішення таких проблемних питань, які стосуються теми, та (або) висловлені авторські пропозиції. Реферат виконаний самостійно та не містить</p>

		некоректних запозичень. Реферат ілюструється за допомогою презентації.
	7	Переважна більшість питань плану реферату висвітлена повно та точно. Одне з питань розкрито недостатньо повно або при його висвітленні допущена суттєва помилка. Проаналізовані основні літературні джерела, рекомендовані кафедрою при написанні роботи на відповідну тему. Реферат виконаний самостійно та не містить некоректних запозичень. Реферат ілюструється за допомогою презентації.
	3	Питання плану теми висвітлені поверхово. При написанні реферату використана незначна кількість монографічних та нормативних джерел із числа рекомендованих кафедрою. При розкритті питань плану допущені грубі помилки.
	Min 0	Тема реферату не розкрита або в ній виявлено некоректні запозичення (плагіат).
Анотування прочитаної додаткової літератури з курсу	Max 4	В роботі здійснена анотація обраних за погодженням з викладачем-науковим керівником джерел. Наведено бібліографічний опис анотованого джерела, надана характеристика його змісту, виділена головна ідея, ключові положення. Анотація містить не лише огляд прочитаного матеріалу, а й аналітичну позицію здобувача вищої освіти з приводу отриманої інформації. Здобувач вищої освіти продемонстрував уміння працювати з літературою, аналізувати норми чинного законодавства, використовувати наукові джерела та правозастосовну практику, робити обґрунтовані висновки. Анотація відповідає вимогам, які пред'являються до такого виду робіт. Вказуються причини обрання певної теми, джерел, робіт конкретних авторів, обґрунтовується актуальність теми, наводиться думка здобувача щодо усвідомленого матеріалу та формулюється висновок.
	2	Анотація здійснена поверхнево, містить лише огляд прочитаного матеріалу. Здобувач не продемонстрував уміння працювати з літературою, ґрунтовно аналізувати норми чинного законодавства, використовувати у необхідній кількості наукові джерела та правозастосовну практику, виокремлювати проблеми правозастосування та головну думку. Зроблені висновки не в повній мірі відображають зміст анотованого матеріалу або є помилковими.

	Min 0	Анотація містить лише загальний огляд дослідженого матеріалу. Зроблені висновки не відображають його зміст, є помилковими або містять ознаки академічного плагіату.
Узагальнення правозастосовної практики	Max 10	Здобувач вищої освіти проаналізував 30-50 судових рішень, процесуальних документів тощо, які були узагальнені ним особисто чи отримані з відповідних реєстрів. Узагальнення належним чином оформлено, наведені посилання на джерела інформації, містить вступ, в якому вказується на актуальність та мету роботи, змістовну частину, яка структурує процесуальні документи відповідно до правової позиції, та висновки. У висновках зроблено акцент на проблемах правозастосування, наявності розбіжностей у тлумаченні норми та/або у правозастосуванні, недоліках і похибках у діяльності правозастосовних органів, існуванні прогалин у законодавстві, неоднаковості у тлумаченні оцінних понять тощо. Узагальнення ілюструється за допомогою презентації.
	8	Здобувач вищої освіти проаналізував не більше 30 судових рішень, процесуальних документів тощо, які були узагальнені ним особисто чи отримані з відповідних реєстрів. Узагальнення оформлено належним чином, має вступ, змістовну частину та висновки. Втім, змістовна частина містить просте перерахування джерел без виокремлення правової позиції правозастосовника, не систематизовані належним чином проблеми правозастосування або це здійснено неповно чи неточно. У висновках вказано на проблеми правозастосування, наявності розбіжностей у тлумаченні норми та/або у правозастосуванні, недоліки та похибки правозастосовних органів, існування прогалин у законодавстві, неоднаковість у тлумаченні оцінних понять, ін.
	6	Здобувач вищої освіти проаналізував не більше 20 судових рішень, процесуальних документів тощо, які були узагальнені ним особисто чи отримані з відповідних реєстрів. Узагальнення оформлено належним чином, має вступ, змістовну частину та висновки. Втім, змістовна частина складається з простого перерахування джерел без виокремлення правової позиції правозастосовника, належним чином не систематизовані проблеми правозастосування або це здійснено неповно чи неточно. У висновках не визначені проблеми

