НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ
ЧЕРКАСЬКИЙ ІНСТИТУТ ПОЖЕЖНОЇ БЕЗПЕКИ
ІМЕНІ ГЕРОЇВ ЧОРНОБИЛЯ

ФАКУЛЬТЕТ ЦИВІЛЬНОГО ЗАХИСТУ

КАФЕДРА УПРАВЛІННЯ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ДЕРЖАВНЕ УПРАВЛІННЯ У СФЕРІ КІБЕРБЕЗПЕКИ»

циклу професійної вибіркової підготовки
за освітньо-професійною програмою «Право»
підготовки за другим (магістерським) рівнем вищої освіти
у галузі знань 08 «Право»
за спеціальністю 081 «Право»

Рекомендовано кафедрою управління
у сфері цивільного захисту
на 2022-2023 навчальний рік.
Протокол від 23 серпня 2022 р. № 1.

Силабус розроблений відповідно до робочої програми навчальної дисципліни «Державне управління у сфері кібербезпеки».

2022 рік

Загальна інформація про дисципліну

Анотація дисципліни

Державне управління у сфері кібербезпеки – навчальна дисципліна підготовки здобувачів вищої освіти освітнього рівня «магістр». Спеціальність 081 «Право», галузь знань 08 «Право».

Поряд із вагомими перевагами сучасного цифрового світу та розвитком інформаційних технологій, дуже активно поширюються випадки незаконного збирання, зберігання, використання, знищення та поширення персональних даних, незаконних фінансових операцій, крадіжок і шахрайства в мережі Інтернет. Разом із тим, сучасні інформаційно-комунікаційні технології можуть використовуватись навіть для вчинення терористичних актів.

Кібербезпека – дуже важливий аспект освіти сучасного студента. Кожен здобувач вищої освіти повинен володіти навичками грамотного поводження з інформацією. Подібні компетентності потрібно формувати одночасно з початковими навиками володіння персональним комп'ютером.

Сучасні кіберзагрози існують повсюди де застосовуються інформаційні технології, отже здобувач вищої освіти будь-якої спеціальності, враховуючи умови сьогодення, у своїй діяльності стикається і з вірусами, і зі зломом комп'ютера, і з багатьма іншими проблемами, на які потрібно вміти не тільки оперативно реагувати, але і на скільки це можливо вміти запобігати їх появі.

Навчальна дисципліна «Державне управління у сфері кібербезпеки» спрямована на оволодіння необхідними базовими поняттями та правилами безпечної поведінки в мережі; ознайомлення із різними типами зловмисного програмного забезпечення та атаками, а також методами захисту від них; основними засадами забезпечення національної кібербезпеки України, об'єктами кібербезпеки та кіберзахисту, суб'єктами забезпечення національної системи кібербезпеки та ін.

Інформація про науково-педагогічних працівників

Загальна інформація	Костенко Віталій Олександрович, старший викладач кафедри управління у сфері цивільного захисту, кандидат наук з державного управління
Контактна інформація	м. Черкаси, вул. Онопрієнка, 8, кабінет № 427.
E-mail	kostenkovo@ukr.net, kostenko_vitalii@chipb.org.in
Наукові інтереси	Державне управління у сферах цивільного захисту, техногенної та пожежної безпеки, захисту населення і територій від надзвичайних ситуацій у мирний час та в особливий період; формування системи цивільного захисту на основі міжнародного досвіду; адаптація законодавства у сфері цивільного захисту до вимог Європейського Союзу
Професійні здібності	здатність робити навчальний матеріал доступним; творчість у роботі; практичне застосування наведеного навчального матеріалу;

