Затверджено
Завідувач кафедри УКБЗІ_____ С. Легомінова
“ 31 “ серпня 2026 р.

СИЛАБУС ПЕРЕДДИПЛОМНОЇ ПРАКТИКИ

Керівник практики			**Щавінський Юрій Віталійович**, кандидат технічних наук, доцент.		**Контактна інформація лектора (e-mail), сторінка курсу в GWE**	**e-mail:** yushchavinsky@ukr.net; **сторінка курсу в GWE –** https://classroom.google.com/c/NzEyODUwNjk2MTA5?cjc=m76nns4	
Галузь знань			F «Інформаційні технології»		**Рівень вищої освіти**	магістр	
Спеціальність			F5 Кібербезпека та захист інформації		**Семестр**	3	
Освітня програма			Управління інформаційною та кібернетичною безпекою		**Тип освітнього компоненту**	Обов’язковий	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	9	270		-	2	-	268

АНОТАЦІЯ КУРСУ

Взаємозв’язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Корпоративна та професійна етика в кібербезпеці, Науково-технічний переклад, Організація і проведення наукових досліджень, Системи управління інформаційною безпекою, Прикладна загальна теорія систем ІБ, Управління проектами, Науково-дослідна практика
Освітні компоненти для яких є базовою	1. Підготовка кваліфікаційної роботи, підсумкова атестація
Мета:	узагальнення і вдосконалення здобутих ними знань, практичних умінь та навичок, оволодіння професійним досвідом та готовності їх до самостійної трудової діяльності, а також збору матеріалів для виконання кваліфікаційної роботи.

Компетентності відповідно до освітньої програми

Інтегральна компетентність

ІК. Здатність особи розв'язувати завдання дослідницького та/ або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності (ЗК)	**Фахові компетентності (КФ)**
КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних завдань у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

	КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу відповідно до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
Програмні результати навчання (ПР)	
РН2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних завдань інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних завдань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

ОРГАНІЗАЦІЯ ПРАКТИКИ		
Тема, опис теми	**Вид заняття**	**Форми і методи навчання/питання до самостійної роботи**
Тема Вступ до переддипломної практики Заняття. Організація проведення практики	Інструкторсько-методичне 2 год	Пояснювально-ілюстративний
Тема 1. Інтеграція систем управління інформаційною безпекою (ISMS) у бізнес-процеси організації **Завдання 1.** Системи управління інформаційною безпекою (ISMS) у бізнес-процеси організації	Самостійне завдання 10 год	Пошуковий метод. Навчальні питання 1. Принципи впровадження та оптимізації систем управління інформаційною безпекою відповідно до стандартів ISO/IEC 27001. 2. Побудова структури ISMS, управління ризиками та оцінка ефективності захисних заходів у бізнес-середовищі.
Завдання 2. Розроблення структури ISMS	Самостійне завдання 5 год	Виконання завдань на практичне застосування знань і вмінь, тестування
Тема 2. Розробка політики захисту персональних даних відповідно до міжнародних стандартів та законодавства **Завдання 3**. Розробка та впровадження захисту персональних даних в організації	Самостійне завдання 10 год	Пошуковий метод. Навчальні питання 1. Зміст та впровадженні політики захисту персональних даних відповідно до вимог законодавств, таких як GDPR.

		2. Впровадження Зміст та впровадженні політики захисту персональних даних відповідно до вимог законодавств, таких як GDPR.
Завдання 4.Розроблення політики захисту персональних даних	Самостійне завдання 5 год	Виконання завдань на практичне застосування знань і вмінь, тестування
Тема 3. Аудит інформаційної безпеки: методології та інструменти **Завдання 5**. Методи і інструменти аудиту інформаційної безпеки	Самостійне завдання 10 год	Пошуковий метод. Навчальні питання 1. Вивчення процедур проведення аудиту інформаційної безпеки. 2. Методики, які використовуються для оцінки стану кібербезпеки організації, а також програмні інструменти для проведення аудитів і оцінки вразливостей.
Завдання 6. Проведення аудиту інформаційної безпеки в організації	Самостійне завдання 5 год	Виконання завдань на практичне застосування знань і вмінь, тестування
Тема 4. Оцінка та управління кіберризиками в корпоративних системах **Завдання 7**. Дослідження ефективності програм навчання співробітників організації	Самостійне завдання 10 год	Пошуковий метод. Навчальні питання 1. Дослідження методів оцінки кіберризиків, а також способів їх мінімізації в корпоративних інформаційних системах. 2. Моделі управління ризиками, такі як OCTAVE, CRAMM або FAIR, та їх інтеграцію в управлінські рішення.
Завдання 8. Застосування моделей управління ризиками	Самостійне завдання 30 год	Підготовка кваліфікаційної роботи

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ

Матеріально-технічне забезпечення бази практики:
Мультимедійний проектор;
Комп'ютерний клас (аудиторія) для проведення практичних занять
Навчальні аудиторії (лабораторії) баз практики.
Моделі управління ризиками, такі як OCTAVE, CRAMM або FAIR

