Силабус курсу

Протидія кіберзлочинності

Ступінь вищої освіти – бакалавр

Галузь знань 25 «Воєнні науки, національна безпека, безпека національного кордону»
Спеціальність 256 «Національна безпека (за окремими сферами забезпечення та видами діяльності)»

Освітньо-професійна програма «Національна безпека (за окремими сферами забезпечення та видами діяльності)»

Рік навчання: 2, Семестр: 3,4

Кількість кредитів: 5 Мова викладання: українська

Керівник курсу

к.е.н., доцент, в.о.зав. кафедри безпеки та правоохоронної діяльності

Муравська Юлія Євгенівна

Контактна інформація yakubivskay@gmail.com, +380970134613

Опис дисципліни

«Протидія кіберзлочинності» є дисципліною, яка сприяє підготовці фахівців у національної безпеки. Дисципліна «Протидія кіберзлочинності» вивчає закономірності та організаційно-економічні механізми побудови й відтворення стану безпечного, захищеного розвитку сфери кібербезпеки на рівні держави і окремих суб'єктів господарювання.

Мета навчальної дисципліни полягає в формуванні комплексних знань про правове регулювання запобігання кіберзлочинності, вивченні національних і міжнародних підходів до забезпечення кібербезпеки, розвитку ключових навичок застосування національного законодавства, активізації аналітичної роботи студентів, проведенні наукових досліджень і формуванні практичних навичок правозастосування.

Одержані теоретичні знання дадуть змогу студентам та слухачам у майбутньому як фахівцям у сфері правоохоронної діяльності вміти вирішувати такі завдання: ідентифікувати внутрішні та зовнішні загрози, виявляти загрози кібербезпеки на рівні держави; прогнозувати наслідки реалізації загроз / ризиків для національної економіки; обґрунтовувати напрями подолання загроз та нейтралізації ризиків національної економічної безпеки в сфері кібербезпеки; розробляти механізми узгодження інтересів суб'єктів відносин кібербезпеки, заходи з подолання кіберзлочинності при міжнародному науково-технічному співробітництві, запобігання інформаційному шпигунству; виявляти потенційні шляхи втрати об'єктів критичної інфраструктури від кіберзагроз.

Структура курсу

Години (лек. / пр.)	Тема	Результати навчання	Завдання
2 / 2	Тема 1. Протидія кіберзлочинності в системі забезпечення національної економічної безпеки	Визначення поняття та формування системи протидії кіберзлочинності в контексті національної безпеки	Питання для обговорення
2 / 2	Тема 2. Об’єкти та суб’єкти системи протидії кіберзлочинності	Засвоїти та закріпити теоретичні знання щодо питання сутності об’єктів та суб’єктів протидії кіберзлочинності в системі інформаційної безпеки	Тести, питання
2 / 2	Тема 3. Кіберзлочин	Засвоїти та закріпити теоретичні знання щодо питання сутності кіберзлочину	Тести, задачі, питання
2 / 2	Тема 4. Кіберзлочинність	Засвоїти та закріпити теоретичні знання щодо питання сутності кіберзлочинності	Тести, задачі, питання
2 / 2	Тема 5. Фактори впливу на кіберзлочинність	Навчитися аналізувати фактори впливу на кіберзлочинність	Тести, задачі, питання
2 / 2	Тема 6. Ознаки кіберзлочинності в умовах воєнного стану	Глибше засвоїти та закріпити теоретичні знання щодо ідентифікації ознак кіберзлочинності в умовах воєнного стану	Тести, питання
2 / 2	Тема 7. Кіберзлочинець	Ознайомлення з особливостями категорії «кіберзлочинець»	Тести, питання
2 / 2	Тема 8. Кіберзлочинність проти конфіденційності, цілісності та доступності комп’ютерних	Вивчення особливостей кіберзлочинності проти конфіденційності, цілісності та доступності комп’ютерних даних і систем	Тести, кейси

	даних і систем		
2 / 2	Тема 9 . Кіберзлочинність, пов’язана з використанням комп’ютера як засобу скоєння злочинів	Вивчення особливостей кіберзлочинності, пов’язаної з використанням комп’ютера як засобу скоєння злочинів	Тести, питання
2 / 2	Тема 10. Кіберзлочинність, пов’язана з з контентом (змістом даних), розміщених у комп’ютерних мережах	Вивчення особливостей кіберзлочинності, пов’язаної з контентом (змістом даних), розміщених у комп’ютерних мережах	Тести, питання
2 / 2	Тема 11. Кіберзлочинність, пов’язана з порушенням авторського права і суміжних прав	Вивчення особливостей кіберзлочинності, пов’язаної з порушенням авторського права і суміжних прав	Тести, питання
2 / 2	Тема 12. Кіберзлочинність, зафіксована в окремому протоколі	Вивчення особливостей кіберзлочинності, зафіксованої в окремому протоколі	Тести, задачі, питання
2 / 2	Тема 13. Кіберзлочинність у сфері економіки	Вивчення особливостей кіберзлочинності у сфері економіки	Питання
2 / 2	Тема 14. Кіберзлочинність у сфері обігу наркотичних засобів	Вивчення особливостей кіберзлочинності у сфері обігу наркотичних засобів	Кейси
2 / 2	Тема 15. Кіберзлочинність	Вивчення особливостей кіберзлочинності та гібридних воєн	Тести, питання