	педагогічно-вольовий вплив на здобувачів; здатність організувати колектив здобувачів; педагогічний такт; здатність зв'язати навчальний предмет з професійною діяльністю; спостережливість; педагогічна вимогливість
Наукова діяльність за освітнім компонентом	1. В.О. Костенко. Геополітичні фактори виникнення терористичних загроз та їх наслідки для України і світу // Вчені записки Таврійського національного університету імені В.І. Вернадського:зб. наук. пр. – К. : Серія: Державне управління». Том 29 (68). № 1, Київ. 2018. – С. 218 – 222. http://www.pubadm.vernadskyjournals.in.ua/journals/2018/1_2018/41.pdf. 2. В.О. Костенко. Концептуальні засади інституційного розвитку системи цивільного захисту України // науково-виробничий журнал «Держава та регіони. Серія: Державне управління» № 2/2018. Запоріжжя.С. 120 – 124.http://pa.stateandregions.zp.ua/archive/2_2018/23.pdf. 3. В.О. Костенко. Удосконалення системи цивільного захисту територіальних громад в контексті розвитку місцевої та добровільної пожежної охорони // фаховий науковий журнал: Публічне управління і адміністрування в Україні», м. Одеса, вип. 29/2022.С. 85-88.http://www.pag-journal.iei.od.ua/archives/2022/29-2022/16.pdf. 4. В.О. Костенко, Ю.М. Горбаченко. Нормативно-правове регулювання волонтерської діяльності у сфері цивільного захисту в умовах мирного часу та особливого періоду//фаховий науковий журнал: Публічне управління і адміністрування в Україні», м. Одеса, вип. 30/2022.С. 133-136.http://www.pag-journal.iei.od.ua/archives/2022/30-2022/23.pdf. 5. В.О. Костенко. Нормативно-правове регулювання питання укриття населення у захисних спорудах цивільного захисту//фаховий науковий журнал: Публічне управління і адміністрування в Україні», м. Одеса, вип. 32/2022.С. 55-58.http://www.pag-journal.iei.od.ua/archives/2022/32-2022/10.pdf. 6. В.О. Костенко. Актуалізація процесу забезпечення кібербезпеки України в умовах воєнного стану. Одеський державний університет внутрішніх справ Центр українсько-європейського наукового співробітництва. Всеукраїнське науково-педагогічне

	підвищення кваліфікації «Безпековий сектор держави: вітчизняний досвід та кращі міжнародні практики». 5 грудня – 15 січня 2023 року. С. 58-62.

Час та місце проведення занять з навчальної дисципліни

Аудиторні заняття з навчальної дисципліни проводяться згідно з затвердженим розкладом.

Консультації з навчальної дисципліни проводяться протягом семестру щовівторка з 15:00 до 16:00 в аудиторії № 129. У разі потреби здобувача отримати додаткову консультацію – час узгоджується з викладачем.

Мета вивчення дисципліни:

Метою викладання навчальної дисципліни «Державне управління у сфері кібербезпеки» є:

- формування у здобувачів вищої освіти теоретичної бази знань з основних засад забезпечення кібербезпеки України;
- сформувати систему знань про виклики та кіберзагрози у національному кіберпросторі, а також інтегрувати здобувачів у освітній процес в інституті та на спеціальності;
- вивчення та усвідомлення значення норм права, що регулюють пошук, одержання, виробництво і поширення інформації, нерозривний зв’язок норм права з їхнім практичним застосуванням відповідними органами;
- закладення знань щодо основних понять нормативно-правового забезпечення кібербезпеки, прав та обов’язків учасників інформаційних правовідносин, можливостей захисту при порушенні їх прав;
- формування навичок використання чинних нормативно-правових норм у сфері забезпечення кібербезпеки України;
- підвищення правової культури і правосвідомості, а також виховання у студентів правового мислення;

У рамках вивчення дисципліни передбачається ознайомлення студентів з нормативно-правовим забезпеченням кібербезпеки. Показати основні аспекти захисту інтересів суб’єктів інформаційних відносин. Ознайомлення із системою суб’єктів забезпечення кібербезпеки в Україні, організацією міжнародного співробітництва у сфері кібербезпеки, міжнародними аспектами кібербезпеки в умовах глобалізації.

Навчальна дисципліна «Державне управління у сфері кібербезпеки» є актуальною в умовах сучасних викликів і загроз, пов’язаних із військовою агресією Російської Федерації проти нашої держави. Її понятійне поле межує з такими дисциплінами, як: «Теорія прийняття управлінських рішень», «Основи теорії управління», «Теорія систем та системного аналізу», «Правові основи організації та забезпечення цивільного захисту», «Система державного управління та місцевого самоврядування», «Управління ризиками виникнення надзвичайних ситуацій», та ін.

Державне управління у сфері кібербезпеки може і повинно знайти своє місце в управлінській теорії та практиці.

Опис навчальної дисципліни

Найменування показників	Форма здобуття освіти	
	очна (денна)	заочна (дистанційна)
Статус дисципліни	професійна обов'язкова	професійна обов'язкова
Рік підготовки	2-й	2-й
Семестр	3-й	3-й
Обсяг дисципліни:		
- в кредитах ЄКТС	3	3
- кількість модулів		
- загальна кількість годин	90 год.	90 год.
Розподіл часу за навчальним планом:		
- лекції (годин)	10 год.	10 год.
- практичні заняття (годин)	0 год.	0 год.
- семінарські заняття (годин)	4 год.	4 год.
- лабораторні заняття (годин)	0 год.	0 год.
– курсовий проект (робота) (годин)	0 год.	0 год.
- інші види занять (годин)	0 год.	0 год.
- самостійна робота (годин)	76 год.	76 год.
- індивідуальні завдання (науково-дослідне) (годин)	0 год.	0 год.
- підсумковий контроль	залік	залік

Передумови для вивчення дисципліни

Вивчення навчальної дисципліни «Державне управління у сфері кібербезпеки» вимагає знань навчальних дисциплін з циклу професійної підготовки: «Теорія прийняття управлінських рішень», «Основи теорії управління», «Теорія систем та системного аналізу», «Правові основи організації та забезпечення цивільного захисту», «Система державного управління та місцевого самоврядування», «Управління ризиками виникнення надзвичайних ситуацій» та ін.

