МАУП

ПРАТ «ВНЗ «МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»

Інститут безпеки

Кафедра інформаційної безпеки

Затверджую: Директор Інституту безпеки _____ (підпис) С.О. Лисенко (П. І. П.) “ 31 ” 08 2023 р.	Схвалено на засіданні кафедри інформаційної безпеки (назва кафедри) Протокол № 2 від 17 серпня 2023 р. Завідувач кафедри _____ (підпис) С. О. Лисенко (П. І. П.)

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Кібербезпека та захист інформаційних систем»

Галузь знань:	25 Воєнні науки, національна безпека, безпека державного кордону 12 Інформаційні технології
Спеціальність:	256 Національна безпека (за окремими сферами забезпечення і видами діяльності) 125 Кібербезпека
Освітньо-професійна програма:	Національна безпека (за окремими сферами забезпечення і видами діяльності)
Освітній рівень:	Магістр
Статус дисципліни:	Обов’язкова
Форма навчання:	денна/ заочна

Курс 1
Семестр 2
Обсяг в кредитах ЄКТС: 3
Всього годин за навчальним планом: 90 (17.08.23 р.)

- лекції (Л) - 16 годин;
-семінарські заняття (СЗ) та практичні заняття (ПЗ) - 20 годин:
-самостійна робота студентів (СРС) - 54 годин
Залік – 2 год.

Київ МАУП 2023 р.

Розробник (-и) силабусу навчальної дисципліни:
доктор економічних наук, професор Кавун С. В.

Викладач: Кавун Сергій Віталійович

Силабус розглянуто і затверджено на засіданні кафедри інформаційної безпеки
Протокол № ___ від _____ 202____ р.

Завідувач кафедри _____ Сергій ЛИСЕНКО
(підпис)

Силабус погоджено з гарантом (керівником) освітньої програми

256 Національна безпека (за окремими сферами забезпечення і видами діяльності)
(назва освітньої програми)

Керівник (гарант) освітньої програми _____ Іван СЕРВЕЦЬКИЙ
(підпис)

Силабус перевірено
(дата)

Заступник директора—декан _____ Тетяна АРІФХОДЖАЄВА
(підпис)

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

ПрАТ «ВНЗ» «Міжрегіональна Академія управління персоналом»
Інститут безпеки

Назва дисципліни	**Кібербезпека та захист інформації**
Викладач (-і)	**Кавун Сергій Віталійович**
Портфоліо викладача (-ів)	**Докторекономічних, професор**
Контактний тел.	+380507413062
E-mail:	**institutbezpeki@gmail.com**
Сторінка дисципліни на сайті	
Консультації	**Корпус 15, ауд., 307 четвер 10:00-12:00**

1. Коротка анотація до дисципліни. Дисципліна "Кібербезпека та захист інформації" присвячена вивченню основних принципів та методів захисту інформаційних систем від кіберзагроз. Курс охоплює питання організації кібербезпеки, правове регулювання цієї сфери, методи виявлення та запобігання кіберзагрозам, а також технології захисту даних. Особлива увага приділяється аналізу сучасних кіберзагроз, розробці стратегій забезпечення безпеки інформаційних ресурсів та практичним аспектам кіберзахисту.

2. Мета: Метою дисципліни є формування у студентів системного розуміння кібербезпеки та захисту інформації, розвиток навичок аналізу та управління кіберризиками, а також підготовка фахівців, здатних ефективно забезпечувати захист інформаційних систем від сучасних кіберзагроз.

3. Завдання: · Ознайомлення студентів з основними поняттями та принципами кібербезпеки та захисту інформації. Вивчення правових аспектів кібербезпеки та міжнародних стандартів у цій сфері. Аналіз сучасних кіберзагроз та їх впливу на інформаційні системи. Дослідження методів виявлення та запобігання кіберзагрозам.Вивчення технологій захисту даних, включаючи криптографію, контроль доступу та мережеву безпеку. Ознайомлення з організаційними аспектами кібербезпеки, включаючи політики безпеки та управління інцидентами. Розробка стратегій забезпечення безпеки інформаційних ресурсів. Розвиток практичних навичок у використанні інструментів кіберзахисту. Оцінка кіберризиків та розробка планів їх мінімізації. Підготовка студентів до професійної діяльності у сфері кібербезпеки та захисту інформації.

