Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського
Спеціальна кафедра № 1

КІБЕРНАВЧАННЯ

Робоча програма навчальної дисципліни (силабус)

Рівень вищої освіти	***Другий (магістерський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Освітньо-професійна програма	*Безпека державних інформаційних ресурсів*
Статус дисципліни	*Обов'язкові компоненти освітньої програми*
Форма навчання	*очна (денна)*
Рік підготовки, семестр	*І рік підготовки, осінній та весняний семестри*
Обсяг дисципліни	*3 кредити*
Семестровий контроль/ контрольні заходи	*залік*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	
Розміщення курсу	

Київ – 2023

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Метою навчальної дисципліни “Кібернавчання” є формування у курсантів системи знань і вмінь щодо існуючих технологій та методик захисту інформації, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, оцінки захищеності інформаційних систем, групової взаємодії при реагуванні на кібератаки. Особлива увага приділяється оцінці захищеності інформаційних систем та технологіям виявлення та протидії кібератакам на інформаційні системи.

Навчальна дисципліна “Кібернавчання” проводиться на базі кіберполігону Тренінгового центру ДЦКЗ Держспецзв’язку у режимі віддаленого доступу в І та ІІ семестрах.

Основне завдання навчальної дисципліни “Кібернавчання” є формування наступних компетентностей:

КЗ-1	Здатність застосовувати знання у практичних ситуаціях.
КЗ-3	Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
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.
КФ4	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
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 у відповідності 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.
КФ9	Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ11	Здатність реалізовувати технічні вимоги на основі технік оцінки рівня захищеності інформаційних систем, технологій аналізу мережевого трафіку та принципів протидії кібератакам.
КФ13	Здатність аналізувати, інтегрувати і використовувати кращі світові практики, міжнародні стандарти при розробці криптографічних систем захисту спеціальних інформаційно-комунікаційних систем.

Виконання програми навчальної дисципліни “Кібернавчання” дозволяє досягти курсантами наступних результатів навчання:

РН1	Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2	Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
РН9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
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.
РН16	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
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.
РН21	Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН24	Оцінювати стан інформаційних систем, розподіляти послуги безпеки і обирати механізми безпеки, впроваджувати технологічні рішення інноваційного характеру щодо виявлення та блокування загроз інформаційним ресурсам.
РН26	Проводити аналіз та синтез криптографічних алгоритмів та криптографічних протоколів; розробляти рекомендації впровадження інноваційних проектів, використовуючи базові методи дослідницької діяльності.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Навчальна дисципліна “Кібернавчання” *базується* на знаннях отриманих у раніше вивченій навчальній дисципліні “Технології виявлення та блокування

загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах".

Навчальна дисципліна "Кібернавчання" *забезпечує* вивчення частини розділів таких навчальних дисциплін: "Військове стажування", "Робота над магістерською дисертацією".

3. Зміст навчальної дисципліни

Семестровий (кредитний) модуль 1. Кібернавчання.

Розділ (змістовий модуль) 1. Обробка кіберінцидентів та реагування на них.

1. Протидія кібератаці "WordPress Blue Bad плагін".
2. Протидія кібератаці "SQL ін'єкція".
3. Протидія кібератаці "Apache Shutdown".
4. Протидія кібератакам "DDoS SYN Flood" та "DDoS DNS".
5. Протидія кібератаці програми вимагача.

Семестровий (кредитний) модуль 2. Кібернавчання.

Розділ (змістовий модуль) 2. Реагування на кіберінциденти.

1. Етапи обробки інцидентів та реагування на них.
2. Процес обробки інцидентів та реагування на них.
3. Моніторинг усіх подій у корпоративній мережі.
4. Обробка та реагування на інциденти безпеки у корпоративній мережі, а саме: електронної пошти, мережі, ОС Windows/Linux.
5. Основні кроки протидії та відновлення у випадку кібератаки.

4. Навчальні матеріали та ресурси

Основна література.

1. Cyberbit Range, SOC Basic Scenario Guide, Version 4.0.
2. Eric C. Thompson. Cybersecurity Incedent Response: How to contain, Eradicate, and Recover from incident, 2018. – 176 p.

Додаткова література.

1. Don Murdoch. Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases Notes from the Field, 2018 – 256 c.
2. Cyberbit Range, Посібник із розширеного сценарію, Версія 4.0
3. Rash, Michael. Linux firewalls: attack detection and response with iptables, psad, and fwsnort / Michael Rash.

Навчальний контент

5. Методика опанування навчальної дисципліни "Кібернавчання".