Результати навчання та компетентності з дисципліни

Відповідно до освітньої програми «Право» вивчення навчальної дисципліни повинно забезпечити:

- досягнення здобувачами вищої освіти таких результатів навчання:

Результати навчання	РН
Ефективно управляти складними робочими процесами у сфері цивільної безпеки, у тому числі непередбачуваними та такими, що потребують нових стратегічних підходів; об'єктивно оцінювати результати діяльності персоналу та колективу.	РН02

Інтегрувати знання з різних галузей для розв’язання теоретичних та/або практичних задач і проблем у сфері цивільної безпеки.	РН03
Розробляти та реалізовувати ефективні заходи, спрямовані на регулювання та забезпечення цивільної безпеки.	РН05
Визначати та аналізувати можливі загрози виникнення надзвичайної ситуації, аварії, нещасного випадку на виробництві та оцінювати можливі наслідки та ризики.	РН06
Розв’язувати проблеми у нових або незнайомих ситуаціях за наявності неповної або обмеженої інформації, оцінювати ризики, здійснювати відповідні дослідження.	РН11
Оцінювати відповідність правових, організаційних, технічних заходів по забезпеченню техногенної безпеки та безпеки праці вимогам законодавства під час професійної діяльності.	РН13
Здійснювати прогнозування, оцінку ризику під час професійної діяльності та можливості відповідних підрозділів щодо реагування на надзвичайні ситуації та події.	РН14
Приймати ефективні рішення у складних непередбачуваних умовах, визначати цілі та завдання, аналізувати і порівнювати альтернативи, оцінювати ресурси.	РН16
Відшуковувати необхідну інформацію в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об’єктивно оцінювати інформацію.	РН17
Визначати закономірності і аналізувати суспільні процеси, що відбувалися у минулому та відбуваються нині, розуміти їх зв'язки та проводити історичні паралелі.	РН19

- формування у здобувачів вищої освіти наступних компетентностей:

Програмні компетентності	К
Здатність до пошуку, оброблення та аналізу інформації з різних джерел.	К01
Здатність приймати обґрунтовані рішення.	К03
Здатність діяти соціально відповідально та свідомо.	К04
Здатність оцінювати та забезпечувати якість виконуваних робіт.	К05
Здатність генерувати нові ідеї (креативність).	К07
Здатність приймати ефективні рішення, керувати роботою колективу під час професійної діяльності.	К08
Здатність до превентивного і оперативного (аварійного) планування, управління заходами безпеки професійної діяльності.	К09

Здатність до проведення техніко-економічного аналізу, оцінювання ризиків, комплексного обґрунтування проектів, планів, рішень, їх реалізації у сфері цивільної безпеки.	К10
Здатність до застосування інноваційних підходів, сучасних методів, спрямованих на регулювання техногенної та виробничої безпеки.	К11
Здатність до створення і реалізації інноваційних продуктів і заходів у сфері професійної діяльності.	К12
Здатність організовувати та проводити моніторинг за визначеними об'єктами, явищами та процесами, аналізувати його результати та розроблювати науково-обґрунтовані рекомендації на підставі отриманих даних.	К14

Програма навчальної дисципліни

Теми навчальної дисципліни:

МОДУЛЬ 1. Сутність кібербезпеки. Кібербезпека як важлива складова всієї системи захисту держави.

Тема 1.1. Основні засади забезпечення кібербезпеки України.

Вступ. Кібербезпека - як складова системи захисту держави. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. Огляд основних положень. Визначення понять та термінів у сфері кібербезпеки України**.**

Тема 1.2. Система суб'єктів забезпечення кібербезпеки в Україні.

Об'єкти кібербезпеки та кіберзахисту. Суб'єкти забезпечення кібербезпеки. Порядок формування переліку об'єктів критичної інформаційної інфраструктури**.**

Тема 1.3. Національний кіберпростір: виклики та кіберзагрози.

Основні виклики та загрози України у сфері кібербезпеки. Передумови та чинники, які формують загрози у сфері кібербезпеки України. Національна система кібербезпеки: засади розбудови. Пріоритети забезпечення кібербезпеки України та стратегічні цілі.

Тема 1.4. Стратегія кібербезпеки України. Стратегічні завдання та напрями.

Кібербезпека: глобальний контекст. Стратегічні завдання щодо розбудови національної системи кібербезпеки. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки.

