ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»

Факультет суспільних і прикладних наук

Кафедра інформаційних технологій

ЗАТВЕРДЖУЮ
Проректор з методичної роботи
_____ Ярослав ШТАНЬКО
"30" 08 2024 р.

LEARN ETHICAL HACKING FROM SCRATCH

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань:	12 "Інформаційні технології"
Спеціальність:	121 Інженерія програмного забезпечення
Освітньо-професійна (освітньо-наукова) програма:	Розробка та тестування програмного забезпечення
Освітній рівень:	перший (бакалаврський)
Статус дисципліни:	вибіркова
Мова викладання, навчання та оцінювання:	українська та англійська

Івано-Франківськ
2024

2

РОЗРОБНИК:

педагогічний працівник кафедри ІТ Сергій ГАВРИЛКО

ЗАТВЕРДЖЕНО:

на засіданні кафедри інформаційних технологій, протокол № 1 від 28.08.2024 р.

Завідувач кафедри Сергій ВАЩИШАК

УЗГОДЖЕНО:

Гарант ОПП/ОНП Олександр ІВАНОВ

на засіданні кафедри інформаційних технологій, протокол № 1 від 28.08.2024 р.

Завідувач кафедри Сергій ВАЩИШАК

СХВАЛЕНО:

на засіданні Науково-методичної ради, протокол № 1 від 30.08.2024 р.

e-mail	serhii.m.havrylko@ukd.edu.ua
Номер аудиторії чи кафедри	Кафедра інформаційних технологій, ауд. 206
Посилання на сайт	https://ukd.edu.ua
Сторінка курсу в СДО	https://online.ukd.edu.ua/

ВСТУП

Анотація навчальної дисципліни

Мета навчальної дисципліни: сформувати у здобувачів актуальні навички критичного мислення стосовно кібербезпеки, зрозуміти причинно-наслідкові зв'язки, зрозуміти складні та дискусійні питання історії кібербезпеки та розвитку кібербезпеки в Україні та за кордоном, зрозуміти суть і філософію галузі кібербезпеки та сформувати в собі звичку щоденних кібербезпекових дій і думок. Ця навчальна дисципліна озброїть вас навичками, необхідними для підготовки до роботи в галузі кібербезпеки початкового рівня. Ви познайомитеся зі світом кібербезпеки за допомогою інтерактивної навчальної програми, розробленої Google. Ви дізнаєтеся про важливі події, які призвели до розвитку сфери кібербезпеки, зрозумієте важливість кібербезпеки в сучасних бізнес-операціях і дослідите посадові робочі обов’язки та навички аналітика з кібербезпеки початкового рівня.

Основні з**авдання**, що стоять перед авторами курсу, полягають в тому, щоб розкрити здобувачам:

- дискусійні проблеми історії розвитку кібербезпеки, а також існуючі наукові судження стосовно змісту кібербезпеки та її впливу на минуле, теперішнє і майбутнє IT індустрії і світового бізнесу загалом;
- аналізувати джерела інформації про кібербезпеку, співставляти наявну в них інформацію та сформувати власну думку стосовно актуальних проблем розвитку кібербезпеки в Україні та в глобальному світі бізнесу;
- усвідомити причини та наслідки різних підходів і законів кібербезпеки;
- зрозуміти особливості процесів розвитку кібербезпеки і етичного хакерства, впливу на цей процес економічних, політичних, соціальних та технологічних чинників;
- усвідомити зміст та філософію підходів щодо управління, лідерства та менеджменту в контексті кібербезпеки і етичного хакерства.

В результаті вивчення дисципліни студент повинен **знати**:

- основи етичного хакерства;
- основи кібербезпеки;
- якими навичками і компетенціями має володіти спеціаліст з кібербезпеки;
- як працює архітектура мереж;
- як працює цільова система;
- слабкі сторони цієї системи;
- як практично використовувати ці слабкі стороно шоб ламати систему;
- різні концепції, інструменти та методи етичного хакерства та кібербезпеки.