		правозастосування, не наведено розбіжностей, які мають місце у правозастосовній практиці.
	4	Здобувач вищої освіти проаналізував не більше 10 судових рішень, процесуальних документів тощо, які були узагальнені ним особисто чи отримані з відповідних реєстрів. Узагальнення оформлено належним чином, має вступ, змістовну частину та висновки. Втім, змістовна частина складається з простого перерахування джерел без виокремлення правової позиції правозастосовника, не систематизовані належним чином проблеми правозастосування або це здійснено неповно чи неточно. У висновках не виокремлено проблеми правозастосування, не наведено розбіжностей, які мають місце у правозастосовній практиці, задля чого здійснювалося узагальнення.
	2	Здобувач вищої освіти проаналізував не більше 5 судових рішень, процесуальних документів тощо, які були узагальнені ним особисто чи отримані з відповідних реєстрів. Узагальнення оформлено належним чином, має вступ, змістовну частину та висновки. Втім, змістовна частина складається з простого перерахування джерел без виокремлення правової позиції правозастосовника, належним чином не систематизовані проблеми правозастосування або це здійснено неповно чи неточно. У висновках не виокремлено проблеми правозастосування, не наведено розбіжностей, які мають місце у правозастосовній практиці, задля чого здійснювалося узагальнення.
	Min 0	Відсутній аналіз обраних судових рішень або відповідних процесуальних документів, викладено лише зміст зібраних матеріалів. Узагальнення належним чином не оформлене та не структуроване; не наведені посилання на використані джерела інформації.
Есе	Max 6	Есе виконано самостійно, сумлінно та добросовісно. Містить ключову ідею, що розкривається у змісті роботи на конкретних прикладах із судової практики, прецедентах Європейського суду з прав людини, підходах науковців, але з формуванням та наведенням автором власного ставлення до досліджуваного питання.
	4	Есе фрагментарно розкриває ключову ідею, містить методологічні помилки, недостатнє обґрунтування досліджуваного питання.

	2	Есе фрагментарно розкриває ключову ідею, не відповідає стилю есе, не містить авторського висновку щодо розглядуваного питання.
	Min 0	Тема есе не розкрита або в ній виявлено некоректні запозичення (плагіат).
Складання термінологічного словника	3	Здобувач вищої освіти повністю виконав завдання стосовно створення заздалегідь узгодженого переліку термінів, що відображають термінологію галузі (кількох галузей) знань або лексику спеціальної сфери. Складено список термінів, пов'язаних із певною тематикою дисципліни, що вивчається, та надано їх визначення. Підготовлений словник містить не менше 10 термінів. Здобувач спирався при підготовці словника на чинне законодавство, міжнародні нормативні акти, практику Європейського суду з прав людини, Конституційного Суду України та Верховного Суду, а також сучасну вітчизняну та зарубіжну наукову літературу за обраною темою.
Розробка схем, таблиць, діаграм	3	Розроблено схему, таблицю, діаграму на основі комплексного аналізу чинного законодавства, узагальнення правозастосовної практики, опанування літературних джерел з навчальної дисципліни, яку вивчає здобувач вищої освіти. Належна систематизація матеріалу дозволила ґрунтовно проаналізувати взаємозв'язки, відмінності тощо. Цей вид індивідуальної роботи бажано проілюструвати презентацією, що значно підвищує її ілюстративність. Робота виконана акуратно, ретельно, ґрунтовно, самостійно.
Створення презентації	3	За допомогою програми Microsoft PowerPoint або за вибором здобувача іншого зручного програмного забезпечення підготовлено презентацію однієї з тем навчальної дисципліни, що вивчається. Подача матеріалу повинна бути динамічною, цікавою, ілюстративною, з використанням різних видів зображень. Презентація має містити не менше 10 слайдів та повністю розкривати питання.
Створення короткометражного фільму	10	Презентується фільм тривалістю не менш 2-3 хвилин аудіо-відео або відео контенту. Сюжет фільму охоплюється єдиною метою, містить ідею, яка заздалегідь обговорена з науковим керівником. Фільм виконаний якісно, звук чіткий, є доступним для перегляду.
Написання та опублікування наукової статті	10	Наукова стаття є логічно завершеною, ґрунтовною, в ній досліджено найбільш актуальні проблеми чи певне питання, яке є важливим для поглиблення знань здобувача