Тема 1.5. Міжнародні аспекти кібербезпеки в умовах глобалізації.

Міжнародне співробітництво у сфері кібербезпеки. Міжнародні аспекти

кібербезпеки в умовах глобалізації. Відповідальність за порушення законодавства з кібербезпеки.

Розподіл дисципліни у годинах за формами організації освітнього процесу та видами навчальних занять:

Назви модулів і тем	Очна (денна) форма здобуття освіти					
	Кількість годин					
	усього	у тому числі				
		лекції	практичні (семінарські) заняття	лабораторні заняття	самостійна робота	модульна контрольна робота
3-й семестр						
Модуль 1. Сутність кібербезпеки. Кібербезпека як важлива складова всієї системи захисту держави.						
Тема 1.1. Основні засади забезпечення кібербезпеки України.	18	2	2	-	14	-
Тема 1.2. Система суб'єктів забезпечення кібербезпеки в Україні.	20	2	2	-	16	-
Тема 1.3. Національний кіберпростір: виклики та кіберзагрози.	18	2		-	16	-
Тема 1.4. Стратегія кібербезпеки України. Стратегічні завдання та напрями.	18	2			16	
Тема 1.5. Міжнародні аспекти кібербезпеки в умовах глобалізації.	16	2			14	
Разом за модулем 1	90	10	4	-	76	-

Назви модулів і тем	Заочна (дистанційна) форма здобуття освіти					
	Кількість годин					
	усього	у тому числі				
		лекції	практичні (семінарські) заняття	лабораторні заняття	самостійнаробота	модульна контрольна робота
3-й семестр						
Модуль 1. Сутність кібербезпеки. Кібербезпека як важлива складова всієї системи захисту держави.						
Тема 1.1. Основні засади забезпечення кібербезпеки України.	18	2	2	-	14	-
Тема 1.2. Система суб'єктів забезпечення кібербезпеки в Україні.	20	2	2	-	16	-
Тема 1.3. Національний кіберпростір: виклики та кіберзагрози.	18	2	-	-	16	-
Тема 1.4. Стратегія кібербезпеки України.	18	2	-	-	16	-

Стратегічні завдання та напрями.						
Тема 1.5. Міжнародні аспекти кібербезпеки в умовах глобалізації.	16	2	-	-	14	-
Разом за модулем 1	90	10	4	-	76	-

Теми лекційних занять

№ з/п	Назва теми	Кількість годин
МОДУЛЬ 1. Сутність кібербезпеки. Кібербезпека як важлива складова всієї системи захисту держави.		
1.	**Лекція 1. Основні засади забезпечення кібербезпеки України.** 1. Вступ. Поняття кібербезпеки. Визначення термінів. 2. Кібербезпека - як складова системи захисту держави. 3. Закон України «Про основні засади забезпечення кібербезпеки України»від 5 жовтня 2017 року № 2163-VIII. Огляд основних положень. 4. Визначення понять та термінів у сфері кібербезпеки України.	2
2.	**Лекція 2. Система суб'єктів забезпечення кібербезпеки в Україні.** 1. Об'єкти кібербезпеки та кіберзахисту. 2. Суб'єкти забезпечення кібербезпеки. 3. Порядок формування переліку об'єктів критичної інформаційної інфраструктури.	2
3.	**Лекція 3. Національний кіберпростір: виклики та кіберзагрози.** 1. Основні виклики та загрози України у сфері кібербезпеки. 2. Передумови та чинники, які формують загрози у сфері кібербезпеки України. 3. Національна система кібербезпеки: засади розбудови. 4. Пріоритети забезпечення кібербезпеки України та стратегічні цілі.	2
4.	**Лекція 4. Стратегія кібербезпеки України. Стратегічні завдання та напрями.** 1. Кібербезпека: глобальний контекст. 2. Стратегічні завдання щодо розбудови національної системи кібербезпеки. 3. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки.	2
5.	**Лекція 5. Міжнародні аспекти кібербезпеки в умовах глобалізації.** 1. Міжнародне співробітництво у сфері кібербезпеки**.** 2. Міжнародні аспекти кібербезпеки в умовах глобалізації. 3. Відповідальність за порушення законодавства з кібербезпеки.	2

Теми семінарських занять

№ з/п	Назва теми	Кількість годин
МОДУЛЬ 1. Державне регулювання у сфері цивільного захисту		
1.	Семінарське заняття 1.1. Об'єкти кібербезпеки та кіберзахисту. Суб'єкти забезпечення кібербезпеки.	2
2.	Семінарське заняття 1.2. Правове регулювання кібербезпеки в Україні.	2
Всього:		4

Орієнтовна тематика індивідуальних завдань

Теми рефератів:

1. Принципи та функції забезпечення кібербезпеки.
2. Методи забезпечення кібербезпеки.
3. Забезпечення кібербезпеки України.
4. Засоби для ураження і знищення інформаційної системи.
5. Основні способи застосування кіберзброї.
6. Об'єкти деструктивного інформаційного впливу.
7. Департамент кібербезпеки в України та Кіберполіція: основні задачі та функції.
8. Види загроз та способи захисту інформації.
9. Кібербезпека і захист прав людини.
10. Права і свободи людини, громадянина та їх обов'язки в сфері кібербезпеки.

