ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»

Факультет суспільних і прикладних наук

Кафедра права та публічного управління
Кафедра Інформаційних технологій

ЗАТВЕРДЖУЮ
Проректор з методичної роботи
_____ Ярослав ШТАНЬКО
"29" ____10____ 2024 р.

КІБЕРБЕЗПЕКА І УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань:	26 Цивільна безпека
Спеціальність:	262 Правоохоронна діяльність
Освітньо-професійна (освітньо-наукова) програма:	Правоохоронна діяльність
Освітній рівень:	перший (бакалаврський)
Статус дисципліни:	обов'язкова
Мова викладання, навчання та оцінювання:	українська

Івано-Франківськ
2024

РОЗРОБНИК:
д.ю.н., професор, професор
кафедри права та
публічного управління Микола КАРЧЕВСЬКИЙ

ЗАТВЕРДЖЕНО:
на засіданні кафедри інформаційних технологій
протокол № 1 від 28.09.24р.

Завідувач кафедри Сергій ВАЩИШАК

УЗГОДЖЕНО:

Гарант ОП Євген ПИСЬМЕНСЬКИЙ

на засіданні кафедри права та публічного
правління протокол №4 від 21.11. 2024 р.

В.о. Завідувач кафедри Олександра ПТАШНИК

СХВАЛЕНО:

на засіданні Науково-методичної ради, протокол №9 від 29.11. 2024 р

e-mail	mykola.karchevskyi@ukd.edu.ua
Номер аудиторії чи кафедри	Кафедра права та публічного управління
Посилання на сайт	Микола Карчевський
Сторінка курсу в СДО	https://online.ukd.edu.ua/enrol/index.php?id=6882

Анотація навчальної дисципліни «Кібербезпека та управління інформаційними ресурсами **»**

ВСТУП

У сучасних умовах цифровізації суспільства кібербезпека є невід'ємним елементом безпеки держави, суспільства, бізнесу та кожного громадянина. Для фахівців у сфері правоохоронної діяльності вивчення кібербезпеки та управління інформаційними ресурсами є особливо важливим, адже їхня професійна діяльність безпосередньо пов'язана із захистом інформації, реагуванням на кіберінциденти та забезпеченням інформаційної безпеки держави та громадян.

Злочинний світ активно використовує цифрові технології, застосовуючи складні методи кібератак, соціальної інженерії та використання штучного інтелекту для незаконних дій. Успішне протистояння таким загрозам потребує від правоохоронців не лише базових знань у сфері інформаційної безпеки, а й глибокого розуміння механізмів атак, сучасних технологічних рішень для їх виявлення, запобігання та реагування.

Дисципліна «Кібербезпека та управління інформаційними ресурсами» спрямована на формування у студентів необхідних знань та практичних навичок для ідентифікації кіберзагроз, управління інформаційними активами, розробки політик інформаційної безпеки, а також реагування на кіберінциденти. Опанування цієї дисципліни дозволить студентам ефективно працювати у правоохоронних органах, кіберпідрозділах, державних структурах та приватних компаніях, які займаються захистом інформаційних ресурсів.

- Згідно з вимогами освітньо-професійних та освітньо-кваліфікаційних програм студенти повинні **знати**:
- Основні поняття кібербезпеки, зокрема активи, загрози, уразливості та ризики.
- Класифікацію та характерні риси кіберзагроз, методи атак та способи їх виявлення.
- Нормативно-правову базу України та міжнародні стандарти кібербезпеки (ISO/IEC 27001, NIST Cybersecurity Framework).
- Основні політики кібербезпеки, управління IT-активами та механізми захисту інформації.
- Технологічні рішення для забезпечення кібербезпеки: шифрування, міжмережеві екрани, системи виявлення та запобігання вторгненням (IDS/IPS), багатофакторну автентифікацію (MFA).
- Життєвий цикл кіберінцидентів та основні підходи до реагування на кіберзагрози.
- Використання штучного інтелекту та великих даних у сфері кібербезпеки.

- **вміти**:

- Ідентифікувати кіберзагрози та оцінювати їхній рівень ризику для інформаційних активів.
- Застосовувати методи аналізу загроз та інцидентів за допомогою сучасних інструментів кіберзахисту.
- Розробляти та впроваджувати політики інформаційної безпеки для організацій та установ.
- Використовувати механізми захисту даних, зокрема шифрування, контроль доступу, резервне копіювання.
- Аналізувати вразливості систем та застосовувати методи їх усунення.
- Здійснювати моніторинг та реагування на кіберінциденти, використовуючи сучасні технологічні засоби (SIEM-системи, антивірусне програмне забезпечення, аналіз мережевого трафіку).
- Інтерпретувати правові аспекти кібербезпеки та застосовувати їх у сфері правоохоронної діяльності.
- Виявляти та документувати кіберзлочини, використовуючи методи цифрової криміналістики.