		вищої освіти з навчальної дисципліни, що ним вивчається. Стаття має науковий стиль викладу. Змістовно їй притаманні точність, зрозумілість, зв'язаність (логічна несуперечливість), цілісність, грамотність, довершеність матеріалу та його високий науковий рівень. Структурні елементи статті відповідають вимогам видання, до якого вона подається. Максимальний бал виставляється за умови опублікування підготовленої статті видавництвом.
Написання та опублікування тез доповіді на конференції	5	Тези виступу на науково-практичній чи науковій конференції відповідають вимогам, які висуваються до такого виду роботи. Вони лаконічно формулюють ключові моменти, що презентують доповідь, з якою здобувач вищої освіти виступив або бажає виступити на конференції. Тези оформлені відповідно до вимог, що висуваються організаторами конференції чи видавництвом. Максимальний бал виставляється за умови їх опублікування.
Диференційований залік Зараховано	Мах 60	1. Всебічне, систематичне і глибоке знання матеріалу, передбаченого програмою навчальної дисципліни, у тому числі орієнтація в основних наукових доктринах і концепціях навчальної дисципліни. 2. Засвоєння основної та додаткової літератури, рекомендованої кафедрою. 3. Здатність до самостійного поповнення знань з навчальної дисципліни й використання отриманих знань у практичній роботі.
	55	1. Повне знання матеріалу, передбаченого програмою навчальної дисципліни. 2. Засвоєння основної літератури та знайомство з додатковою літературою, рекомендованою кафедрою. 3. Здатність до самостійного поповнення знань з дисципліни, розуміння їх значення для практичної роботи.
	50	1. Достатньо повне знання матеріалу, передбаченого програмою навчальної дисципліни, за відсутності у відповіді суттєвих помилок. 2. Засвоєння основної літератури, рекомендованої кафедрою. 3. Здатність до самостійного поповнення знань з дисципліни, розуміння їх значення для практичної роботи.
	45	1. Знання основного матеріалу, передбаченого програмою навчальної дисципліни, в обсязі, достатньому для подальшого навчання і майбутньої роботи за професією. 2. Засвоєння основної літератури,

		рекомендованої кафедрою. 3. Помилки й суттєві неузгодженості у відповіді на запитання за наявності знань для їх самостійного усунення або за допомогою викладача.
	40	1. Знання основного матеріалу, передбаченого програмою навчальної дисципліни, в обсязі, достатньому для подальшого навчання і майбутньої роботи за професією. 2. Ознайомлення з основною літературою, рекомендованою кафедрою. 3. Помилки у відповіді на запитання за наявності знань для усунення найсуттєвіших помилок за допомогою викладача.
	35	1. Прогалини в знаннях з певних частин основного матеріалу, передбаченого програмою навчальної дисципліни. 2. Наявність помилок у відповіді на питання на запитання.
Не зараховано	Min 0	1. Відсутність знань значної частини основного матеріалу, передбаченого програмою навчальної дисципліни. 2. Неможливість продовжити навчання або здійснювати професійну діяльність без проходження повторного курсу з цієї дисципліни.