	та гібридна війна		

Літературні джерела

Нормативно-правові акти:

1. Кримінальний кодекс України: Закон України від 05. 04. 2001 р. № 2341-III із змін., внес. згідно із Законами України та Рішеннями Конституційного Суду. Електрон. дан. (1 файл). URL : https://zakon.rada.gov.ua/laws/show/2341-14.
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text
3. «Про інформацію»: Закон України від від 02.10.1992 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
4. «Про захист персональних даних»: Закон України від 01.06.2010 р. № 2297-VI URL : // https://zakon.rada.gov.ua/laws/show/2297-17
5. «Про електронні довірчі послуги»: Закон України від 05.10.2017 р. № 2155-VIII URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.
6. «Про основні засади забезпечення кібербезпеки України»: Закону України від 05.10.2017 р. № 2163-VIII URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text
7. «Про національну безпеку України»: Закон України від 21.06.2018 р. № 2469-VIII URL : https://zakon.rada.gov.ua/laws/show/2469- 19#Text
8. «Про кіберзлочинність»: Конвенція ратифіковано із застереженнями і заявами Законом N 2824-IV ( ) від 07.09.2005, URL : https://zakon.rada.gov.ua/laws/show/994_575#Text
9. «Про Стратегію кібербезпеки України»: Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text

Основні джерела інформації:

1. Muravska Yuliia. Theoretical and conceptual approaches to defining the concept and forms of economic intelligence.in the Ukrainian scientific practice. Osteuropa-Recht. 2022. Vol. 4. P. 476-485.
2. Муравська Ю. Побудова ефективної системи національної безпеки України як передумова євроінтеграції. Наукові заходи Юридичного факультету Західноукраїнського національного університету. 2022: Пріоритети зміцнення безпеки держави та підвищення ефективності правоохоронної діяльності: національні та міжнародні контексти (Тернопіль, 6 травня 2022 р.)
3. http://confuf.wunu.edu.ua/index.php/confuf/article/view/829
4. Муравська (Якубівська) Ю. Є. Інформаційна безпека суспільства: концептуальний аналіз / Ю. Є. Муравська (Якубівська) // Економіка та суспільство [Електронне наукове фахове видання]. - № 9. – Мукачево : Мукачівський державний університет, 2017. Режим доступу: http://www.economyandsociety.in.ua/
5. Муравська (Якубівська) Ю. Є. Формування понятійного апарату у сфері кібербезпеки: іноземний досвід та нормативно-правова регламентація / Ю. Є. Муравська (Якубівська) // Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід: [Матеріали II Міжнародній науково-практичній конференції, м. Тернопіль, 21-22 квітня 2017 р.]. – Тернопіль: Економічна думка, 2017. – С.362-365.

6. Муравська (Якубівська) Ю. Є. Термінологічна та нормативно-правова невизначеність у сфері кібербезпеки / Ю. Є. Муравська (Якубівська) // Збірник тез доповідей всеукраїнської науково-практичної конференції «Тактичні та стратегічні пріоритети зміцнення фінансово-економічної безпеки держави», м. Тернопіль, 21 квітня 2017 р., ТНЕУ. – Тернопіль, 2017. – С. 56-59.
7. Карапетян О.М., Будник Л.А., Метельський І.Д. Кіберзлочини: типології, фінансова розвідка, використання спеціальних знань. Актуальні проблеми правознавства. 2022. Вип. 3. С. 115-120.
8. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи / Тарасюк А. В. : монографія / А. В. Тарасюк. – Київ; Одеса : Фенікс, 2020. – 404 с.
9. Захист прав, приватності та безпеки людини в інформаційну епоху / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с.
10. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. Інформація і право. № 1(28)/2019. С. 108-117.
11. Viacheslav V. Vapniarchuk, Iryna I. Puchkovska, Oleksii V. Tavolzhanskyi, Roman I. Tashian Protection of ownership right in the court: the essence and particularities (Захист права власності в суді) // Asia life science, Supplement 21(2), December 2019. Iss. 2. P. 863-879. Філіпини. (Scopus) https://www.scopus.com/record/display.uri?eid=2-s2.0-85077221643&origin=resultslist
12. V. Tsypko, K. I. Alieksieieva, I. A. Venger, O. V. Tavolzhanskyi, N. I. Galunets, A. V. Klyuchnik. Information policy of the enterprise as the basis for the reproduction of human potential in the structure of public social interaction () // Journal of Advanced Research in Law and Economics (Журнал перспективных исследований в области права и экономики). - 2019. Румыния. - Vol. 10 Issue 6.- P.1664-1672. (Scopus) https://www.scopus.com/record/display.uri?eid=2-s2.0-85087468504&origin=resultslist