Компетентності та результати навчання, яких набувають здобувачі освіти внаслідок вивчення навчальної дисципліни (шифри та зміст компетентностей та програмних результатів навчання вказано відповідно до ОПП "Правоохоронна діяльність" (2024/2025).

Шифр та назва компетентності	Результати навчання
СК8. Здатність ефективно забезпечувати публічну безпеку та порядку.	РН2. Організовувати культурний діалог на рівні, необхідному для ефективної професійної діяльності
СК9. Здатність ефективно застосовувати сучасні техніку і технології захисту людини, матеріальних цінностей і суспільних відносин від проявів криміногенної обстановки та обґрунтовувати вибір засобів та систем захисту людини і суспільних відносин.	РН4. Формулювати і перевіряти гіпотези, аргументувати висновки
СК11. Здатність до аналізу та оцінки ризиків що впливають на вчинення адміністративних правопорушень та кримінальних злочинів (проступків).	РН8. Здійснювати пошук інформації у доступних джерелах для повного та всебічного встановлення необхідних обставин.

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Курс	**1**		
Семестр	**2**		
Кількість кредитів ЄКТС	**3**		
Аудиторні навчальні заняття		**денна форма**	**заочна форма**
	лекції	14	-
	семінари, практичні	28	-
Самостійна робота		48	_
Форма підсумкового контролю	**екзамен**		

Тема 1. Вступ до кібербезпеки

Кібербезпека та інформаційна безпека. Актуальність кібербезпеки в умовах цифровізації суспільства. Значення кібербезпеки для державних установ, бізнесу та громадян.

Основні поняття кібербезпеки: активи, загрози, уразливості, ризики. Активи: що потрібно захищати (дані, системи, люди, процеси). Загрози: що може завдати шкоди (зловмисники, природні катастрофи, помилки персоналу). Уразливості: слабкі місця системи (незахищені мережі, застаріле ПЗ). Ризики: імовірність втрати чи шкоди для активів. Оцінка ризиків

Розвиток кіберзагроз: історичний аспект та сучасні тренди. Історія перших вірусів і атак: від Morris Worm до сучасних APT-угруповань. Еволюція кіберзагроз: класичні віруси та черв'яки; мережеві атаки (DDoS, маніпуляція даними); сучасні виклики: ransomware, deepfake-атаки, використання штучного інтелекту зловмисниками.

Нормативне регулювання кібербезпеки. Міжнародні стандарти кібербезпеки: ISO/IEC 27001 (система управління інформаційною безпекою), NIST Cybersecurity Framework. Закон України "Про основні засади забезпечення кібербезпеки України". Діяльність CERT-UA.

Завдання для семінарського заняття.

1. *Доповнити наведені у лекції чинники значення кібербезпеки для держави, бізнесу та громадян на основі аналізу чинного законодавства України*

2. *Проаналізувати визначення поняття «актив інформаційної безпеки», що наводяться у глосарії National Institute of Standards and Technology (посилання в лекції) та запропонувати власний висновок щодо найбільш вдалого.*
3. *На основі Закону України "Про основні засади забезпечення кібербезпеки України" та ISO 27001 запропонувати аналіз кіберзагрози, що мала місце в Україні, коротко описати її наслідки*
4. *Проаналізуйте інфографіку глобальних ризиків з матеріалів світового економічного форуму 2023 року. Які загрози можна віднести до загроз кібербезпеки. Обґрунтуйте свої бачення.*
5. *Наскрізний проєкт ч.1. Проягом вивчення курсу, працюючи у групах, представити проєкт політики кібербезпеки для установи, підприємства, організації, стартапу тощо. Визначити активи, загрози, уразливості та ризики для Ваших проєктів.*

Тема 2. IT активи та їх захист

IT активи: поняття та види. Дані: персональні дані, корпоративна інформація, державні реєстри. Програмне забезпечення: системи управління базами даних, прикладні програми. Інфраструктура: сервери, мережі, системи зберігання даних.

Класифікація IT активів за критичністю. Критерії оцінки критичності. Значення для бізнесу чи організації. Потенційні наслідки втрати чи компрометації. Приклади класифікації: особисті дані користувачів як критичні, загальнодоступні ресурси як некритичні.