Тези доповіді для участі у Всеукраїнській науково-практичній конференції «Організаційно-управлінське та економіко-правове забезпечення діяльності Єдиної державної системи цивільного захисту (ЄДСЦЗ)», на секцію «Нормативно-правове регулювання ЄДСЦЗ: стан та проблеми».

Оцінювання освітніх досягнень здобувачів вищої освіти

Засоби оцінювання

Засобами оцінювання та методами демонстрування результатів навчання є: теоретичне опитування (усне або письмове), тестування, виконання практичних завдань, доповіді, реферати, презентації результатів виконаних завдань та досліджень, студентські презентації та виступи на наукових заходах, заліки, іспит.

Оцінювання рівня освітніх досягнень здобувачів за освітніми компонентами, здійснюється за 100-бальною шкалою, що використовується в ЧІПБ імені Героїв Чорнобиля НУЦЗ України з переведенням в оцінку за рейтинговою шкалою – ЄКТС та в 4-бальну шкалу.

Таблиця відповідності результатів оцінювання знань з навчальної дисципліни за різними шкалами

За 100-бальною шкалою	За рейтинговою шкалою (ЄКТС)	За 4-бальною шкалою
90–100	A	відмінно
80–89	B	добре
65–79	C	
55–64	D	задовільно
50–54	E	
35–49	FX	незадовільно
0–34	F	

Критерії оцінювання

Форми поточного та підсумкового контролю

Поточний контроль результатів навчання здобувачів вищої освіти проводиться у формі індивідуального опитування, проведення термінологічних диктантів, виконання письмових завдань, вирішення практичних ситуацій, виконання тестових завдань, модульної контрольної роботи.

Розподіл та накопичення балів, які отримують здобувачі, за видами навчальних занять та контрольними заходами з дисципліни

Модуль 1

Види навчальних занять		Кількість навчальних занять	Максимальний бал за вид навчального заняття	Сумарна максимальна кількість балів за видами навчальних занять
І. Поточний контроль				
Модуль 1	лекції	5	-	-
	семінарські заняття	2	8*	50
	модульна робота	1	20	20
Разом за модуль 1				70
Разом за поточний контроль				
ІІ. Індивідуальні завдання (науково-дослідне):				не більше 20
- написання реферату - виступ на студентській науковій конференції з публікацією тез - підготовка та публікація наукової статті				5 10 10
ІІІ. Підсумковий контроль (модульна робота)				30
Разом за всі види навчальних занять та контрольні заходи				100

Примітки:*В таблиці зазначено 8 балів – це максимальний бал за 2-ме семінарське заняття.

Поточний контроль

Поточний контроль проводиться на кожному семінарському занятті. Він передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначеної теми (у тому числі, самостійно опрацьованого матеріалу) під час роботи на занятті та набуття навичок під час виконання відповідних завдань.

Критерії поточного оцінювання знань здобувачів на семінарському занятті(оцінюється в діапазоні від 0 до 8 балів):

4-8 балів – завдання виконане в повному обсязі, відповідь вірна, наведено аргументацію, використовуються професійні терміни, граматично і стилістично без помилок оформлено роботу;

3 бали – завдання виконане, але обґрунтування відповіді недостатнє, у роботі допущені незначні граматичні чи стилістичні помилки;

2 бали – завдання виконане частково, у роботі допущені незначні граматичні чи стилістичні помилки;

1 бал – завдання виконане частково, у роботі допущені значні граматичні чи стилістичні помилки;

0 балів – завдання не виконане.

Доповнення виступу:

1 бал – отримують здобувачі вищої освіти, які глибоко володіють матеріалом, чітко визначили його зміст; зробили глибокий системний аналіз змісту виступу, виявили нові ідеї та положення, що не були розглянуті, але суттєво впливають на зміст доповіді, надали власні аргументи щодо основних положень даної теми.

Запитання до доповідачів:

1 бал – отримують здобувачі вищої освіти, які своїм запитанням до виступаючого суттєво і конструктивно можуть доповнити хід обговорення теми.

Викладачем оцінюється повнота розкриття питання, цілісність, системність, логічна послідовність, вміння формулювати висновки, використання основної та додаткової літератури.