4.5. Навчально-методичне та інформаційне забезпечення

навчальної дисципліни

Нормативно-правові акти

1. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР.
URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
2. Кодекс України про адміністративні правопорушення (ст.ст. 1-212⁻²⁴)
: Закон України від 07.12.1984 р. № 8073-Х. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text>
3. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>
4. Про Державну прикордонну службу України : Закон України від 03.04.2003 р. № 661-IV. URL: <https://zakon.rada.gov.ua/laws/show/661-15#Text>

5. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 р. № 3475-IV. URL: <https://zakon.rada.gov.ua/laws/show/3475-15#Text>
6. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII. URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>
7. Про електронні комунікації : Закон України від 16.12.2020 р. № 1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>
8. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
9. Про Збройні Сили України : Закон України від 06.12.1991 р. № 1934-XII. URL: <https://zakon.rada.gov.ua/laws/show/1934-12#Text>
10. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
11. Про контррозвідувальну діяльність : Закон України від 26.12.2002 р. № 374-IV. URL: <https://zakon.rada.gov.ua/laws/show/374-15#Text>
12. Про медіа : Закон України від 13.12.2022 р. № 2849-IX. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>
13. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
14. Про Національну гвардію України : Закон України від 13.03.2014 р. № 876-VII. URL: <https://zakon.rada.gov.ua/laws/show/876-18#Text>
15. Про Національну програму інформатизації : Закон України від 01.12.2022 р. № 2807-IX. URL: <https://zakon.rada.gov.ua/laws/show/2807-20#Text>
16. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

17. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 р. № 183/98-ВР. URL: <https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text>

18. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII. URL: <https://zakon.rada.gov.ua/laws/show/2229-12#Text>

19. Про Службу зовнішньої розвідки України : Закон України від 01.12.2005 р. № 3160-IV. URL: <https://zakon.rada.gov.ua/laws/show/3160-15#Text>

20. Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних : Указ Президента України від 24.09.2001 р. № 891/2001. URL: <https://zakon.rada.gov.ua/laws/show/891/2001#Text>

21. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні : Указ Президента України від 31.07.2000 р. № 928/2000. URL: <https://zakon.rada.gov.ua/laws/show/928/2000#Text>

22. Про Концепцію боротьби з тероризмом в Україні : Указ Президента України від 05.03.2019 р. № 53/2019. URL: <https://zakon.rada.gov.ua/laws/show/53/2019#Text>

23. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 р. № 242/2016. URL: <https://zakon.rada.gov.ua/laws/show/242/2016#Text>

24. Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації : Указ Президента України від 23.11.2011 р. № 1067/2011. URL: <https://zakon.rada.gov.ua/laws/show/1067/2011#Text>

25. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 р. № 1229/99. URL: <https://zakon.rada.gov.ua/laws/show/1229/99#Text>

26. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ

Президента України від 14.09.2020 р. № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>

27. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>

28. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017. URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text>

29. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах : Постанова Кабінету Міністрів України від 16.11.2002 р. № 1772. URL: <https://zakon.rada.gov.ua/laws/show/1772-2002-%D0%BF#Text>

30. Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади : Постанова Кабінету Міністрів України від 04.01.2002 р. № 3. URL: <https://zakon.rada.gov.ua/laws/show/3-2002-%D0%BF#Text>

31. Про затвердження Змін до Зводу відомостей, що становлять державну таємницю : Наказ Служби безпеки України від 04.03.2019 р. № 361. URL: <https://zakon.rada.gov.ua/laws/show/z0306-19#Text>

32. Про забезпечення інформаційних потреб та інформаційної безпеки громадян : Рішення Національної ради України з питань телебачення і радіомовлення від 01.12.2004 р. URL: <https://zakon.rada.gov.ua/rada/show/n0001295-04#Text>

Література

Основна література

1. Бобало Ю. Я., Горбатий І. В., Кіселичник М. Д., Бондарєв А. П., Войтусік С. С., Горпенюк А. Я., Немкова О. А., Журавель І. М., Березюк Б. М., Яковенко Є. І., Отенко В. І., Тишик І. Я. Інформаційна безпека : навч. посіб. Львів : Вид-во Львівської політехніки, 2019. 580 с.
2. Інформаційна безпека : навч. посіб. / під ред. В. В. Остроухова. Київ : ЛПРА-К, 2021. 240 с.
3. Основи інформаційної безпеки : навч. посіб. / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2020. 128 с.
4. Титова Н. М., Рідей Н. М., Настрадін В. П., Присяжнюк М. М., Мамченко С. М., Артюх С. В., Яворська Р. О. Інформаційна безпека та кібербезпека держави : навч. посіб. Київ : Література, 2024. 224 с.
5. Управління інформаційною безпекою : навч. посіб. / уклад.: Толюпа С. В. та ін. Чернівці : Чернівецьк. нац. ун-т ім. Ю. Федьковича, 2021. 540 с.