Додаткова література

1. Таволжанський О.В. Інформаційна безпека України: стан правового забезпечення в контексті глобалізаційних процесів.// Журнал східноєвропейського права. – 2018. - № 56. – С. 90-105. (0,71 д.а). Таволжанський О.В. (у співавт.) International Experience of the Process of Re- Socialization of Convicts // Журнал східноєвпроейського права. – 2019. - № 63. – С. 125-136.
2. Кримінологія : підручник / Б. М. Головкін, В. В. Голіна, О. Ю. Шостко та ін.; за ред. Б. М. Головкіна. – Харків : Право, 2020
3. Карчевський М.В. Правове регулювання соціалізації штучного інтелекту. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. Науково-теоретичний журнал. 2017. С. 99-08.
4. Таволжанський О. В. Основи державної кіберполітики України: формування та реалізація / О. В. Таволжанський // Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія : Право. - 2017. - № 4. - С. 158-164. - Режим доступу: http://nbuv.gov.ua/UJRN/Nivif_2017_4_27
5. Гладка Н. М. Боротьба з кіберзлочинністю: напрями вдосконалення кримінального законодавства України [Електронний ресурс] / Н. М. Гладка // Науковий вісник Ужгородського національного університету. Серія : Право. - 2020. - Вип. 60. - С. 139-142.
6. Леонов Б. Д. Методичне забезпечення заходів з класифікації ідентифікації та фіксації кіберзлочинів [Електронний ресурс] / Б. Д. Леонов, В. С. Серьогін // Інформація і право. - 2021. - № 1. - С. 99-105

7. Саєнко М. І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству [Електронний ресурс] / М. І. Саєнко, Є. А. Савела, Ю. Ю. Тополянський // Науковий вісник Ужгородського національного університету. Серія : Право. - 2021. - Вип. 64. - С. 386-391.
8. Волощук В., Заєць К., Муравська Ю. Національна безпека як інструмент збереження української державності. Актуальні проблеми правознавства. 2 (38)/2024. С. 111-117.
9. Zaiets K., Muravska Yu., Slipchenko T., Kaniuka V., Melnyk I. The etymology of the concept “military conflict” as a determinant of political orientation. Law, Policy and Security, 2(2), 39-51.

Політика оцінювання

У процесі вивчення дисципліни «Протидія кіберзлочиннисті» використовуються такі засоби оцінювання та методи демонстрування результатів навчання: поточне опитування, тестування; презентації результатів виконаних завдань; результати модульного контролю; оцінювання результатів самостійної роботи; інші види індивідуальних і групових завдань; екзамен.

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань студентами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу студент може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими студентами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. Відвідування занять є обов’язковим. За об’єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування тощо) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Підсумковий бал (за 100-бальною шкалою) з дисципліни “Протидія кіберзлочинності” визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2		Модуль 3	Модуль 4
20%	20%	20%	20%	5%	15%
Усне опитування (тестування) на заняттях: Теми 1-7. Поточне оцінювання Оцінка за поточне оцінювання визначається як середнє арифметичне з оцінок отриманих під час занять	Модульний контроль 1 включає 20 тестів. Теми 1-7. Модульний контроль 1 планувати на проведених занять. Модульний контроль проводити в системі Мудл	Усне опитування (тестування) на заняттях: Теми 8-15. Поточне оцінювання Оцінка за поточне оцінювання визначається як середнє арифметичне з оцінок отриманих під час занять	Модульний контроль 2 включає 20 тестів. Теми 8-15. Модульний контроль 2 планувати на проведених занять. Модульний контроль проводитться в системі Мудл	Тренінги Тренінг з дисципліни пропонує 2 завдання різного змісту на кожного студента (Виконання завдань: №1-5 ((на вибір), Студенти отримують одне із завдань (на вибір), формуючи групи. Критерії оцінювання залежать від окремо взятого завдання та описані в розділі Тренінг. Оцінка за тренінг визначається як середнє арифметичне з	Визначається як середнє арифметичне з оцінок, отриманих під час вивчення дисципліни за самостійну роботу: - наукового есе на актуальну для воєнного стану тематику. - Опрацювання розділів програми, які не виносяться на лекції (тематика

				відповідностей критеріям виконання. Результати виконання тренінгу подаються у вигляді презентації або відеоролику.	подана у розділі Самостійна робота).