В результаті вивчення дисципліни студент повинен **вміти**:

- професійно надавати послуги з кібербезпеки на початковому рівні;
- здійснювати аналіз проблем та інцидентів з кібербезпеки;
- аналізувати процеси кібербезпеки і етичного хакерства, критично сприймати інформацію про побудову і розвиток кібербезпеки на рівні організацій і на індивідуальному рівні;
- використовувати різні типи джерел для співставлення та узагальнення інформації про розвиток кібербезпеки і етичного хакерства;
- аргументувати думку про систему цінностей властиву етичному хакерству та кібербезпеці, а також філософію, роль і значення кібербезпеки у розвитку людства і світової економіки;
- створювати та управляти засобами кібербезпеки з різними типами складності;
- прогнозувати як будуть розвиватися кібербезпека і етичне хакерство в майбутньому;
- аналізувати кібербезпеку з точки зору різних якісних атрибутів та ідентифікувати причини їх успіхів або невдач.

Компетентності та результати навчання, **яких набувають здобувачі освіти внаслідок вивчення навчальної дисципліни (шифри та зміст компетентностей та програмних результатів навчання вказано відповідно до ОПП «*Розробка та тестування програмного забезпечення*»**).

Шифр та назва компетентності	**Шифр та назва програмних результатів навчання**
ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.	ПРН1. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.
ЗК2. Здатність застосовувати знання у практичних ситуаціях.	
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.	
ЗК4. Здатність спілкуватися іноземною мовою як усно, так і письмово.	
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.	

ФК8. Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення.	
ФК14. Здатність до алгоритмічного та логічного мислення.	

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Курс	**четвертий (4)**		
Семестр	**сьомий (7)**		
Кількість кредитів ЄКТС	**3**		
Аудиторні навчальні заняття		**денна форма**	**заочна форма**
	лекції	**14 (в годинах)**	**4**
	практичні	**16 (в годинах)**	**4**
Самостійна робота		**60 (в годинах)**	**82**
Форма підсумкового контролю	**Екзамен (сьомий (7) семестр)**		

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Перелік тем лекційного матеріалу

Тема 1. Course introduction. Cybersecurity for Beginners (2 год.)

Що таке кібербезпека? (What is cybersecurity?). Основні навички професіоналів з кібербезпеки (Core skills for cybersecurity professionals). Огляд: Ласкаво просимо в захоплюючий світ кібербезпеки (Review: Welcome to the exciting world of cybersecurity). Історія безпеки (History of security). Вісім доменів безпеки (Eight security domains). Огляд: Еволюція кібербезпеки (Review: The evolution of cybersecurity).

***Питання для самостійного вивчення*:** *Фреймворки безпеки та контроль безпеки (Security frameworks and control). Етика для професіонала з кібербезпеки (Ethics for a cybersecurity professional). Огляд: захист від загроз, ризиків і вразливостей (Review: Protecting against threats, risks, and vulnerabilities). Важливі інструменти кібербезпеки (Important cybersecurity tools). Мови програмування в кібербезпеці (Programming languages in cybersecurity). Огляд: інструменти кібербезпеки (Review: Cybersecurity tools).*

Тема 2. Setting up a Hacking Lab. How To Manage Security Risks & Threats (2 год.)

Докладніше про домени безпеки CISSP (More about the CISSP security domains). Розуміння загроз, ризиків і вразливостей (Navigate threats, risks, and vulnerabilities). Огляд: домени безпеки (Review: Security domains). Докладніше про фреймворки та елементи керування (More about frameworks and controls). Тріада КЦД: конфіденційність, цілісність і доступність (The CIA triad: Confidentiality, integrity, and availability). Фреймворки NIST (NIST frameworks). Принципи OWASP і перевірки безпеки (OWASP principles and security audits).

Питання для самостійного вивчен*ня: Огляд: системи безпеки та елементи керування (Review: Security frameworks and controls). Інформаційні панелі безпеки та управління подіями (SIEM) (Security information and event management (SIEM) dashboards). Ознайомтеся з інструментами безпеки та управління подіями (SIEM) (Explore security information and event management (SIEM) tools). Огляд: Знайомство з інструментами кібербезпеки (Review: Introduction to cybersecurity tools). Етапи реагування на інциденти (Phases of incident response playbooks).*

Тема 3. Linux Basics. Internet Networks & Network Security (2 год.)