Бали, отримані здобувачами вищої освіти за результатами поточного контролю з дисципліни викладач оголошує в кінці кожного семінарського заняття та виставляє в Журнал обліку роботи академічної групи.

Сумарна кількість отриманих балів з кожного виду навчальної діяльності здобувача вищої освіти за різними формами поточного контролю виставляється викладачем у Журнал обліку роботи академічної групи.

Сума балів, яку накопичив здобувач вищої освіти в результаті поточного навчання, є складовою загальної підсумкової оцінки з дисципліни відповідно до виду підсумкового контролю.

Модульний контроль

Критерії оцінювання знань здобувачів під час виконання модульних контрольних робіт(оцінюється в діапазоні від 0 до 20 балів):

20 балів – надана послідовна та повна відповідь на поставлені три

питання і правильно дані відповіді на тестові питання;

16-19 балів – у відповіді зроблена незначна помилка, при повних знаннях програмного матеріалу, повна відповідь на перші два питання та неповна відповідь на третє питання або є неправильні відповіді на тестові питання;

11-15 балів – у відповіді на питання зроблені деякі незначні помилки, при повних знаннях програмного матеріалу, повна відповідь на перші два питання, помилки в відповідях на тестові питання;

6-10 балів – у відповіді зроблено деякі помилки, при не повних знаннях програмного матеріалу, повна відповідь на перше питання та неповна відповідь на друге і третє питання, помилки в відповідях на тестові питання;

1-5 балів – недостатня повнота викладення матеріалу, наявність неточностей при викладенні теоретичних питань. Порушення логічної послідовності викладення матеріалу. Не повні відповіді на всі питання. Помилки в відповідях на тестові питання;

0 балів – правильні відповіді на питання та тестові питання відсутні.

Сума балів, яку накопичив здобувач вищої освіти за результатами виконання модульної контрольної роботи, є складовою загальної підсумкової оцінки з дисципліни. Результати модульного контролю виставляються викладачем у Журнал обліку роботи академічної групи.

Індивідуальні завдання

Критерії оцінювання знань здобувачів при виконанні індивідуальних завдань (оцінюється в діапазоні від 0 до 10 балів)

Викладачем оцінюється понятійний рівень здобувача, логічність та послідовність під час підготовки індивідуального завдання, самостійність мислення, впевненість в правоті своїх суджень, вміння виділяти головне, вміння встановлювати міжпредметні та внутрішньодисциплінарні зв’язки, вміння робити висновки, показувати перспективу розвитку ідеї або проблеми, уміння публічно чи письмово представити звітнийматеріал.

Індивідуальна самостійна робота є однією з форм роботи здобувача, яка передбачає створення умов для повної реалізації його творчих можливостей, застосування набутих знань на практиці.

Здобувачу вищої освіти необхідно обрати одну з рекомендованих тем та самостійно виконати індивідуальне завдання, результати якого оформити у відповідній формі (реферат, презентація, тези доповіді на конференцію, наукова публікація).

Підсумковий контроль

Підсумковий контроль проводиться з метою оцінки результатів навчання на завершальному етапі, проводиться у формі диференційованих заліків та іспиту.

Критерії оцінювання знань здобувачів на диференційованомузаліку, іспиті (оцінюється від 0 до 40балів):

30-40 балів – здобувач вищої освіти в повному обсязі володіє навчальним матеріалом, глибоко та всебічно розкрив зміст теоретичних питань;

20-30 балів – здобувач вищої освіти достатньо повно володіє навчальним матеріалом, в основному розкрив зміст теоретичних питань, але при наданні відповіді на деякі питання є певні неточності;

10-19 балів – в цілому здобувач вищої освіти володіє навчальним матеріалом, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки;

5-9 балів – здобувач вищої освіти не в повному обсязі володіє навчальним матеріалом, недостатньо розкрив зміст теоретичних питань, допускаючи при цьому суттєві неточності;

1-4 бали – здобувач вищої освіти лише частково володіє навчальним матеріалом, відповіді загальні, при цьому допущено суттєві помилки;

0 балів – здобувач вищої освіти не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань.