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Закон від 01.07.2014 № 1556-VII «Про вищу освіту» [Електронний ресурс]. – Доступний http://zakon1.rada.gov.ua/laws/show/1556-18
2. Закон України від 26.11.2015 № 848-VIII «Про наукову і науково-технічну діяльність». [Електронний ресурс]. – Доступний https://zakon.rada.gov.ua/laws/show/848-19#Text
3. Наказ МОН України від 08.04.1994 № 93 «Про затвердження Положення про проведення практики студентів вищих навчальних закладів України» [Електронний ресурс]. – Доступний https://zakon.rada.gov.ua/go/z0035-93
4. Положення про проведення практики студентів у Державному університеті інформаційно-комунікаційних технологій [Електронний ресурс]. – Доступний https://duikt.edu.ua/uploads/p_447_23214805.pdf

5. Положення про організацію освітнього процесу у Державному університеті інформаційно-комунікаційних технологій [Електронний ресурс]. – Доступний https://duikt.edu.ua/uploads/p_447_49109699.pdf
6. Положення про кафедру Державного університету інформаційно-комунікаційних технологій. [Електронний ресурс]. – Доступний https://duikt.edu.ua/uploads/p_447_65682809.pdf
7. Програма науково-дослідної практики для студентів спеціальності 125 Кібербезпека та захист інформації. [Електронний ресурс]. – Доступний https://classroom.google.com/c/NzEyODUyNzM3MjQ4
8. Вимоги до оформлення курсових і дипломних проектів: методичні рекомендації для студентів галузі знань 12 ″Інформаційні технології″ / уклад. А. А. Гаврилова, С. П. Євсеєв, Г. П. Коц, О. Г. Руденко. – Харків : ХНЕУ ім. С. Кузнеця, 2018. – 50 с.
9. Про затвердження Вимог до оформлення дисертації: Наказ від 12.01.2017 р. № 40 [Електронний ресурс] // База даних ″Законодавство України″ / ВР України. – Режим доступу до журн. : http://zakon2.rada.gov.ua/laws/show/z0155-17/print1509912703741 483 (дата звернення: 10.04.2024).

Додаткова

1. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (1994);
2. Закон України “Про захист персональних даних” (2010)
3. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015).
4. Закон України “Про національну безпеку (2018)
5. ISO/IEC 27001. "Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. "
6. ISO/IEC 27002. "Інформаційні технології. Методи забезпечення безпеки. Правила управління інформаційною безпекою."
7. ISO/IEC 27005. "Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки".

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

Індивідуальне завдання повинно бути узгоджене з вибраною темою кваліфікаційної роботи.

Поточний та підсумковий контроль за виконанням студентами програми практики здійснює керівник практики від кафедри.

Щоденник практики є основним документом студента під час проходження практики. Під час практики студент щотижня коротко повинен записувати в щоденник усе, що він зробив за тиждень для виконання календарного графіку проходження практики.

У щоденнику в загальній послідовності відображається й діяльність з громадсько-політичної практики. Не рідше, як раз на тиждень, студент зобов’язаний подавати щоденник на перегляд керівнику практики. Після закінчення практики щоденник разом із звітом має бути переглянутий керівником практики, який складає відгук й підписує його. Оформлений щоденник разом із звітом студент повинен здати на кафедру. Без заповненого щоденника практика не зараховується. Практика завершується заліком з доповіддю студента про виконане завдання.

Виставлення оцінки за практику для кожного студента-практиканта відбувається на захисті після виконання ним усіх завдань відповідно до плану практики.

На захист кожен студент повинен подати пакет звітної документації, який включає:

1. Звіт про проходження практики.
2. Щоденник практики, оформлений належним чином.

Для проведення захисту практики завідувачем кафедри призначається комісія з прийому звітів з практики за встановленим графіком. Оцінка з практики вноситься в залікову відомість, залікову книжку та навчальну картку студента

КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до захисту практики є виконання всіх індивідуальних завдань, які передбачені програмою, та належним чином оформленого звіту і щоденнику практики.

Оцінка комісії є остаточною. У випадку отримання студентом 0 балів (неприйнятно) тягне відрахування за невиконання навчального плану.

Оцінювання студентів здійснюється за накопичувальною 100-бальною системою і складається із врахуванням оцінок керівника практики від бази практики, керівника практики від університету, захисту звіту про практику та оформлення звіту і щоденника практики.

Форми контролю	**Види навчальної роботи**	**Оцінювання**
ПІДСУМКОВЕ ОЦІНЮВАННЯ *залік*	Самостійне виконання індивідуального завдання, практичне проведення дослідження. Залік проходить у вигляді захисту звіту практики перед комісією кафедри.	100 балів

Додаткова оцінка	
Види навчальної роботи	**Оцінювання**
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- Тези доповіді на фаховій конференції	3 бали
- Стаття у фаховому виданні	5 балів
- Стаття в іноземному рецензованому виданні	10 балів
Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти - 10 балів.	