Мережевий зв'язок (Network communication). Місцевий і глобальний зв'язок (Local and wide network communication). Огляд: Архітектура мережі (Review: Network architecture). Знайомство з мережевими протоколами (Introduction to network protocols). Ідентифікація системи (System identification). Огляд: мережеві операції (Review: Network operations). Вступ до тактики вторгнення в мережу (Introduction to network intrusion tactics). Захистіть мережі від атак типу «Відмова в обслуговуванні» (DoS) (Secure networks against Denial of Service (DoS) attacks).

Питання для самостійного вивчен*ня: Тактика мережевих атак і захисту (Network attack tactics and defense). Огляд: захист від мережевих вторгнень (Review: Secure against network intrusions). Вступ до посилення безпеки (Introduction to security hardening). Загартування ОС (OS hardening).*

Загартування мережі (Network hardening). Хмарне загартування (Cloud hardening). Огляд: посилення безпеки (Review: Security hardening).

Тема 4. Network Hacking. The Basics of Computing Security: Linux & SQL (2 год.)

Чудовий світ операційних систем (The wonderful world of operating systems). Операційна система в роботі (The operating system at work). Інтерфейс користувача (The user interface). Огляд: Введення в операційні системи (Review: Introduction to operating systems). Все про Linux (All about Linux). Дистрибутиви Linux (Linux distributions). Оболонка (The shell). Огляд: операційна система Linux (Review: The Linux operating system). Навігація файловою системою Linux (Navigate the Linux file system).

Питання для самостійного вивчення: *Керуйте вмістом файлу в Bash (Manage file content in Bash). Автентифікація та авторизація користувачів (Authenticate and authorize users). Отримати допомогу в Linux (Get help in Linux). Огляд: команди Linux в оболонці Bash (Review: Linux commands in the Bash shell). Вступ до SQL і баз даних (Introduction to SQL and Databases). SQL запити (SQL queries). Більше фільтрів SQL (More SQL filters). SQL приєднання (SQL joins). Огляд: Бази даних і SQL (Review: Databases and SQL)*

Тема 5. Gaining Access to Computers. Cybersecurity Assets, Network Threats & Vulnerabilities (2 год.)

Знайомство з активами (Introduction to assets). Цифрові та фізичні активи (Digital and physical assets). Ризик і безпека активів (Risk and asset security). Огляд: Вступ до безпеки активів (Review: Introduction to asset security). Інформація про захист (Safeguard information). Методи шифрування (Encryption methods). Автентифікація, авторизація та облік (Authentication, authorization, and accounting). Огляд: Захист організаційних активів (Review: Protect organizational assets). Недоліки в системі (Flaws in the system). Мислення кібер-зловмисника (Cyber attacker mindset).

Питання для самостійного вивчення: *Визначте вразливі місця системи (Identify system vulnerabilities). Огляд: Вразливості систем (Review: Vulnerabilities in systems). Соціальна інженерія (Social engineering). Шкідливе програмне забезпечення (Malware). Веб-експлойти (Web-based exploits). Моделювання загроз (Threat modeling). Огляд: Загрози безпеці активів (Review: Threats to asset security).*

Тема 6. Post Exploitation. Cybersecurity IDR: Incident Detection & Response (2 год.)

Життєвий цикл реагування на інцидент (The incident response lifecycle). Операції з реагування на інциденти (Incident response operations). Інструменти

реагування на інциденти (Incident response tools). Огляд: Вступ до виявлення та реагування на інциденти (Review: Introduction to detection and incident response). Розуміння мережевого трафіку (Understand network traffic). Захоплення та перегляд мережевого трафіку (Capture and view network traffic). Перевірка пакетів (Packet inspection). Огляд: моніторинг і аналіз мережі (Review: Network monitoring and analysis).