Поточне оцінювання під час заняття:

90-100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час відповідей, глибоко та всебічно розкриває зміст теоретичних питань.

75-89 балів – достатньо повно володіє навчальним матеріалом, але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки.

65-74 бали – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки.

60-64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності.

1-59 балів – не володіє навчальним матеріалом, не розкриває зміст теоретичних питань.

Тестування під час заняття:

10 тестів, правильна відповідь на кожен із яких оцінюється у 10 балів.

Модульний контроль 1 (підсумкове тестування):

20 тестів, правильна відповідь на кожен із яких оцінюється у 5 балів.

Модульний контроль 2:

20 тестів, правильна відповідь на кожен із яких оцінюється у 5 балів.

90–100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час відповідей, глибоко та всебічно розкриває зміст теоретичних питань, тестових та практичних завдань.

75–89 балів – достатньо повно володіє навчальним матеріалом, але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки.

65–74 балів – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки.

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності.

1-59 балів – не володіє навчальним матеріалом, не розкриває зміст теоретичних питань та практичних завдань.

Тренінг:

90–100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його використовує під час виконання завдань тренінгу, виявляє творчий підхід до виконання завдань.

75–89 балів – достатньо повно володіє навчальним матеріалом, але при виконанні окремих

завдань тренінгу не вистачає достатньої глибини та аргументації його використання, допускаються при цьому окремі несуттєві неточності та незначні помилки, загалом виявляє творчий підхід до виконання завдань.

65–74 бали – в цілому володіє навчальним матеріалом та загалом його використовує при виконанні завдань тренінгу, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому суттєві неточності та помилки, в окремих моментах виявляє творчий підхід до виконання завдань.

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його використовує, недостатньо розкриває зміст завдань тренінгу, допускаючи при цьому суттєві неточності, не виявляє творчого підходу до виконання завдань.

1-59 – не володіє навчальним матеріалом, не розкриває зміст завдань тренінгу, не бере участі у колективних завданнях підчас проведення тренінгу.

Активність під час тренінгу:

Оцінюється у діапазоні від 1 до 10 балів, де 1 бал – найнижча активність (студент практично не виявляє інтересу до завдань тренінгу), 10 балів – найвища активність (студент активно залучений у виконання завдань тренінгу, виявляє творчу ініціативу, ґрунтовне знання навчального матеріалу).

встановленим вимогам, містить елементи самостійного дослідження, свідчить про високий рівень опанування навчального матеріалу, студент на високому рівні виявляє творчий підхід до виконання завдань.

75–89 балів – зміст самостійної роботи в основному відповідає встановленим вимогам, можуть бути несуттєві недопрацювання за окремими завданнями, свідчить про належний рівень опанування навчального матеріалу, студент належно виявляє творчий підхід до виконання завдань.

60–74 балів – поставлені завдання виконані на недостатньому рівні; наведені авторські напрацювання є загальними і слабко обґрунтованими, свідчать про недостатній рівень опанування навчального матеріалу; студент припускається значних помилок у виконанні завдань, в окремих моментах виявляє творчий підхід до виконання завдань.

1-59 балів – завдання практично не виконані; відсутні авторські напрацювання; грубі помилки у вирішенні завдань роботи, що свідчать про низький рівень опанування навчального матеріалу; студент не виявляє творчого підходу до виконання завдань.

Залік: Визначається як середнє арифметичне з оцінок, отриманих під час вивчення дисципліни за самостійну роботу:

- наукового есе на актуальну для воєнного стану тематику.

Критерії оцінювання есе:

- Глибина аналізу актуальної на сьогодні ситуації, зважаючи на воєнний стан (30 балів)
- Виявлення ключових проблем (30 балів)
- Пропозиції щодо стратегії реагування та запобігання (30 балів)
- Якість викладу та аргументації (10 балів)

- Опрацювання розділів програми, які не виносяться на лекції (тематика подана у розділі Самостійна робота), що оцінюється в діапазоні:

90-100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час відповіді, глибоко та всебічно розкриває зміст теоретичного питання.

75-89 балів – достатньо повно володіє навчальним матеріалом, але при викладанні питання не вистачає достатньої глибини та аргументації, допущені окремі несуттєві неточності та незначні

помилки.

65-74 бали – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки.

60-64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичного питання, допускаючи при цьому суттєві неточності.

1-59 балів – не володіє навчальним матеріалом, не розкриває зміст теоретичного питання.

Шкала оцінювання:

За шкалою ЗУНУ	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов’язковим повторним курсом)