Додаткова література

1. Лісовська Ю. П. Інформаційна безпека : навч. посіб. Київ : Кондор, 2018. 172 с.
2. Лужецький В. А., Войтович О. П., Дудатьєв А. В. Інформаційна безпека : навч. посіб. Вінниця : УНІВЕР-СУМ-Вінниця, 2019. 240 с.
3. Основи управління інформаційною безпекою : навч. посіб. / А. М. Гребенюк, Л. В. Рибальченко. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2020. 144 с.

Інтернет-ресурси:

- Офіційний веб-портал Верховної Ради України - <http://rada.gov.ua/>
 Офіційний веб-портал Міністерства оборони України - <https://www.mil.gov.ua/>

Офіційний веб-портал Наукової бібліотеки НЮУ імені Ярослава Мудрого - <https://library.nlu.edu.ua/>

СЕНМК

Стандартизований електронний навчально-методичний комплекс кафедри військового права Військово-юридичного інституту. URL: <https://library.nlu.edu.ua/senmk/itemlist/category/555-kafedryviiskovoiurydychnoho-instytutu.html>

НЕІК

Навчальний електронний інформаційний комплекс «262 ПД Правові основи інформаційної безпеки у воєнній сфері». URL: <https://neik.nlu.edu.ua/moodle/course/view.php?id=1394>

Додаток 1

Карта предметних компетентностей з навчальної дисципліни

Шифр та назва компетентностей за спеціальністю і/або спеціалізацією	Шифр та назва компетентностей з навчальної дисципліни
ЗК – загальні (універсальні) компетентності (обрати компетентності згідно зі змістом навчальної дисципліни)	ПК – предметні компетентності з навчальної дисципліни
ЗК1. Здатність застосовувати знання у практичних ситуаціях.	ПК-7. Здатність тлумачити нормативно-правові акти, які регламентують інформаційну безпеку як функцію забезпечення державної безпеки. ПК-8. Здатність використовувати правові основи у сфері інформаційної безпеки держави. ПК-15. Здатність аналізувати, досліджувати та коментувати нормативно-правові акти у сфері інформаційної безпеки.
ЗК2. Знання та розуміння предметної області та розуміння професійної діяльності.	ПК-1. Здатність характеризувати конституційні положення діяльності Збройних Сил України. ПК-2. Здатність характеризувати положення нормативно-правових актів, які регулюють діяльність Збройних Сил України в інформаційній сфері. ПК-3. Здатність демонструвати знання принципів державної політики у сфері інформаційної безпеки України. ПК-4. Здатність демонструвати знання концепції державної інформаційної політики України. ПК-6. Розуміння сутності та основних способів інформаційної протидії. ПК-9. Здатність демонструвати знання повноважень суб'єктів національної системи забезпечення інформаційної безпеки. ПК-11. Здатність демонструвати знання правових механізмів захисту державної таємниці. ПК-12. Розуміння сутності та основних видів юридичної відповідальності військовослужбовців за правопорушення в інформаційній сфері держави. ПК-18. Розуміння сутності історії, причин і цілей інформаційного протистояння.
ЗК4. Здатність використовувати інформаційні та комунікаційні технології.	ПК-14. Здатність працювати з масивами інформації, здійснювати її контент-аналіз і критично-конструктивну оцінку.