Питання для самостійного вивчення: *Виявлення і перевірка інцидентів (Incident detection and verification). Створення та використання документації (Create and use documentation). Відповідь і відновлення (Response and recovery). Дії після інциденту (Post-incident actions). Огляд: Розслідування інциденту та реагування (Review: Incident investigation and response). Огляд журналів (Overview of logs). Огляд систем виявлення вторгнень (IDS) (Overview of intrusion detection systems (IDS)). Перегляньте інструменти SIEM (Reexamine SIEM tools). Огляд інструментів керування подіями безпеки інформації (SIEM) (Overview of security information event management (SIEM) tools). Огляд: мережевий трафік і журнали за допомогою інструментів IDS і SIEM (Review: Network traffic and logs using IDS and SIEM tools).*

Тема 7. Website Hacking. Conclusions and next steps. How To Prepare For Your Cybersecurity Career (2 год.)

Вимірювання впливу та цінності інновацій. Виявлення подій та інцидентів (Event and incident detection). Ваш вплив на захист даних (Your impact on data protection). Огляд: захистіть активи та повідомляйте про інциденти (Review: Protect assets and communicate incidents). Ескалація кібербезпеки (Escalation in cybersecurity). Загострювати чи не загострювати (To escalate or not to escalate). Час - це все (Timing is everything). Огляд: ескалація інцидентів (Review: Escalate incidents). Зрозумійте своїх зацікавлених сторін (Understand your stakeholders). Спілкуйтеся для впливу (Communicate for impact).

Питання для самостійного вивчення: *Візуальна комунікація за допомогою панелі керування (Visual communication using a dashboard). Огляд: ефективно спілкуйтеся, щоб впливати на зацікавлених сторін (Review: Communicate effectively to influence stakeholders). Надійні джерела мають велике значення (Reliable sources go a long way). Створіть свою мережу кібербезпеки (Build your cybersecurity network). Огляд: взаємодія зі спільнотою кібербезпеки (Review: Engage with the cybersecurity community). Знайдіть і підготуйтеся до роботи в сфері кібербезпеки (Find and prepare for a job in cybersecurity). Процес співбесіди з питань кібербезпеки (The cybersecurity job interview process). Дайте відповіді на запитання співбесіди (Answer interview questions). Розробіть ліфтовий пітч (Develop an elevator pitch). Огляд: знайдіть і подайте заявку на роботу в сфері кібербезпеки (Review: Find and apply for cybersecurity jobs).*

Зміст практичних занять

1. Setting up a Hacking Lab. Installing Kali Linux on VM (2 год).
2. Network Hacking. Pre-Connection Attacks. Gaining Access - WEP Cracking (2 год).
3. Network Hacking. WPA / WPA2 Cracking (2 год).
4. Network Hacking. Post Connection Attacks (3 год).
5. Gaining Access. Server Side Attacks (3 год).
6. Gaining Access. Client Side Attacks (2 год).
7. Social Engineering. (2 год).

Зміст самостійної роботи здобувачів

Розподіл годин, виділених на вивчення дисципліни

Найменування видів робіт	**Розподіл годин**	
	денна форма	**заочна форма**
Самостійна робота, год, у т.ч.:	60	82
Опрацювання матеріалу, викладеного на лекціях	10	4
Підготовка до практичних занять та контрольних заходів	10	4
Підготовка звітів з практичних робіт	10	4
Підготовка до поточного контролю	6	-
Опрацювання матеріалу, винесеного на самостійне вивчення	24	70

ПОЛІТИКА КУРСУ

Коротко, з покликанням на відповідну нормативну базу УКД, висвітлити питання:

1) щодо системи поточного і підсумкового контролю

Організація поточного та підсумкового семестрового контролю знань студентів, проведення практик та атестації, переведення показників академічної успішності за 100-бальною шкалою в систему оцінок за національною шкалою здійснюється згідно з "Положенням про систему поточного і підсумкового контролю, оцінювання знань та визначення рейтингу здобувачів освіти". Ознайомитись з документом можна за покликанням.

2) щодо оскарження результатів контрольних заходів

Здобувачі вищої освіти мають право на оскарження оцінки з дисципліни отриманої під час контрольних заходів. Апеляція здійснюється відповідно до «Положення про політику та врегулювання конфліктних ситуацій». Ознайомитись з документом можна за покликанням.