Політики управління IT активами. Документ, що регулює процеси доступу, використання та захисту активів. Елементи політики: розмежування прав доступу; регламент роботи з персональними даними (GDPR, Закон України "Про захист персональних даних"); резервне копіювання і відновлення даних. Ролі в управлінні: власники інформації, адміністратори ресурсів, користувачі (працівники, підрядники).

Завдання для семінарського заняття.

1. *Обговорення кейсів витоку даних у великих компаніях (наприклад, Facebook або Uber).*
2. *Пропозиції щодо політики доступу до IT активів для університету. Для виконання завдання обов'язково використати NIST Data Classification Guide.*
3. *Наскрізний проєкт ч.2. Визначити IT активи для вашого проєкту та запропонувати відповідні політики доступу.*

Тема 3. Кіберзагрози та методи атак

Визначення кіберзагроз. Класифікація кіберзагроз. За джерелами загроз: внутрішні (недбалість працівників, зловмисні дії співробітників); зовнішні (хакери, кібершпигуни, організовані кіберзлочинні угруповання). За характером впливу (порушення конфіденційності, порушення цілісності, порушення

доступності). За метою: економічні (шахрайство, крадіжка даних); політичні (кібершпигунство, пропаганда); соціальні (дезінформація, маніпуляція суспільною думкою).

Методи атак та їхні характеристики. Фішинг, підроблені електронні листи або сайти для крадіжки облікових даних. Шкідливе ПЗ: віруси, трояни. Соціальна інженерія, маніпуляція людьми для отримання доступу до інформації (дзвінки, фальшиві листи). DDoS-атаки (розподілені атаки на відмову в обслуговуванні). SQL-ін’єкції, впровадження шкідливого коду в запити до баз даних. Ransomware (програми-вимагачі), шифрування даних із вимогою викупу.

Атаки із застосуванням штучного інтелекту. Автоматизація фішингу, генерація deepfake-відео для маніпуляцій. IoT-атаки, злом "розумних" пристроїв (камери, термостати) для доступу до мереж. Zero-day атаки, використання невідомих вразливостей програмного забезпечення.

Відповідальність і етичні аспекти. Кримінальна відповідальність за правопорушення в сфері використання інформаційних технологій (ст.ст. 361 - 363-1 Кримінального кодексу України). Використання кіберзасобів у військових та політичних цілях. Роль етичних хакерів у забезпеченні безпеки.

Завдання для семінарського заняття.

1. *Аргументоване повідомлення про те, який метод атаки слухачі курсу вважають найбільш небезпечним і чому?*
2. *Дослідження реального прикладу кіберзагрози, що сталася в Україні чи світі, та коротке описання методів атаки та наслідків. Для відповіді бажано скористатися ресурсами CERT-UA.*
3. *Наскрізний проєкт ч. 3. Визначити можливі кіберзагрози для Вашого проєкту*

Тема 4. Інформаційна безпека в організації

Захист даних як основа довіри між компанією, клієнтами та партнерами. Типові виклики в організації: людський фактор, невчасне оновлення ПЗ, відсутність чітких процедур і політик.

Політики інформаційної безпеки. Документ, що визначає правила, процедури та стандарти для забезпечення безпеки. Основні компоненти політики: розмежування доступу до даних; процедури резервного копіювання та відновлення даних; регламент реагування на інциденти; навчання працівників з питань безпеки. Регулярний аудит політик.

Управління доступом. Моделі доступу. DAC (Discretionary Access Control): власник даних визначає доступ. RBAC (Role-Based Access Control): доступ визначається роллю користувача в організації. ABAC (Attribute-Based Access Control): доступ базується на атрибутах (час, місце, рівень). Інструменти для управління доступом. Active Directory. Системи SSO (Single Sign-On). MFA (багатофакторна автентифікація).

Ролі та відповідальності в інформаційній безпеці. CISO (Chief Information Security Officer): стратегічне управління безпекою. IT-відділ: технічне забезпечення захисту. Користувачі: дотримання правил безпеки.

Резервне копіювання та відновлення. Політика "3-2-1".

Регламент реагування на інциденти кібербезпеки.

Важливість навчання працівників. Проведення тренінгів з протидії фішинговим атакам. Інструкції щодо безпечної роботи з пристроями та системами.

Завдання для семінарського заняття.

1. Аналіз кейсу співробітник отримує фальшивий лист із запитом на доступ до конфіденційної інформації. Як діяти?

2. Скласти коротку політику доступу до корпоративної Wi-Fi мережі.