	ПК-22. Здатність використовувати інформаційні технології в процесі професійної діяльності.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.	ПК-5. Здатність характеризувати потенційні загрози національній безпеці України в інформаційній сфері. ПК-10. Здатність демонструвати знання основ правового забезпечення захисту інформації з обмеженим доступом у воєнній сфері. ПК-24. Здатність демонструвати знання особливостей інформаційного забезпечення правової діяльності у воєнній сфері.
ЗК7. Здатність до адаптації та дії в новій ситуації.	ПК-23. Здатність моделювати та прогнозувати правові ситуації в інформаційній сфері.
ЗК9. Здатність працювати в команді.	ПК-17. Здатність оцінювати рівень негативного інформаційного впливу противника на морально-психологічний стан особового складу. ПК-19. Здатність демонструвати знання алгоритму організації, підготовки та проведення інформаційних кампаній. ПК-20. Здатність характеризувати місце, роль і обсяг інформаційної складової при плануванні та проведенні військових операцій.
ЗК 1.1. Здатність удосконалювати свій професійний рівень та набувати нові знання.	ПК-13. Здатність демонструвати знання видів міжнародно-правового співробітництва з державами Північно-атлантичного альянсу (НАТО) в інформаційній сфері. ПК-16. Здатність до аналізу інструментарію, методології та організації роботи по забезпеченню інформаційної безпеки в умовах бойових дій. ПК-25. Здатність до аналізу міжнародного досвіду правової регламентації протидії кібертероризму.
ЗК 1.5. Здатність до креативності у предметно-практичній діяльності.	ПК-21. Здатність до аналізу проблем інформаційного забезпечення військової діяльності та формування правових пропозицій щодо їх розв'язання.
СК – фахові компетентності за спеціальністю (обрати компетентності згідно зі змістом навчальної дисципліни)	
СК1. Усвідомлення функцій держави у сфері правоохоронної діяльності, способів та механізмів реалізації цих функцій.	ПК-1. Здатність характеризувати конституційні положення діяльності Збройних Сил України. ПК-2. Здатність характеризувати положення нормативно-правових актів, які регулюють діяльність Збройних Сил України в інформаційній сфері.

	<p>ПК-3. Здатність демонструвати знання принципів державної політики у сфері інформаційної безпеки України.</p> <p>ПК-4. Здатність демонструвати знання концепції державної інформаційної політики України.</p> <p>ПК-9. Здатність демонструвати знання повноважень суб'єктів національної системи забезпечення інформаційної безпеки.</p>
СК3. Здатність до критичного мислення та системного аналізу правових явищ.	ПК-15. Здатність аналізувати, досліджувати та коментувати нормативно-правові акти у сфері інформаційної безпеки.
СК4. Здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати правову інформацію з різних джерел.	<p>ПК-14. Здатність працювати з масивами інформації, здійснювати її контент-аналіз і критично-конструктивну оцінку.</p> <p>ПК-18. Розуміння сутності історії, причин і цілей інформаційного протистояння.</p>
СК5. Здатність визначати придатні для юридичного аналізу факти, систематизувати одержані результати, встановлювати причинно-наслідкові зв'язки, формулювати аргументовані висновки та рекомендації.	ПК-12. Розуміння сутності та основних видів юридичної відповідальності військовослужбовців за правопорушення в інформаційній сфері держави.
СК8. Здатність ефективно застосовувати сучасну техніку та інформаційні технології, використовувати технічні засоби, спеціалізовані інформаційно-пошукові системи, бази та банки даних, а також відповідне програмне забезпечення для захисту прав і свобод людини, власності, суспільних відносин від протиправних посягань.	ПК-22. Здатність використовувати інформаційні технології в процесі професійної діяльності.
СК16. Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об'єктів критичної інфраструктури.	<p>ПК-5. Здатність характеризувати потенційні загрози національній безпеці України в інформаційній сфері.</p> <p>ПК-6. Розуміння сутності та основних способів інформаційної протидії.</p> <p>ПК-7. Здатність тлумачити нормативно-правові акти, які регламентують інформаційну безпеку як функцію забезпечення державної безпеки.</p> <p>ПК-8. Здатність використовувати правові основи у сфері інформаційної безпеки держави.</p> <p>ПК-13. Здатність демонструвати знання видів міжнародно-правового співробітництва з державами Північно-атлантичного альянсу (НАТО) в інформаційній сфері.</p> <p>ПК-19. Здатність демонструвати знання алгоритму організації, підготовки та проведення інформаційних кампаній.</p>