4. Формат курсу: очний (offline). Перелік теоретичних тем:

МОДУЛЬ 1 КІБЕРБЕЗПЕКА ТА ЇЇ РОЛЬ У СУЧАСНОМУ СВІТІ

1. ***Вступ до кібербезпеки: основні поняття та принципи***
2. ***Типи кіберзагроз та їх характеристики***
3. ***Правове регулювання кібербезпеки та захисту інформації***
4. ***Міжнародні стандарти та протоколи у сфері кібербезпеки***
5. ***Методи виявлення та аналізу кіберзагроз***
6. ***Технології захисту даних: криптографія та шифрування***
7. ***Контроль доступу та управління ідентифікацією***
8. ***Мережева безпека: принципи та методи***
9. ***Захист веб-додатків та серверів***
10. ***Управління інцидентами кібербезпеки***
11. ***Оцінка кіберризиків та управління ними***
12. ***Кібербезпека у хмарних обчисленнях***
13. ***Захист персональних даних та конфіденційності***
14. ***Соціальна інженерія та методи захисту від неї***
15. ***Моніторинг та аудит інформаційних систем***
16. ***Розробка політик та стратегій кібербезпеки***

5. Програмні результати навчання (інтегральні, фахові компетентності):

Табл. 1

Інтегральна компетентність	Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у галузі національної безпеки (за окремими сферами забезпечення і видами діяльності).
Загальні компетентності (ЗК)	ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність приймати обґрунтовані рішення. ЗК6. Здатність вчитися і оволодівати сучасними знаннями.
Спеціальні (фахові) компетентності (СК)	СК7. Здатність інтегрувати знання та розв'язувати складні задачі національної безпеки (за окремими сферами забезпечення і видами діяльності) у широких та/або мультидисциплінарних контекстах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності.
Програмні результати навчання	ПРН2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (за сферами забезпечення та видами діяльності), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.

	ПРН7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності). ПРН15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів. ПРН16.Здатність застосовувати набуті сучасні знання в галузі національної безпеки для збору, систематизації і аналізу отриманої з публічних джерел інформації стосовно загроз безпеці. ПРН17. Демонструвати та застосовувати навики управління суб'єктами національної безпеки та їх структурними підрозділами.

6. Тривалість курсу. 90 годин (3 кредити ЄКТС), з них: 36 години аудиторної роботи; 54 годин – самостійної роботи.

7. Статус дисципліни: *обов'язкова*

8. Пререквізити: Курс «Кібербезпека та захист інформації» не пов'язаний з іншими дисциплінами, вивчається у другому семестрі на першому курсі. Для вивчення курсу студенти мають розуміти основні принципи роботи кіберсистеми та володіти комп'ютером.

9. Технічне й програмне забезпечення /обладнання – офіційний сайт МАУП: *http://maup.com.ua*

10. Політика курсу:

- Передбачає роботу в команді.
- Клімат в аудиторії є дружнім, творчим, відкритим.
- Виконання завдань у встановлений термін.
- Відпрацювання пропущених занять можливе під час самостійної підготовки та консультацій викладача.
- Дотримання академічної доброчесності.
- Презентації та доповіді мають бути авторськими і оригінальними.

11. Зміст дисципліни: Курс складається з одногодвох модулів. Кожен модуль, у свою чергу, складається з лекційної та семінарської частин:

Модуль 1.МОДУЛЬ 1 КІБЕРБЕЗПЕКА ТА ЇЇ РОЛЬ У СУЧАСНОМУ СВІТІ (лекційні теми 1- 16; семінарські заняття теми 1-16).

12. Форми і методи навчання.

Основними видами навчальних аудиторних занять є **лекції, семінарські заняття, консультації.**

При викладанні ***лекційного матеріалу*** передбачено поєднання

таких форм і методів навчання, як лекції-бесіди, лекції-візуалізації.