ПІДСУМКОВА ОЦІНКА

Бали	Критерії оцінювання	Рівень компетентності	Оцінка / запис в екз. відомості
90-100	Студент на високому рівні виконав весь визначений обсяг роботи відповідно до програми, виявив професійні вміння, спираючись на теорію; правильно визначив і ефективно здійснював індивідуальні завдання. Роботу виконав на високому рівні (висока якість практики визначена науковим керівником дослідження, представниками базового закладу); виявив сумлінність, організованість, ініціативність на всіх етапах роботи; отримав виключно позитивну оцінку керівника практики, гаранта освітньо-наукової програми; здав у визначений термін правильно оформлену документацію; виконав на високому рівні наукове дослідження з теми кваліфікаційної роботи	Високий Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в програмі практики. Повністю набуті компетентності, визначені в освітньо-професійній програмі	Відмінно / Зараховано (А)
82-89	Студент повністю виконав програму практики; виявив уміння, базуючись на психологічну теорію, визначив основне завдання і способи його розв'язання, проявляв ініціативу в роботі; організована на достатньому методичному рівні. При загальній позитивній оцінці наукового керівника дослідження практикант допустив методичні помилки в оформленні результатів дослідження, але зміг їх із власної ініціативи самостійно виправити або пояснити причину їх допущення в процесі обговорення результатів роботи; здав у визначений термін належним чином оформлену документацію; виконав на достатньому рівні дослідження з теми кваліфікаційної роботи	Достатній Забезпечує студенту самостійне вирішення основних прикладних завдань науково-дослідної діяльності під час проходження практики. Набуті компетентності, визначені в освітньо-професійній програмі, забезпечують професійну діяльність	Добре / Зараховано (В)
75-81	Завдання за програмою практики виконані на достатньому рівні, але при загальній позитивній оцінці керівника дослідження практикант допускав незначні помилки у	Достатній Забезпечує студенту використання набутих	Добре / Зараховано (С)

	роботі, які не завжди міг самостійно виправити або пояснити в процесі їх аналізу. У ході практики був організованим, відповідальним, самостійним, критичним на всіх етапах роботи, одержав схвальні відгуки колективу бази практики, наукового керівника; подав вчасно документацію, до якої можуть бути внесені незначні доповнення і виправлення за вказівкою керівника практики.	знань і покращення навичок науково-дослідної діяльності за незначної підтримки керівника практики. Поглиблені питання щодо підготовки і проведення занять викликають утруднення. Набуті компетентності, визначені в освітньо-професійній програмі, забезпечують професійну діяльність	
64-74	Завдання практики виконано, але шаблонно і не в повному обсязі, результати практики оцінено науковим керівником на задовільному рівні. У студента виявлено дослідницькі вміння, але допущені незначні порушення вимог щодо доцільної організації науково-дослідницької діяльності; на задовільному рівні виконано заплановане дослідження та індивідуальні завдання. Студент проявив себе як організований, дисциплінований, але недостатньо самостійний та ініціативний. Загальна характеристика діяльності практиканта у період проходження практики одержала позитивні відгуки. Здобувач із невеликим запізненням подав документацію.	Середній Забезпечує достатньо надійний рівень відтворення основних знань і навичок щодо науково-дослідної діяльності за умови спрямування керівником. Набуті компетентності, визначені в освітньо-професійній програмі, в основному забезпечують професійну діяльність	Задовільно / Зараховано (D)
60- 63	Завдання практики виконано, але неповно, на задовільному рівні. Студент проявив себе як недостатньо організований і дисциплінований, безініціативний та несамостійний. Загальна характеристика діяльності на базі практики керівником оцінена на «задовільно». Завдання дослідження виконано на задовільному рівні, але під постійним контролем наукового керівника. Невчасно подано документацію, яка потребує доповнень і виправлень..	Середній Є мінімально допустимим за всіма складовими програми практики.	Задовільно / Зараховано (E)
35-59	Завдання практики виконані не в повному обсязі, програму навчальної, науково-дослідної роботи не виконано. Студент виявив низький рівень теоретичної та практичної підготовки в галузі інформаційної та кібербезпеки, невміння реалізувати програмні та індивідуальні завдання, налагоджувати контакт із колективом бази практики, не готовий до забезпечення доцільної наукової діяльності внаслідок недостатніх знань з провідноих дисциплін, методики і основ організації наукової діяльності.	Низький Не забезпечує практичної реалізації завдань програми практики.	Незадовільно з можливістю повторного захисту) / Не зараховано (FX)
1-34	Завдання не виконано або виконано із значними помилками; не сформовано вміння проводити наукові дослідження. Студент потребує повторного проходження не тільки практики, а й фахової підготовки загалом.	Незадовільний **Студент не підготовлений до самостійного виконання завдань програми практики.**	Незадовільно Не допущений (F) Не ставиться в залікову книжку

ДОТРИМАННЯ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Виконання навчальних завдань на практичних заняттях та під час самостійної підготовки, проведення поточного контролю результатів навчання, з використанням

самостійних (індивідуальних) форм роботи, зокрема за допомогою системи **GWE** перевіряється **на плагіат у відповідності з Кодексом академічної доброчесності Державного університету інформаційно-комунікаційних технологій** **https://duikt.edu.ua/uploads/p_447_96297052.pdf?2**