3) щодо відпрацювання пропущених занять

Згідно "Положення про організацію освітнього процесу" здобувач допускається до семестрового контролю з конкретної навчальної дисципліни (семестрового екзамену, диференційованого заліку), якщо він виконав усі види робіт, передбачені на семестр навчальним планом та силабусом/робочою програмою навчальної дисципліни, підтвердив опанування на мінімальному рівні результатів навчання (отримав ≥35 бали), відпрацював визначені індивідуальним навчальним планом всі лекційні, практичні, семінарські та лабораторні заняття, на яких він був відсутній. Ознайомитись з документом можна за покликанням.

4) щодо дотримання академічної доброчесності

"Положення про академічну доброчесність" закріплює моральні принципи, норми та правила етичної поведінки, позитивного, сприятливого, доброчесного освітнього і наукового середовища, професійної діяльності та професійного спілкування спільноти Університету, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання. Ознайомитись з документом можна за покликанням.

5) щодо використання штучного інтелекту

"Положення про академічну доброчесність" визначає політику щодо використання технічних засобів на основі штучного інтелекту в освітньому процесі. Ознайомитись з документом можна за покликанням.[1] *"Положення про систему запобігання та виявлення академічного плагіату, самоплагіату, фабрикації та фальсифікації академічних творів" містить рекомендації щодо використання в академічних текстах генераторів на основі штучного інтелекту. Ознайомитись з документом можна за покликанням.*

[1] визначається політика використання ШІ в навчальній дисципліні - дозволене/заборонене, правила використання

6) щодо використання технічних засобів в аудиторії та правила комунікації

Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та практичних занять дозволяється виключно у навчальних цілях (для уточнення певних даних, перевірки правопису, отримання довідкової інформації тощо). На гаджетах повинен бути активований режим «без звуку» до початку заняття. Під час занять заборонено надсилання текстових повідомлень, прослуховування музики, перевірка електронної пошти, соціальних мереж тощо. Під час виконання заходів контролю використання гаджетів заборонено (за винятком, коли це передбачено умовами його проведення). У разі порушення цієї заборони результат анульовується без права перескладання.
Комунікація відбувається через електронну пошту і сторінку дисципліни в Moodle.

7) щодо зарахування результатів навчання, здобутих шляхом формальної/інформальної освіти

Процедури визнання результатів навчання, здобутих шляхом формальної/інформальної освіти визначаються «Положенням про порядок визнання результатів навчання, здобутих шляхом неформальної та / або інформальної освіти». Ознайомитись з документом можна за покликанням.[2]

МЕТОДИ НАВЧАННЯ

При вивченні дисципліни застосовується комплекс методів для організації навчання студентів з метою розвитку їх логічного та абстрактного мислення, творчих здібностей, підвищення мотивації до навчання та формування особистості майбутнього фахівця в галузі інформаційних технологій.

Програмний результат навчання	Метод навчання	Метод оцінювання
ПРН1. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.	МН 1.1 - лекція, МН 1.2 - розповідь-пояснення, МН 1.3 - бесіда, МН 2.1 - ілюстрування, МН 2.4 - комп'ютерні і мультимедійні методи, МН 3.4 - практичні роботи, МН 4 - індуктивний метод, МН 5 - дедуктивний метод, МН 9 - порівняння, МН 10 -узагальнення, МН 13 -репродуктивний,	МФО 4 - поточний контроль, МФО 5 - усний контроль, МФО 6 -письмовий контроль, МФО 8 - тестовий контроль, МФО 1 - іспит

[2] визначається перелік електронних та інших ресурсів та умови перезарахування

	МН 15 -проблемно-пошуковий, МН 16 - евристичний, МН 19 - робота під керівництвом викладача, МН 20 - інтерактивні методи.	

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Контрольні заходи

Вид	***Зміст***	***% від загальної оцінки***	***Бал***	
			min	***max***
Поточні контрольні заходи	всього	**60**	**35**	**60**
Підсумкові контрольні заходи	екзамен	**40**	**25**	**40**
Всього:		**100**	**60**	**100**

Процедура проведення контрольних заходів, а саме поточного контролю знань протягом семестру та підсумкового семестрового контролю, регулюється «Положенням про систему поточного та підсумкового контролю оцінювання знань та визначення рейтингу студентів».