СК17. Здатність забезпечувати охорону державної таємниці та працювати з носіями інформації з обмеженим доступом.	ПК-10. Здатність демонструвати знання основ правового забезпечення захисту інформації з обмеженим доступом у воєнній сфері. ПК-11. Здатність демонструвати знання правових механізмів захисту державної таємниці.
СК – фахові компетентності за спеціалізацією (обрати компетентності згідно зі змістом навчальної дисципліни)	
СК 1.2. Уміння виявляти проблеми правозастосування та пропонувати шляхи їх вирішення під час здійснення правоохоронної діяльності.	ПК-21. Здатність до аналізу проблем інформаційного забезпечення військової діяльності та формування правових пропозицій щодо їх розв'язання.
СК 1.3. Здатність до перенесення диференційованих фізичних навантажень; експлуатації й обслуговування техніки; прийняття рішень в ході повсякденної службової діяльності, під час мобілізації, воєнного/надзвичайного стану та в умовах ведення бойових дій.	ПК-16. Здатність до аналізу інструментарію, методології та організації роботи по забезпеченню інформаційної безпеки в умовах бойових дій. ПК-17. Здатність оцінювати рівень негативного інформаційного впливу противника на морально-психологічний стан особового складу.
СК 1.4. Здатність використовувати спеціальні знання в різних сферах правоохоронної діяльності.	ПК-20. Здатність характеризувати місце, роль і обсяг інформаційної складової при плануванні та проведенні військових операцій. ПК-24. Здатність демонструвати знання особливостей інформаційного забезпечення правової діяльності у воєнній сфері.
СК 1.5. Вміння визначати напрями і способи виявлення та протидії організованим та транснаціональній злочинності.	ПК-23. Здатність моделювати та прогнозувати правові ситуації в інформаційній сфері. ПК-25. Здатність до аналізу міжнародного досвіду правової регламентації протидії кібертероризму.

Додаток 2

**Карта результатів навчання здобувача вищої освіти,
сформульованих у термінах компетентностей**

Шифр та назва РН за спеціальністю і / або спеціалізацією	Модуль НД	Шифр та назва РН з навчальної дисципліни
РН – результати навчання за спеціальністю / спеціалізацією (обрати результати навчання згідно зі змістом навчальної дисципліни)		Результати навчання з навчальної дисципліни
РН3. Розуміти та професійно застосовувати понятійний апарат права та правоохоронної діяльності.	№ 1	РН НД 1.1. Демонструвати розуміння змісту конституційних положень щодо діяльності військових формувань. РН НД 1.2. Демонструвати розуміння змісту нормативно-правових актів, які регулюють порядок діяльності військових формувань. РН НД 1.7. Роз'яснювати сутність нормативно-правових актів, які регламентують інформаційну безпеку як функцію держави. РН НД 1.8. Використовувати правові знання у сфері інформаційної безпеки.
РН4. Формулювати і перевіряти гіпотези, виокремлювати юридично значущі факти, виявляти причинно-наслідкові зв'язки в діях і явищах для прийняття оптимального рішення в конкретних ситуаціях.	№ 2	РН НД 2.7. Досліджувати проблеми інформаційного забезпечення військової діяльності та надавати правові пропозиції щодо їх розв'язання.
РН7. Взаємодіяти із суб'єктами забезпечення публічної (громадської) безпеки і порядку, а також здійснювати комунікацію з фізичними та юридичними особами з метою виконання завдань у сфері правоохоронної діяльності.	№ 2	РН НД 2.5. Усвідомлювати зміст алгоритмів організації, підготовки та проведення інформаційних кампаній.
РН8. Здійснювати пошук інформації у доступних джерелах, аналізувати і оцінювати її для повного та всебічного встановлення обставин, необхідних для виконання професійних завдань.	№ 1	РН НД 1.6. Демонструвати розуміння сутності основних способів інформаційного протистояння.

