СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРАКТИКА(ПЕРЕДДИПЛОМНА)

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	125 Кібербезпека та захист інформації
Назва освітньо-професійної програми	Кібербезпека та захист інформації
Рівень вищої освіти	Перший (бакалаврський)
Факультет	Інформаційних технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	**ОК-29** ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Лімарь Ігор Валерійович
quantum.biology@outlook.com

Старший викладач кафедри Інформаційних технологій та кібербезпеки,
кандидат технічних наук, спеціальність «Системи захисту інформації»

Загальна інформація

Анотація

Практика є обов'язковою компонентною ОПП «Кібербезпека та захист інформації», в межах якої передбачено набуття та удосконалення професійноважливих практичних умінь/навичок зі спеціальності 125 Кібербезпека та захист інформації. На практиці діяльність здобувача вищої освіти спрямована на опанування сучасними технологіями, методами, інструментами, обладнанням і т. ін.
По завершенню практики здобувач буде здатен виконувати професійну роботу фахівця і відповідно до Національного класифікатора України: Класифікатор професій (ДК 003:2010) займати первинну посаду за категоріями:

	• 3439 – фахівець з режиму секретності; • 3439 – фахівець із організації захисту інформації з обмеженим доступом; • 3439 – фахівець із організації інформаційної безпеки.
Мета дисципліни	– формування, розвиток, удосконалення професійноважливих практичних умінь та навичок зі спеціальності 125 Кібербезпека та захист інформації.
Компетентності, формуванню яких сприяє дисципліна	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадження системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

	КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
Результати навчання	ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки. ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту. ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів. ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

	ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та кібербезпеки відповідно до цілей і завдань організації. ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
Обсяг дисципліни	Загальний обсяг дисципліни: 4 кредити
Форма підсумкового контролю	Екзамен
Терміни викладання дисципліни	Дисципліна викладається: у 8-му семестрі

Нормативні посилання

1.	Положення Про порядок проведення практичної підготовки здобувачів вищої освіти Державного університету інтелектуальних технологій і зв'язку (Затверджено Вченою радою ДУІТЗ протокол №1 від 10.02.2023 р.) https://suitt.edu.ua/polozennja-duitz;
2.	Закону України «Про вищу освіту», стаття 51 «Практична підготовка осіб, які навчаються у закладах вищої освіти» (Відомості Верховної Ради, 2014, № 37-38).

Програма ПРАКТИКИ

Тема 1.	***Інструктаж з техніки безпеки.*** Ознайомлення та вивчення інструкцій та правил техніки безпеки на об'єкті. Вивчення інструкцій пожежної безпеки. Складання іспиту з техніки безпеки та пожежної безпеки.
Тема 2.	***Знайомство із структурою організації.*** Ознайомлення з поняттям організаційно-штатної структури підприємства. Вивчення призначенням і структури власне організації: розміщення, склад, взаємозв'язки, правила внутрішнього розпорядку, організація роботи обслуговуючого персоналу.
Тема 3.	***Організація робіт із захисту інформації на об'єкті інформаційної діяльності (ОІД).*** Дослідження об'єкту інформаційної діяльності. Ознайомлення та вибір порядку та методики проведення дослідження ОІД. Вивчення нормативно-технічної документації, планів

	приміщення. Виконання дослідження інформаційного, фізичного, технологічного середовища та середовища користувачів. Розробка моделей загроз та порушника: визначення видів загроз, їх класифікації, істотних загроз (витік інформації технічними каналами та каналами спеціального впливу), методів та способів їх здійснення, класифікації порушника при складанні моделі порушника. Розробка політики безпеки і організація охорони ОІД, пропускного режиму та контролю відвідувачів. Складання плану служби безпеки ОІД, загальної концепції безпеки інформації та контролю доступу.
Тема 4.	***Організаційні заходи захисту інформації на ОІД.*** Розбиття ОІД на зони безпеки. Ознайомлення та вивчення правил розбиття ОІД на зони безпеки. Створення рубежів безпеки, типових зон безпеки. Розробка організаційних заходів при роботі із співробітниками, організації діловодства та електронного документообігу: управління персоналом підприємства з урахуванням питань захисту інформації з обмеженим доступом, які необхідно здійснювати під час проведення процесу діловодства та електронного документообігу.

Список рекомендованих джерел

1. Голев Д.В., Кільдишев В.Й., Кононович В.Г. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум Частина 1 – Комплекси засобів захисту інформації від НСД: Навч. посібник / За ред. чл.- кор. МАЗ В.Г. Кононовича.– Одеса: ОНАЗ ім. О.С. Попова, 2010. – С.176.
2. Д. В. Голев, О.Ю.Русляченко, Ю.В.Бєлова, Д.С.Гончарук Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум Частина 2 – Комплекси техничного захисту інформації Навч. посібник / За ред. чл.-кор. МАЗ В.Г. Кононовича.– Одеса: ОНАЗ ім. О.С. Попова, 2010. – С. 184.
3. Стайкуца С.В., Методичні вказівки до виконання курсової роботи з дисципліни «Технічні засоби охорони об'єктів» / Стайкуца С. В., Осадчук К. О., Бєлова Ю. В., Сєдов К. С. - Одеса: ОНАЗ ім. О. С. Попова, 2019. – 67 с.
4. Методичні вказівки для виконання лабораторних робіт з дисципліни «Фізична безпека»/С. В. Стайкуца, Ю. В. Бєлова, К. О. Смаженко, К. С. Сєдов, О. В. Швець Одеса: ДУІТЗ, 2021. 139 с.
5. Стайкуца С.В., Бєлова Ю.В., Сєдов К.С., Севастєєв Є.О. «Комплексні системи безпеки». Методичні вказівки для виконання лабораторних робіт, Одеса: ДУІТЗ, 2021, 80 с.
6. Інформаційна безпека цифрових програмно-керованих АТС : [навч. посіб.] / В.Г. Кононович , С.В. Стайкуца, Т.М. Лемеха, Ю.В. Копитін; за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – С.

Інформація про консультації

Щовівторка у лютому-травні 2024 року з 11^{00} до 14^{00} год., ауд. 108 2-й лабораторний корпус – ст. викл. І. В. Лімарь

Загальна схема оцінювання

Сума балів за всі види	**Шкала**	**Оцінка за національною шкалою**	**Н а**	**Бали нараховуються таким чином:**

<table>
<tr><td>навчальної діяльності</td><td>ЄКТС</td><td>для іспиту</td><td>для заліку</td><td rowspan="8"></td><td rowspan="8">Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою
При оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань здобувачів вищої освіти за різними системами</td></tr>
<tr><td>90-100</td><td>A</td><td>Відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>Незадовільно з можливістю повторного складання</td><td>Не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-34</td><td>F</td><td>Незадовільно з обов’язковим повторним вивченням дисципліни</td><td>Не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

Політика опанування дисципліни

Відвідування: Здобувачі вищої освіти зобов’язані дотримуватися графіку проходження практики, своєчасно пройти інструктаж з техніки безпеки. Важливим є виконання індивідуальних завдань, правильне заповнення документації практики (щоденник, звіт та ін.).

Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності.

Інші умови: Здобувач вищої освіти бере участь (особисто та/або в команді з іншими студентами) у підсумковій конференції з практики, де презентує свої досягнення, подає рекомендації щодо удосконалення практичної підготовки в ДУІТЗ.