СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРОВЕДЕННЯ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Галузь знань	12–Інформаційні технолошії
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 і кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-26 ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Голев Денис Володимирович
d.v_holev@suitt.edu.ua

Старший викладач кафедри Кібербезпеки та технічного захисту інформації

Кільдішев Віталій Йосипович
kildishev@ukr.net

Доцент кафедри Кібербезпеки та технічного захисту інформації,
кандидат технічних наук, доцент

Загальна інформація про дисципліну

Анотація до дисципліни	Дисципліна «Проведення розслідування інцидентів інформаційної безпеки» базується на професійно-орієнтованих дисциплінах. Предметом вивчення навчальної дисципліни є методи та технології проведення розслідування інцидентів в області інформаційної безпеки. Ця дисципліна зосереджується на аспектах, пов'язаних зі збором,

	аналізом та інтерпретацією даних, що стосуються інцидентів інформаційної безпеки
Мета дисципліни	– формування знань, навичок та компетенцій у сфері виявлення, аналізу та розслідування інцидентів, що пов'язані з порушенням інформаційної безпеки в організаціях та установах. Навчає розпізнавати та аналізувати різноманітні інциденти в галузі інформаційної безпеки, такі як вторгнення, крадіжки даних, шпигунство, віруси, фішингові атаки тощо. Також вона орієнтує студентів на ефективні методи виявлення та розслідування інцидентів, в тому числі використання спеціального програмного забезпечення, інструментів та технологій.
Компетентності, формуванню яких сприяє дисципліна	КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ5. Здатність до пошуку, оброблення та аналізу інформації. КФ1. Здатність застосовувати законодавчу та нормативноправову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ2. Здатність до використання інформаційно–комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ12. 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 4. Аналізувати, аргументувати, приймати рішення при розв’язуванні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. 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 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки. ПРН 11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах. ПРН 15. Використовувати сучасне програмно–апаратне забезпечення інформаційно–комунікаційних технологій. ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН 43. Застосовувати національні та міжнародні регулюючи акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.
Обсяг дисципліни	Загальний обсяг дисципліни: 3 кредита ЄКТС 90 годин. Для денної форми навчання: лекції – 16 годин, практичні заняття –8 годин, лабораторні заняття – 20 годин, самостійна робота – 46 годин.
Форма підсумкового	Екзамен

контролю	
Терміни викладання дисципліни	Дисципліна викладається у 2-му семестрі

Програма дисципліни

Тема 1.	**Основні поняття та класифікація цифрової криміналістики**
Тема 2.	**Технології збору, аналізу та збереження цифрових доказів**
Тема 3.	**Техніки дослідження доказів в цифровому середовищі**
Тема 4.	**Аналіз даних, збережених на електронних пристроях та в Інтернеті**
Тема 5.	**Техніки виявлення та аналізу цифрових слідів**
Тема 6.	**Основи кібербезпеки та захисту від кіберзлочинів**
Тема 7.	**Правові та етичні аспекти роботи в галузі цифрової криміналістики.**
Тема 8.	**Техніки протидії комп'ютерній криміналістиці**

Список рекомендованих джерел

1. Шон Харрис. CISSP Руководство для подготовки к екзамену / Шон Харрис // Пятая редакции, 2019. - 875 с.

2. Digital Forensics Basics: A Practical Guide Using Windows OS / Nihad A. Hassan New York, New York, USA 342c

3. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory 1st Edition / Michael Hale Ligh; Andrew Case; Jamie Levy; Aaron Walters, 2014 – 914c

4. Johansen G. Digital Forensics and Incident Response / Gerard Johansen. – Birmingham: Packt Publishing, 2022. – 532 с.

Інформація про консультації

Щопонеділка у вересні-грудні 2023 року з 13^{00} до 14^{30} год., ауд. 250 або zoom

Загальна схема оцінювання

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Шкала ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td><td rowspan="2">Нарахування балів</td><td>Бали нараховуються таким чином:</td></tr>
<tr><td>для іспиту</td><td>для заліку</td><td rowspan="8">Оцінювання знань здобувачів вищої освіти здійснюється
за 100-бальною шкалою і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів, за результати екзамену – до 40 балів.</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 самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях та контрольних заходах (екзамен/залік) є обов’язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.

Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **Unicheck.**

Умови зарахування пропущених занять:

Інші умови: Навчально-методичні матеріали дисципліни розміщені на платформі Moodle.