Перелік теоретичних питань для підготовки до заліку:

1. Цифрова революція: поняття та становлення.
2. Зміст та ознаки кіберполітики.
3. Засади формування кіберполітичної функції держави.
4. Стан наукових досліджень правової кіберполітики.
5. Поняття та правовий зміст кіберзагроз.
6. Нормативно-правове регулювання кіберзагроз в Україні.
7. Класифікація кіберзагроз та їх зміст.
8. Поняття та загальна характеристика суб’єктів кіберполітики.
9. Класифікація суб’єктів забезпечення кіберполітики.
10. Повноваження спеціальних суб’єктів забезпечення кіберполітики України.
11. Поняття та основний зміст кібербезпеки.
12. Роль та значення інформаційних ресурсів у розвитку людства.
13. Кібернетика і кібернетичний підхід.
14. Системний та матричний підхід вивчення кібербезпеки.
15. Чинники, які впливають на інформаційний суверенітет.
16. Оцінка стану національного інформаційного суверенітету у сучасних умовах.
17. Витоки та наслідки соціальних мереж.
18. Основні принципові наслідки глобалізації інформаційного простору.
19. Поняття національної системи кібербезпеки.
20. Поняття системи забезпечення кібербезпеки.
21. Об’єкти правовідносин у сфері кібербезпеки.
22. Зміст правовідносин у сфері кібербезпеки.
23. Поняття кіберполітики, її природа, ознаки та особливості.
24. Загальна характеристика формування кіберполітичних функцій держави.
25. Сучасний стан досліджень правової кіберполітики.
26. Сучасний правовий зміст державної кібербезпекової політики.
27. Напрями державної кібербезпекової політики відповідно до Закону України «Про основні засади забезпечення кібербезпеки України».
28. Напрями державної кібербезпекової політики відповідно до Закону України

«Про основи національної безпеки України».
29. Напрями державної кібербезпекової політики відповідно до Доктрини інформаційної безпеки України
30. Поняття агентів впливу.
31. Поняття та загальна характеристика лобізму в кібербезпековій політиці.
32. Правові та організаційні засади формування фахівців із кібербезпеки
33. Стан підготовки фахівців у сфері кібербезпеки.
34. Напрями підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки.
35. Поняття та дефініції кіберпростору.
36. Публічність кіберпростору та соціальні мережі
37. Сфера міжнародних та публічних відносин у кіберпросторі.
38. Електронна демократія та електронне урядування.
39. Інтернет дипломатія.
40. Кібервійна та кіберзлочинність.
41. Кібертехнології: поняття та загальна характеристика.
42. Україна в контексті кіберполітики на ранньому етапі.
43. Глобальна мережа в контексті революційних подій в Україні.
44. Російсько-українська кібервійна.
45. Сьогодення та майбутнє України в контексті кіберполітики.
46. Стан кіберполітики провідних держав світу.
47. Особливості державотворення інформаційними потоками.
48. Кіберзагроза : поняття та правовий зміст.
49. Критичні об’єкти національної інформаційної інфраструктури.
50. Особливості електронного голосування та електроні петиції, як елементи політичного процес.

МОДУЛЬ 1. Сутність кібербезпеки. Кібербезпека як важлива складова всієї системи захисту держави.

1. Визначіть поняття «кібербезпека».
2. Охарактеризуйте сутність забезпечення кібербезпеки.
3. Які існують життєво важливі інтереси особи, держави та суспільства в електронній сфері?
4. Принципи та функції забезпечення кібербезпеки.
5. Методи забезпечення кібербезпеки.
6. Забезпечення кібербезпеки України.
7. Геополітичні особливості сучасного інформаційного простору.
8. Основні об’єкти при застосуванні кіберзброї у мирний та воєнний час.
9. Засоби для ураження і знищення інформаційної системи.
10. Основні способи застосування кіберзброї.
11. Об’єкти деструктивного інформаційного впливу.
12. Національна система кібербезпеки: засади розбудови
13. Міжнародне співробітництво в сфері кібербезпеки.
14. Кібербезпека і захист прав людини.
15. Правове регулювання кібербезпеки в Україні.

Політика викладання навчальної дисципліни

1. Сумлінне дотримання розкладу занять з навчальної дисципліни (здобувачі вищої освіти, які запізнилися, до заняття не допускаються).
2. Активна участь в обговоренні навчальних питань, попередня підготовка до семінарських занять за рекомендованою літературою, якісне і своєчасне виконання завдань та обов'язкове виконання самостійних завдань, наданих викладачем.
3. Користуватися мобільними пристроями під час заняття дозволяється тільки з дозволу викладача і лише з навчальною метою.
4. Здобувач вищої освіти має право дізнаватися свою кількість накопичених балів у викладача навчальної дисципліни або в журналі обліку навчальних занять взводу (групи).
5. При виконанні індивідуальної самостійної роботи до захисту допускаються роботи, що містять не менше 60 % оригінального тексту при перевірці на плагіат.