РН10. Виокремлювати юридично значущі факти і формувати обґрунтовані правові висновки.	№ 1	РН НД 1.12. Характеризувати види юридичної відповідальності військовослужбовців військових формувань за правопорушення в інформаційній сфері.
РН11. Знати і розуміти сучасні правові доктрини, цінності та принципи функціонування національної правової системи.	№ 1	РН НД 1.3. Усвідомлювати сутність принципів державної політики у сфері національної безпеки і оборони України. РН НД 1.4. Тлумачити концепцію державної інформаційної політики.
РН12. Адаптуватися і ефективно діяти у стандартних професійних ситуаціях, а також у разі ускладнення оперативної обстановки, підвищення фізичного та психологічного навантаження.	№ 2	РН НД 2.2. Володіти інструментарієм, методологією та навичками організації роботи у військових формуваннях по забезпеченню інформаційної безпеки в умовах бойових дій.
РН14. Здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя, підвищення професійної майстерності, вивчення та використання передового досвіду у сфері правоохоронної діяльності.	№ 2	РН НД 2.1. Демонструвати уміння ведення науково-дослідницької роботи в інформаційній сфері. РН НД 2.4. Демонструвати розуміння сутності історії, причин і цілей інформаційних війн сучасності. РН НД 2.10. Пояснювати особливості інформаційного забезпечення правової діяльності у воєнній сфері. РН НД 2.11. Використовувати міжнародний досвід правової регламентації боротьби з кібертероризмом.
РН15. Працювати самостійно та в команді при виконанні службових (посадових) обов'язків та під час розв'язання складних спеціалізованих задач у сфері правоохоронної діяльності.	№ 1	РН НД 1.13. Аналізувати види міжнародно-правового співробітництва з державами Північно-Атлантичного альянсу (НАТО) в інформаційній сфері.
РН18. Застосовувати вогнепальну зброю та спеціальні засоби (штатне та бойове озброєння), фізичну силу; інформаційні системи та технології, технології захисту даних, методи обробки, накопичення та аналізу інформації, інформаційно-аналітичні системи, бази даних (в тому числі міжвідомчі та міжнародні), криміналістичні та оперативно-технічні засоби, безпілотну авіацію, іншу спеціальну та військову техніку і спорядження.	№ 2	РН НД 2.8. Характеризувати інформаційні технології в процесі професійної діяльності.

РН21. Організувати та здійснювати заходи щодо дотримання режиму секретності та захисту інформації.	№ 1	РН НД 1.10. Демонструвати розуміння основ правового забезпечення захисту інформації з обмеженим доступом. РН НД 1.11. Описувати правові механізми захисту державної таємниці.
РН22. Оцінювати оперативну (бойову) обстановку, рівень потенційних загроз та викликів, прогнозувати їх розвиток, застосовувати тактичні методи превентивного та силового втручання для запобігання та припинення правопорушень, усунення загроз внутрішньому безпековому середовищу, державному суверенітету та територіальній цілісності держави, у тому числі у взаємодії з іншими уповноваженими на це органами та громадою.	№ 1, 2	РН НД 1.5. Пояснювати сутність потенційних загроз національній безпеці України в інформаційній сфері. РН НД 2.3. Проводити оцінювання рівня негативного інформаційного впливу противника на морально-психологічний стан особового складу.
РН 1.1. Виконувати оперативні завдання правоохоронної діяльності із залученням фахівців з інших галузей знань.	№ 1	РН НД 1.9. Характеризувати повноваження суб'єктів національної системи інформаційної безпеки.
РН 1.2. Демонструвати навички верифікації отриманої під час здійснення правоохоронної діяльності інформації.	№ 1	РН НД 1.14. Працювати з масивами інформації, здійснювати її контент-аналіз і критично-конструктивну оцінку.
РН 1.4. Визначати професійні завдання і організувати підлеглих для їх виконання, брати на себе відповідальність за отримані результати та здійснювати службові обов'язки у нестандартних ситуаціях за наявності неповної або обмеженої інформації.	№ 2	РН НД 2.9. Прогнозувати правові ситуації в інформаційній сфері.
РН 1.5. Виявляти навички фізичної підготовленості; експлуатації й обслуговування техніки; тактичного планування, моделювання та прийняття оптимальних рішень в умовах невизначеності.	№ 2	РН НД 2.6. Інтегрувати знання про місце, роль і обсяг інформаційної складової при плануванні та проведенні військових операцій.

