СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

НАУКОВО-ДОСЛІДНА ПРАКТИКА

<table>
<tr><td colspan="3">Керівник практики</td><td colspan="3">Пепа Юрій Володимирович, кандидат технічних наук, доцент, професор кафедри технічних систем кіберзахисту</td><td>Контактна інформація лектора (e-mail), сторінка курсу в GWE</td><td colspan="2">e-mail: y.pepa@duikt.edu.ua;
сторінка курсу в GWE –
https://classroom.google.com/c/ODc3ODIzNjM2MzI2?cjc=xqe44exx
код доступу – xqe44exx</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="3">F Інформаційні технології</td><td>Рівень вищої освіти</td><td colspan="2">магістр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="3">F5 Кібербезпека та захист інформації</td><td>Семестр</td><td colspan="2">3</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="3">Технічні системи інформаційного та кібернетичного захисту</td><td>Тип освітнього компоненту</td><td colspan="2">Обов’язковий</td></tr>
<tr><td rowspan="2">Обсяг:</td><td rowspan="2">Кредитів ECTS</td><td rowspan="2">Годин</td><td colspan="5">За видами занять:</td></tr>
<tr><td>Лекцій</td><td>Семінарських занять</td><td>Практичних занять</td><td>Лабораторних занять</td><td>Самостійна підготовка</td></tr>
<tr><td></td><td>6</td><td>180</td><td></td><td>-</td><td>120</td><td>-</td><td>60</td></tr>
<tr><td colspan="9">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="9">Взаємозв’язок у структурно-логічній схемі</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="6">Корпоративна та професійна етика в кібербезпеці, Науково-технічний переклад, Педагогіка та психологія у вищій школі, Організація проведення наукових досліджень, Теорія захисту інформаційних ресурсів обмеженого доступу, Ліцензування , атестація та сертифікація у сфері безпеки ОІД, Організація і проведення спеціальних досліджень на ОІД, Науково-педагогічна практика</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6">Переддипломна практика, Кваліфікаційна робота</td></tr>
<tr><td>Мета:</td><td colspan="8">поглиблення навичок самостійної наукової роботи, розширення наукового світогляду здобувачів другого (магістерського) рівня вищої освіти, вивчення проблем теорії та практики дослідження, проведення досліджень за темою кваліфікаційної роботи.</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="9">Інтегральна компетентність</td></tr>
<tr><td colspan="9">ІК. Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.</td></tr>
<tr><td colspan="4">Загальні компетентності (КЗ)</td><td colspan="5">Фахові компетентності (КФ)</td></tr>
<tr><td colspan="4">КЗ1. Здатність застосовувати знання у практичних ситуаціях.
КЗ2. Здатність проводити дослідження на відповідному рівні.
КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.</td><td colspan="5">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 задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного</td></tr>
</table>

	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. 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 оцінювати ефективність їх використання.
Програмні результати навчання (РН)	
РН3. Провадити дослідницьку та/або інноваційну діяльність у сфері інформаційної безпеки та/або кібербезпеки, а також у сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі у сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. 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. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації, а також аналізувати і надавати оцінку ефективності їх використання. 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 проєкти із захисту інформації.	

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 придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень та аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них у галузі інформаційної безпеки та/або кібербезпеки.