Фіксація **поточного** контролю здійснюється в “Електронному журналі обліку успішності академічної групи” на підставі чотирибальної шкали - “2”; “3”; “4”; “5”. У разі відсутності студента на занятті виставляється “н”. За результатами поточного контролю у Журналі, автоматично визначається підсумкова оцінка, здійснюється підрахунок пропущених занять.

Усі пропущені заняття, а також негативні оцінки студенти зобов'язані відпрацювати впродовж трьох наступних тижнів. У випадку недотримання цієї норми, замість “н” в журналі буде виставлено “0” (нуль балів), без права перездачі. Відпрацьоване лекційне заняття в електронному журналі позначається літерою «в».

Критерії оцінювання (за необхідності, поточного та/або підсумкового контролю):

«незадовільно»	володіє навчальним матеріалом на рівні елементарного розпізнавання і відтворення окремих фактів, елементів, об'єктів, що позначаються окремими словами чи реченнями; володіє матеріалом на елементарному рівні засвоєння, викладає його уривчастими реченнями, виявляє здатність висловити думку на елементарному рівні; володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу;
«задовільно»	володіє матеріалом на початковому рівні, значну частину матеріалу відтворює на репродуктивному рівні; володіє матеріалом на рівні, вищому за початковий, здатний за допомогою викладача логічно відтворити значну його частину; може відтворити значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, за допомогою викладача може аналізувати навчальний матеріал, порівнювати та робити висновки, виправляти допущені помилки;
«добре»	здатний застосовувати вивчений матеріал на рівні стандартних ситуацій, частково контролювати власні навчальні дії, наводити окремі власні приклади на підтвердження певних тверджень: вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати її на практиці, контролювати власну діяльність, виправляти помилки і добирати аргументи на підтвердження певних думок під керівництвом викладача; вільно володіє вивченим обсягом матеріалу, та вміє застосовувати його на практиці; вільно розв'язує задачі в стандартних ситуаціях, самостійно виправляє допущені помилки, добирає переконливі аргументи на підтвердження вивченого матеріалу;
«відмінно»	виявляє початкові творчі здібності, самостійно визначає окремі цілі власної навчальної діяльності, оцінює окремі нові факти, явища, ідеї; знаходить джерела інформації та самостійно використовує їх відповідно до цілей, поставлених викладачем; вільно висловлює власні думки і відчуття, визначає програму особистої пізнавальної діяльності, самостійно оцінює різноманітні життєві явища і факти, виявляючи особисту позицію щодо них; без допомоги викладача знаходить джерела інформації і використовує одержані відомості відповідно до мети та завдань власної пізнавальної діяльності; використовує набуті знання і вміння в нестандартних ситуаціях; виявляє особливі творчі здібності, самостійно розвиває власні обдарування і нахили, вміє самостійно здобувати знання.

До підсумкового контролю допускаються студенти які за результатами поточного контролю отримали не менше 35 балів. Усі студенти, що отримали 34 балів і менше, не допускаються до складання підсумкового контролю і на підставі укладання додаткового договору, здійснюють повторне вивчення дисципліни впродовж наступного навчального семестру. За результатами підсумкового контролю (диференційований залік/екзамен) студент може отримати 40 балів. Студенти, які під час підсумкового контролю отримали 24 бали і менше, вважаються такими, що не здали екзамен/диференційований залік і повинні йти на перездачу.

Загальна семестрова оцінка з дисципліни, яка виставляється в екзаменаційних відомостях оцінюється в балах (згідно з **Шкалою оцінювання знань за ЄКТС**) і є сумою балів отриманих під час поточного та підсумкового контролю.

Шкала оцінювання знань за ЄКТС:

Оцінка за національною шкалою	**Рівень досягнень, %**	**Шкала ECTS**
Національна диференційована шкала		
Відмінно	90 – 100	A
Добре	83 – 89	B
	75 – 82	C
Задовільно	67 – 74	D
	60 – 66	E
Незадовільно	35 – 59	FX
	0 – 34	F
Національна недиференційована шкала		
Зараховано	60 – 100	-
Не зараховано	0 – 59	-

Студенти, які не з'явилися на заліки/екзамени без поважних причин, вважаються такими, що одержали незадовільну оцінку.