Лекція-бесіда забезпечує безпосередній контакт викладача з аудиторією і дозволяє привернути увагу до найбільш важливих питань теми лекції, визначити у процесі діалогу особливості сприйняття навчального матеріалу. Студенти мають можливість обмірковувати поставлені запитання, робити самооцінку рівня своєї підготовки, навчитися самостійно формулювати висновки і узагальнення.

Лекція-візуалізація включає візуальну форму подачі лекційного матеріалу технічними засобами навчання. Читання такої лекції зводиться до розгорнутого або короткого коментування викладачем візуальних матеріалів, що переглядаються.

При проведенні ***семінарських занять*** передбачено поєднання таких форм і методів навчання як робота у малих групах, дискусія, публічний виступ, групові проекти та кейс завдання.

Студенти працюють з інформацією вдома (*див. рекомендовану літературу*), під час занять виконують усні та письмові завдання, виступають з доповідями і презентаціями, підготовленими як групою так і індивідуально, моделюють поведінку у конкретних професійних ситуаціях. Програмою курсу передбачено такі проекти:

- Підготовка публічного виступу.
- Виступ-інформування за темами семінарських занять.

13. Оцінювання знань здійснюється відповідно до «Положення про оцінювання навчальних досягнень здобувачів вищої освіти у ПрАТ «ВНЗ«МАУП»(https://drive.google.com/file/d/1ENRncPYdU2qLke7awVKn1OdfG88Hg8D/view).

14. Критерії оцінювання: - змістовність – 5 балів.

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	зараховано
82-89	**B**	добре	
75-81	**C**		
68-74	**D**	задовільно	
60-67	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

- відповідність темі та вимогам оформлення – 1 бал.

Максимальна кількість балів за самостійну роботу – **6 балів.**

15. Форми проведення модульного контролю та критерії оцінювання. Модульний контроль відбувається в кінці вивчення блоків змістових модулів і здійснюється у вигляді тестування. Студентами пропонуються тестові завдання у кількості 30 запитань. Максимальна кількість балів - 10 балів.

16. Форми проведення семестрового контролю та критерії оцінювання: *Залік.*

17. Рекомендовані джерела інформації

1. Баранов, О. А. (2014). Про тлумачення та визначення поняття «кібербезпека». Правова інформатика, 2(42), 54-62.

2. Фурашев, В. М. (2012). Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право, (2 (5)), 162-169.

3. Биков, В. Ю., Буров, О. Ю., & Дементієвська, Н. П. (2019). Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання, (70,№ 2), 313-331.

4. Сопілко, І. М. (2021). Інформаційна безпека та кібербезпека: порівняльно-правовий аспект (Doctoral dissertation, Національний авіаційний університет).

5. Tkachenko, O., & Tkachenko, K. (2018). Кіберпростір і кібербезпека: проблеми, перспективи, технології. Цифрова платформа: інформаційні технології в соціокультурній сфері, (1), 75-86.

6. Вітер, С. А., Витер, С. А., Світлишин, І. І., & Светлишин, И. И. (2017). Захист облікової інформації та кібербезпека підприємства.

7. Інформаційна безпека організації як фактор посилення бренду роботодавця [Електронний ресурс] Л. В. Мазник, О. І. Драган Київський економічний науковий журнал. 2023. № 1. С. 39-44. Режим доступу: http://nbuv.gov.ua/UJRN/kecscj_2023_1_7

8. Безпека інформаційних систем організацій [Електронний ресурс] / Я. Пахольчук, А. Митко // Міжнародні відносини, суспільні комунікації та регіональні студії. 2017. № 1. С. 89-96.

Режим доступу: http://nbuv.gov.ua/UJRN/mvckrc_2017_1_11

9. Трофименко, О. Г., Прокоп, Ю. В., Логінова, Н. І., & Задерейко, О. В. (2019). Кібербезпека України: аналіз сучасного стану. Ukrainian Information Security Research Journal, 21(3), 150-157.

10. Аналіз теоретичних викладок організації та управління соціально-економічною безпекою [Електронний ресурс] / А. Д. Калько // Інвестиції: практика та досвід. - 2012. - № 23. - С. 118-123. - Режим доступу: http://nbuv.gov.ua/UJRN/ipd_2012_23_30