ОРГАНІЗАЦІЯ ПРАКТИКИ		
Тема, опис теми	**Вид заняття**	**Форми і методи навчання/питання до самостійної роботи**
Вступ до науково-дослідної практики Заняття. Організація проведення практики: ознайомлення з програмою, індивідуальним планом, вимогами до проведення досліджень, оформлення та захисту звіту.	Інструкторсько-методичне 2 год	Пояснювально-ілюстративний
Тема 1. Розробка політик і стандартів інформаційної безпеки Заняття 1. Дослідження процесу створення ефективних політик інформаційної безпеки та стандартів для захисту інформації. Формування компетентностей: КЗ1, КЗ2, КЗ3, КЗ4; КФ2, КФ3. Результати навчання: РН3, РН5, РН20, РН23.	Самостійне заняття 15 год	Пошуковий та аналітичний методи. Навчальні питання: 1. Дослідження процесу створення ефективних політик інформаційної безпеки. 2. Аналіз стандартів і нормативних вимог у сфері інформаційної та кібербезпеки.
Заняття 2. Розроблення політики інформаційної безпеки організації та обґрунтування її положень. Формування компетентностей: КЗ1, КЗ2, КЗ3, КЗ4; КФ2, КФ3. Результати навчання: РН3, РН5, РН20, РН23.	Практичне заняття 28 год	Виконання дослідницького завдання, аналіз нормативної бази, формування та обґрунтування пропозицій.
Тема 2. Дослідження кібербезпеки об'єктів інформаційної діяльності Заняття 3. Аналіз структури об'єкта, його функціонального призначення та технічних характеристик засобів захисту інформації. Формування компетентностей: КЗ1, КЗ2, КЗ3, КЗ4; КФ1, КФ3, КФ8. Результати навчання: РН3, РН4, РН5, РН8, РН13, РН19, РН20, РН21, РН22, РН23.	Самостійне заняття 15 год	Пошуковий, аналітичний та дослідницький методи. Навчальні питання: 1. Аналіз структури об'єкта інформаційної діяльності. 2. Дослідження функціонального призначення та характеристик засобів захисту. 3. Вибір методів і засобів проведення дослідження.

Заняття 4. Проведення дослідження кібербезпеки об’єкта інформаційної діяльності та оцінювання ефективності засобів захисту. Формування компетентностей: КЗ1, КЗ2, КЗ3, КЗ4; КФ1, КФ3, КФ8. Результати навчання: РН3, РН4, РН5, РН8, РН13, РН19, РН20, РН21, РН22, РН23.	Практичне заняття 30 год	Проведення теоретичного та/або експериментального дослідження, оброблення даних, оцінювання достовірності результатів.
Тема 3. Дослідження систем контролю та управління доступом Заняття 5. Дослідження програмних засобів захисту, організаційних заходів та інженерно-технічного забезпечення захисту інформації. Формування компетентностей: КЗ1, КЗ2, КЗ3, КЗ4; КФ1, КФ3, КФ6, КФ8. Результати навчання: РН4, РН8, РН11, РН13, РН19, РН20, РН21, РН22, РН23.	Самостійне заняття 15 год	Пошуковий та експериментальний методи. Навчальні питання: 1. Дослідження програмних засобів захисту та організаційних заходів. 2. Дослідження інженерно-технічного забезпечення захисту інформації.
Заняття 6. Аналіз та експериментальне оцінювання систем контролю і управління доступом. Формування компетентностей: КЗ1, КЗ2, КЗ3, КЗ4; КФ1, КФ3, КФ6, КФ8. Результати навчання: РН4, РН8, РН11, РН13, РН19, РН20, РН21, РН22, РН23.	Практичне заняття 30 год	Практичне дослідження, моделювання, аналіз результатів і підготовка обґрунтованих висновків.
Тема 4. Аналіз основних напрямів подальшого розвитку підприємства та розроблення рекомендацій щодо вдосконалення його системи інформаційної і кібербезпеки з урахуванням вразливостей, ризиків та кіберінцидентів Заняття 7. Формування пропозицій щодо поліпшення стану організації та забезпечення кібербезпеки на підприємстві. Формування компетентностей: КЗ1, КЗ2, КЗ3, КЗ4; КФ2, КФ3, КФ7, КФ8. Результати навчання: РН3, РН5, РН8, РН12, РН17, РН19, РН20, РН22, РН23.	Самостійне заняття 15 год	Аналітичний та проблемно-пошуковий методи. Навчальні питання: 1. Аналіз вразливостей, ризиків і кіберінцидентів. 2. Формування рекомендацій щодо вдосконалення системи інформаційної та кібербезпеки.
Заняття 8. Проведення підсумкового дослідження, узагальнення результатів та підготовка рекомендацій за темою кваліфікаційної роботи. Формування компетентностей: КЗ1, КЗ2, КЗ3, КЗ4; КФ2, КФ3, КФ7, КФ8.	Практичне заняття 30 год	Виконання дослідження, систематизація та інтерпретація результатів, підготовка науково обґрунтованих рекомендацій.