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ[3]

Основна література

[3] обов’язково: враховувати вимоги ДСТУ 8302:2015 (відповідно до Наказу № 65, від 4.03. 2016), рекомендації Національного агентства з забезпечення якості вищої освіти, використовувати літературу за останні 5-7 років, наводити власні публікації за змістом навчальної дисципліни.

1. How Cybersecurity Really Works: A Hands-On Guide for Total Beginners by Sam Grubb - 2021, 216p.
2. Hacking and Security: The Comprehensive Guide to Penetration Testing and Cybersecurity (Rheinwerk Computing) by Michael Kofler, Klaus Gebeshuber, Peter Kloep, Frank Neugebauer – 2023, 1141p.
3. 11 Strategies of a World-Class Cybersecurity Operations Center by Kathryn Knerler, Ingrid Parker, Carson Zimmerman - 2022, 767p.
4. How to Measure Anything in Cybersecurity Risk 2nd Edition by Douglas W. Hubbard, Richard Seiersen - 2023, 368p.
5. Python for Cybersecurity: Using Python for Cyber Offense and Defense 1st Edition by Howard E. Poston III - 2022, 240p.
6. Navigating the Cybersecurity Career Path 1st Edition by Helen E. Patton - 2021, 336p.
7. CYBERSECURITY DATA PROTECTION: AGAINST ATTACKS AND THEAT TRENDS WITH LEGAL AND ETHICAL CONSIDERATIONS Kindle Edition by Reginald Miller - 2024, 143p.
8. CC Certified in Cybersecurity Study Guide (Sybex Study Guide) 1st Edition by Mike Chapple - 2024, 256p.
9. CYBERSECURITY DICTIONARY for Everyone: 1250 Terms Explained in Simple English by Tolga Tavlas - 2024, 429p.
10. CompTIA Security+ SY0-701 Certification Guide - Third Edition: Master cybersecurity fundamentals and pass the SY0-701 exam on your first attempt 3rd ed. Edition by Ian Neil - 2024, 622p.

Електронні інформаційні ресурси

11. Google Cyber Security - https://www.youtube.com/playlist?list=PLTZYG7bZ1u6puLWxUtqAjZkIB4dB_JFzk
12. Cybersecurity for Beginners | Google Cybersecurity Certificate - https://www.youtube.com/watch?v=_DVVNOGYtmU&list=PLTZYG7bZ1u6ocTMdhDwwmfjaNv134KcWn
13. How To Manage Security Risks & Threats | Google Cybersecurity Certificate - https://www.youtube.com/watch?v=34BtwcL7Mkg&list=PLTZYG7bZ1u6ocTMdhDwwmfjaNv134KcWn&index=2

14. Internet Networks & Network Security - https://www.youtube.com/watch?v=NIRXtMg-0z8&list=PLTZYG7bZ1u6ocTMdhDwwmfjaNv134KcWn&index=3
15. The Basics of Computing Security: Linux & SQL - https://www.youtube.com/watch?v=gmzQgmlR1eI&list=PLTZYG7bZ1u6ocTMdhDwwmfjaNv134KcWn&index=4
16. Cybersecurity Assets, Network Threats & Vulnerabilities - https://www.youtube.com/watch?v=Rgl7C0P6NsE&list=PLTZYG7bZ1u6ocTMdhDwwmfjaNv134KcWn&index=5
17. Cybersecurity IDR: Incident Detection & Response - https://www.youtube.com/watch?v=MsGl6lX-YaI&list=PLTZYG7bZ1u6ocTMdhDwwmfjaNv134KcWn&index=6
18. How To Prepare For Your Cybersecurity Career | Google Cybersecurity Certificate - https://www.youtube.com/watch?v=3EgYr7jR4NI&list=PLTZYG7bZ1u6ocTMdhDwwmfjaNv134KcWn&index=8