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу		Кількість годин				
		Всього	у тому числі			
			Лекції	Практичні заняття	Семін. заняття	СРК
Розділ (змістовий модуль) 1. Обробка кіберінцидентів та реагування на них.						
Тема 1	**Обробка кіберінцидентів та реагування на них.**	**45**		**30**		**15**
Заняття 1/1	1. Протидія кібератаці "WordPress Blue Bad плагін". 1. Розгляд послідовності атаки WordPress Blue Bad плагін. 2. Етапи та реалізація сценарію атаки.	**9**		6		3

	3. Усунення атаки WordPress Blue Bad плагін. Основна література: [1,2].					
Заняття 1/2	Протидія кібератаці “SQL ін’єкція”. 1. Розгляд послідовності атаки “SQL ін’єкція”. 2. Етапи та реалізація сценарію атаки. 3. Усунення атаки “SQL ін’єкція”. Основна література: [1,2].	**9**		6		3
Заняття 1/3	Протидія кібератаці “Apache Shutdown”. 1. Розгляд послідовності атаки “Apache Shutdown”. 2. Етапи реалізації сценарію атаки. 3. Усунення атаки “Apache Shutdown”. Основна література: [1,2].	**9**		6		3
Заняття 1/4	Протидія кібератакам “DDoS SYN Flood” та “DDoS DNS”. 1. Розгляд послідовності атаки “DDoS SYN Flood”. 2. Етапи та реалізація сценарію атаки “DDoS SYN Flood”. 3. Усунення атаки “DDoS SYN Flood”. 4. Розгляд послідовності атаки “DDoS DNS”. 5. Етапи та реалізація сценарію атаки “DDoS DNS”. 6. Усунення атаки “DDoS DNS”. Основна література: [1,2].	**9**		6		3
Заняття 1/5	Протидія кібератаці програми вимагача. 1. Розгляд послідовності атаки програми вимагача. 2. Етапи реалізації сценарію атаки. 3. Усунення атаки програми вимагача. Основна література: [1,2].	**9**		6		3
Разом за розділом 1		**45**		**30**		**15**
Розділ (змістовий модуль) 2. Реагування на кіберінциденти.						
Тема 2	**Реагування на кіберінциденти.**	**45**		**30**		**15**
Заняття 2/1	Етапи обробки інцидентів та реагування на них. 1. Розгляд послідовності атаки “Java NMS Shutdown”. 2. Етапи та реалізація сценарію атаки “Java NMS Shutdown”. Основна література: [1,2].	**9**		6		3
Заняття 2/2	Процес обробки інцидентів та реагування на них.	**9**		6		3

	1. Розгляд послідовності атаки “DB Dump via FTP Exploit”. 2. Етапи та реалізація сценарію атаки “DB Dump via FTP Exploit”. Основна література: [1,2].					
Заняття 2/3	Моніторинг усіх подій у корпоративній мережі. 1. Послідовність атаки “WMI Worm”. 2. Етапи та реалізація сценарію атаки “WMI Worm”. Основна література: [1,2].	**9**		6		3
Заняття 2/4	Обробка та реагування на інциденти безпеки у корпоративній мережі, а саме: електронної пошти, мережі, ОС Windows/Linux. 1. Розгляд послідовності атаки “WPAD Man-in-the-Middle”. 2. Етапи та реалізація сценарію атаки “WPAD Man-in-the-Middle”. Основна література: [1,2].	**9**		6		3
Заняття 2/5	Основні кроки протидії та відновлення у випадку кібератаки. 1. Розгляд послідовності атаки “Ransomware”. 2. Етапи та реалізація сценарію атаки “ Ransomware”. Основна література: [1,2].	**9**		6		3
Разом за розділом 2		**45**		**30**		**15**
Всього годин		**90**		**60**		**30**

6. Самостійна робота курсанта

Головним видом самостійної роботи курсантів є самостійна підготовка до аудиторних занять.

Доцільно час самостійної підготовки для поглибленого вивчення та закріплення навчального матеріалу розподілити наступним чином:

№ з/п	Назва теми та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу)	Кількість годин СР
1	**Тема 1. Обробка кіберінцидентів та реагування на них.** Методологія й засоби реалізації атаки на веб-сервер. Протидія й засоби захисту від атак на веб-сервер. Методологія й засоби реалізації атаки на веб-додатки. Протидія й засоби захисту від атак на веб-додатки. Методологія й засоби реалізації SQL-ін’єкцій. Протидія й засоби захисту від SQL-ін’єкцій. Основна література: [1,2]. Додаткова література: [1-3].	15
2	**Тема 2. Реагування на кіберінциденти.** Типова схема організації ІКС та технології її захисту (мережеві сканери та аналізатори, системи моніторингу мережі, міжмережеві екрани, проксі-сервери, системи виявлення та попередження вторгнень IDS, мережеве антивірусне програмне забезпечення, тощо). Технології менеджменту інформаційними подіями та подіями безпеки в мережі та на кінцевих пристроях.	15

	Етапи обробки інцидентів та реагування на них. Основна література: [1,2]. Додаткова література: [1-3].	
Всього		30

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Політика навчальної дисципліни визначає систему вимог, які викладач ставить перед здобувачем:

Правила поведінки та відвідування навчальних занять передбачають: оволодівати теоретичними знаннями і практичними навичками за обраною спеціальністю; дотримуватися графіка навчального процесу та вимог навчального плану; відвідувати навчальні заняття і виконувати у встановлені терміни усі види завдань, передбачені навчальними планами і програмами; у разі хвороби, несення служби в наряді або у виняткових випадках здобувач може бути відсутності на заняттях (з подальшим відпрацюванням пропущеного матеріалу).