Результати навчання: РН3, РН5, РН8, РН12, РН17, РН19, РН20, РН22, РН23.		

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ

Матеріально-технічне забезпечення бази практики:
Мультимедійний проектор;
Комп'ютерний клас (аудиторія) для проведення практичних занять
Навчальні аудиторії (лабораторії) баз практики.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

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
Закон від 01.07.2014 № 1556-VII «Про вищу освіту» [Електронний ресурс]. – Доступний http://zakon1.rada.gov.ua/laws/show/1556-18
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
Положення про проведення практики студентів у Державному університеті інформаційно-комунікаційних технологій [Електронний ресурс]. – Доступний https://duikt.edu.ua/uploads/p_447_23214805.pdf
Положення про організацію освітнього процесу у Державному університеті інформаційно-комунікаційних технологій [Електронний ресурс]. – Доступний https://duikt.edu.ua/uploads/p_447_49109699.pdf
Положення про кафедру Державного університету інформаційно-комунікаційних технологій. [Електронний ресурс]. – Доступний https://duikt.edu.ua/uploads/p_447_65682809.pdf
Програма науково-дослідної практики для студентів спеціальності F5 «Кібербезпека та захист інформації». [Електронний ресурс]. – Доступний https://classroom.google.com/c/NzEyODUyNzM3MjQ4
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.
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
Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (1994);
Закон України "Про захист персональних даних" (2010)
СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015).
Закон України "Про національну безпеку (2018)
ISO/IEC 27001. "Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. "
ISO/IEC 27002. "Інформаційні технології. Методи забезпечення безпеки. Правила управління інформаційною безпекою."
ISO/IEC 27005. "Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки".

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

Індивідуальне завдання повинно бути узгоджене з обраною темою кваліфікаційної роботи. Поточний та підсумковий контроль за виконанням здобувачами програми практики здійснює керівник практики від кафедри. Щоденник практики є основним документом здобувача під час проходження практики. У ньому систематично відображаються виконані роботи відповідно до календарного графіка та індивідуального плану. Не

рідше одного разу на тиждень щоденник подається керівнику практики для контролю та консультацій. Після завершення практики щоденник разом зі звітом перевіряється керівником, який складає відгук і підписує документи. Практика завершується заліком у формі захисту звіту перед комісією кафедри. На захист здобувач подає звіт про проходження практики та належним чином оформлений щоденник. Обов'язковими є дотримання академічної доброчесності, вимог безпеки, правил роботи з конфіденційною інформацією та нормативних вимог бази практики.

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 дослідницької роботи відповідно до програми, виявив професійні вміння, спираючись на теорію; правильно визначив і ефективно здійснював індивідуальні дослідницькі завдання. Науково-дослідну 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	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)

	наукове дослідження з теми кваліфікаційної роботи		
82-89	Студент повністю виконав програму практики; виявив уміння, базуючись на психологічну теорію, визначив основне дослідницьке завдання і способи його розв'язання, проявляв ініціативу в роботі; дослідницька робота 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 науково-дослідної роботи; здав у визначений термін належним чином оформлену документацію; виконав на достатньому рівні наукове 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 (B)
75-81	Завдання за програмою практики виконані на достатньому рівні, але при загальній позитивній оцінці керівника дослідження практикант допускав незначні помилки у 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.	Достатній Забезпечує студенту використання набутих 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	Добре / Зараховано (C)
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». Наукове завдання дослідження виконано на задовільному рівні, але під постійним контролем наукового керівника. Невчасно подано документацію, яка потребує	Середній Є мінімально допустимим за всіма складовими програми практики.	Задовільно / Зараховано (E)

	доповнень і виправлень..		
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