Рекомендовані джерела інформації

Базова література:

1. Кібербезпека як складова економічної безпеки україни. Станіслав Горбаченко Одеський національний університет імені І. І. / Електронний ресурс. Режим доступу: https://galicianvisnyk.tntu.edu.ua /pdf/66/903.pdf.
2. Конституція України./ Електронний ресурс. Режим доступу:https://www.president.gov.ua/documents/constitution.
3. Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) від 5 жовтня 2017 року № 2163-VIII.
4. Закон України "Про основи національної безпеки України".
5. Сліпченко Т. О. Кібербезпека як складова системи захисту національної безпеки: європейський досвід. Актуальні проблеми правознавства. 2020. № 1 (21). С. 128–133. https://doi.org/10.35774/app2020.01.128.
6. Стратегія кібербезпеки України: затв. Указом Президента України від 15 берез. 2016 р. URL: https:// www.president.gov.ua/documents/962016-19836.
7. Тарасюк А.В. Науково-дослідний інститут інформатики і права Національної академії правових наук України.Система суб'єктів забезпечення кібербезпеки в Україні. Режим доступу: https://juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_2/25.pdf.
8. Ліпкан В.А., Ліпкан О.С. Національна і міжнародна безпека у визначеннях та поняттях. Київ : Текст, 2008. 400 с.
9. Тімкін І.Ф., Новікова Н.Є. Структурно-функціональна характеристика системи забезпечення національної безпеки України. URL: er.nau.edu.ua.
10. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ : ТОВ «Видавничий

дім «АртЕк», 2018. 422 с.

11. Бухарєв В.В. Адміністративно-правові засади забезпечення кібербезпеки України : дис. ... канд. юрид. наук : 12.00.07. Суми, 2018. 221 с.

12. Ткачук Т.Ю. Суб'єкти забезпечення інформаційної безпеки держави: функціональний аналіз. Jurnalul juridic national: teorie şi practică. 2017. № 6. С. 42–46.

13. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України». URL: https://zakon5.rada.gov.ua/laws/show/96/2016.

14. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». URL: https://zakon.rada.gov.ua/laws/show/3475-15.

15. Закон України «Про національну поліцію». URL: https://zakon.rada.gov.ua/ laws/show/580-19.

16. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19.

17. Закон України «Про Службу безпеки України». URL: https://zakon.rada.gov.ua/laws/show/2229-12.

18. Указу Президента України № 27/2020 «Про внесення змін до Указів Президента України від 27 січня 2015 р. № 37 та від 7 червня 2016 р. № 242». URL: https://www.president.gov.ua/ documents/ 272020-32041.

19. Конвенція про захист прав людини і основоположних свобод.

20. Конвенція про кіберзлочинність.

21. Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392.

22. Концепція боротьби з тероризмом в Україні, затверджена Указом Президента України від 5 березня 2019 року № 53, інших нормативно-правових актів.

23. Ю.П. Лісовська кібербезпека: ризики та заходи. Навчальний посібник. Київ. 2019. URL : http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf.

24. Петрик В. Щодо визначення кібербезпеки та її різновидів / В. Петрик // Форми та методи забезпечення кібер- 261 безпеки держави : зб. матер. міжнар. наук.-практ. конф. (м. Київ, 13 березня 2008 р.). — К. : Видавець Захаренко В.О., 2008. — 216 с.

25. Бесчастний В. Міжнародний досвід у діяльності міліції України // Віче. Грудень, 2009. — № 24. URL : http://veche. kiev.ua/joLirnal/1780/7feed (дата звернення: 06.03.2018).

Додаткова:

26. Мялковський Д. В. Організаційно-правові механізми державного управління міжнародним співробітництвом України у сфері кібербезпеки [Електронний ресурс] / Д. В. Мялковський // Теорія та практика державного управління. - 2019. - Вип. 3. - С. 216-226. - Режим доступу: http://nbuv.gov.ua/UJRN/Tpdu_2019_3_28

27. Семенченко А. І. Організаційно-правові механізми державного управління забезпеченням кібербезпеки та кіберзахисту України: сутність, стан та перспективи розвитку [Електронний ресурс] / А. І. Семенченко, В. Л.

Плескач, О. А. Заярний, М. В. Плескач // Проблеми програмування. - 2020. - № 2-3. - С. 278-286.

28. Шпачук В. В. Державне управління кібербезпекою України: правовий аспект [Електронний ресурс] / В. В. Шпачук. // Державне управління: удосконалення та розвиток. - 2018. - № 11. - Режим доступу: http://nbuv.gov.ua/UJRN/Duur_2018_11_6.

29. Філінович В. В. Кібербезпека та Інтернет речей: правовий аспект [Електронний ресурс] / В. В. Філінович // Юридичний вісник. Повітряне і космічне право. - 2020. - № 4. - С. 122-127. - Режим доступу: http://nbuv.gov.ua/UJRN/Npnau_2020_4_19.

30. Інформаційні ресурси: Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс] – Режим доступу до ресурсу: https://cip.gov.ua/.

Розробник:

Старший викладач
кафедри управління
у сфері цивільного захисту  Віталій КОСТЕНКО