По прибутті на навчальні заняття здобувачі повинні відключати мобільні телефони; входити і виходити з аудиторії тільки з дозволу керівника на робочому місці; уважно слухати пояснення керівника на робочому місці; не розмовляти і не займатися сторонніми справами; виконувати всі вказівки керівника на робочому місці; підтримувати чистоту і порядок в приміщеннях, дотримуватися морально-етичних правил поведінки і спілкування.

Дотримання академічної доброчесності здобувачами освіти передбачає: самостійне виконання навчальних завдань, завдань поточного контролю результатів навчання; посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; дотримання норм законодавства про авторське право і суміжні права; надання достовірної інформації про результати власної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

У випадку запровадження обмежувальних заходів, що унеможливлюють організацію і здійснення освітнього процесу в навчальних приміщеннях у складі груп, проведення навчальних занять з даної навчальної дисципліни можна здійснювати віддалено з використанням технологій дистанційного навчання. В цьому випадку з курсантів вимагається обов'язково наявність справних відеокамери та мікрофону, які мають бути увімкнені на кожному дистанційному занятті. Навчальна література навчальної дисципліни зазначена в розділі 4, є відкритою, не містить відомостей з обмеженим доступом і може бути оприлюднена з використанням технологій дистанційного навчання, а сама програма не потребує коригування у випадку проведення навчальних занять у дистанційному режимі.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Оцінювання результатів навчання курсантів здійснюється у відповідності до Положення про систему оцінювання результатів навчання в КПІ ім. Ігоря Сікорського.

Рейтинг здобувача з навчальної дисципліни розраховується зі 100 балів, які він отримує за:

виконання практичного завдання заняття 1/1 – 10 балів;

виконання практичного завдання заняття 1/2 – 10 балів;

виконання практичного завдання заняття 1/3 – 10 балів;
виконання практичного завдання заняття 1/4 – 10 балів;
виконання практичного завдання заняття 1/5 – 10 балів;
виконання практичного завдання заняття 2/1 – 10 балів;
виконання практичного завдання заняття 2/3 – 10 балів;
виконання практичного завдання заняття 2/3 – 10 балів;
виконання практичного завдання заняття 2/4 – 10 балів;
виконання практичного завдання заняття 2/5 – 10 балів;

Правильність виконання практичного завдання та відповідний рейтинговий бал визначається за наступними критеріями:

- правильно і повністю виконане завдання – 95-100% максимального балу;
- частково виконане завдання або наявні незначні помилки – 75-84% максимального балу;
- завдання виконано з помилками – 60-74% максимального балу;
- завдання не виконано – 0 балів.

Семестровий контроль: залік.

Умовою допуску до заліку є отримання курсантом позитивних оцінок з усіх практичних занять.

Курсанти, які набрали рейтинг з кредитного модуля менше $0{,}6R$, зобов'язані виконувати залікову контрольну роботу.

Курсанти, які набрали необхідну кількість балів ($RD \geq 0{,}6R$), мають можливості:

1) за рішенням викладача застосовується жорстка РСО – попередній рейтинг курсанта з дисципліни скасовується і він отримує оцінку тільки за результатами залікової контрольної роботи, яка оцінюється в 100 балів. Цей варіант змушує курсанта критично оцінити рівень своєї підготовки та ретельно готуватися до заліку.

На заліку курсант виконує практичне відпрацювання одного із сценарію, що відповідає практичним завданням.

Критерії нарахування балів за виконання завдання:

– "відмінно" – повна виконання завдань сценарію (не менше 90% визначених контролів) – 95 - 100 балів;

– "дуже добре" – часткове виконання завдань сценарію, наявні незначні помилки в роботі з інструментарієм та формуванні звітів сценарію (не менше 85% визначених контролів) – 85 – 94 балів;

– "добре" – виконання завдань сценарію з помилками формування звітів сценарію (не менше 75% визначених контролів) – 75 – 84 балів;

– "задовільно" – сценарії виконано з помилками (не менше 65% визначених контролів) – 65 – 74 балів;

– "достатньо" – неповне виконання сценарію (не менше 60% визначених контролів) – 60 - 64 балів;

– "незадовільно" – виконання сценарію не відповідає вимогам для оцінювання на "задовільно" – 0 балів.

Отриманий рейтинг визначає оцінку за дисципліну, є остаточним і вноситься в залікову відомість.

2) за рішенням викладача отримати залікову оцінку (залік) так званим "автоматом" відповідно до набраного рейтингу R.

Вважається, що курсант успішно виконав програму навчальної дисципліни, якщо він отримав позитивну загальну рейтингову оцінку $RD \geq 60$.

Рейтингова оцінка трансформується до університетської системи оцінювання згідно з таблицею:

Кількість балів	Оцінка
95-100	Відмінно
85-94	Дуже добре
75-84	Добре
65-74	Задовільно
60-64	Достатньо
менше 60	Незадовільно

9. Додаткова інформація з дисципліни (освітнього компонента)

Інформаційне забезпечення – апаратно-програмні засоби Навчального ситуаційного центру кібербезпеки: SIEM QRadar, IDS Fortinet, Honeypot, FireWall.