3. Запропонувати вдосконалення до політики інформаційної безпеки університету.

4. Наскрізний проєкт ч. 4. На підставі попередніх завдань підготувати чорнову версію політики кібербезпеки Вашого проєкту.

Тема 5. Базові технологічні рішення кібербезпеки

Роль технологій у запобіганні, виявленні та реагуванні на кіберзагрози. Еволюція захисних рішень: від антивірусів до комплексних систем кіберзахисту.

Шифрування даних. Типи шифрування. Симетричне шифрування. Асиметричне шифрування. Захист електронної пошти (PGP). Шифрування дисків (BitLocker, VeraCrypt). SSL/TLS для захисту веб-трафіку. Криптографічні протоколи HTTPS, IPsec, OpenVPN.

Міжмережеві екрани. Типи міжмережевих екранів.

Системи виявлення та запобігання вторгненням (IDS/IPS). IDS (Intrusion Detection System): система виявляє підозрілу активність, але не блокує її. IPS (Intrusion Prevention System): виявляє та блокує загрози в режимі реального часу.

Інструменти: Snort, Suricata. Приклади кейсів: атаки DDoS та їх нейтралізація за допомогою IDS/IPS.

Захист кінцевих пристроїв. Антивірусні системи: як працюють та чому важливі (ESET, Windows Defender). Можливості моніторингу та аналізу поведінки пристроїв. Багатофакторна автентифікація (MFA).

Практичний кейс: санкції США проти компанії Kaspersky Lab.

Захист хмарних сервісів. Доступ до ресурсів з різних пристроїв і локацій. Захист від атак на API.

Завдання для семінарського заняття.

1. Перевірити сертифікат SSL/TLS на реальному сайті.

2. Описати, які технології кіберзахисту доцільно використовувати для захисту мережі в університеті.

3. Наскрізний проєкт ч. 5. Запропонуєте перелік технічних засобів кібербезпеки Вашого проєкту з описанням функціонального призначення по кожній позиції.

Тема 6. Реагування на кіберінциденти

Що таке кіберінцидент? Мета реагування на кіберінциденти. Аналіз практичних кейсів вдалого та невдалого реагування.

Життєвий цикл кіберінциденту. Етапи реагування на кіберінциденти. Підготовка: створення плану реагування, навчання персоналу, використання інструментів моніторингу. Виявлення: методи ідентифікації інцидентів, приклади ознак інцидентів. Аналіз: оцінка масштабу загрози, визначення впливу на системи та дані. Локалізація: ізоляція уражених систем, запобігання поширенню загрози. Усунення: видалення шкідливого програмного забезпечення, встановлення оновлень безпеки. Відновлення: перевірка систем після очищення, повернення систем до нормального стану. Підсумковий аналіз: висновки з інциденту, внесення змін до планів безпеки.

Інструменти моніторингу та аналізу. SIEM-системи (Security Information and Event Management). Популярні рішення: Splunk, ArcSight, IBM QRadar. Інструменти аналізу шкідливого ПЗ. Пісочниці (Sandbox): аналіз програм у безпечному середовищі. Аналітичні платформи: VirusTotal, Hybrid Analysis. Захист від DDoS: Cloudflare, Akamai. Відстеження атак: Wireshark для аналізу мережевого трафіку.

Взаємодія з CERT та іншими інституціями. CERT-UA: роль у забезпеченні кібербезпеки України. Співпраця з органами правопорядку (кіберполіція). Міжнародна взаємодія: FIRST, ENISA, Global Forum on Cyber Expertise.

Завдання для семінарського заняття:

1. Сценарій: у мережі інтернет магазину зафіксовано аномальний сплеск трафіку. Студенти повинні: обґрунтувати висновок щодо можливого інциденту, визначити можливу причину, запропонувати кроки для локалізації та усунення проблеми.

Бажано використовувати: посібник NIST "Computer Security Incident Handling Guide" (SP 800-61); огляд інструментів аналізу інцидентів від CERT-UA.

2. Наскрізний проєкт ч. 6. Деталізуйте розділ реагування на інциденти у розробленій Вами політиці кібербезпеки проєкту

Тема 7. Перспективи кібербезпеки: штучний інтелект і великі дані

Зростання кількості пристроїв і даних у мережах (IoT, хмари) та ускладнення атак через використання нових технологій як передумови автоматизації процесів кібербезпеки.

ШІ у кібербезпеці. Використання машинного навчання для аналізу аномалій у трафіку. Поведінкова аналітика. Автоматизація реагування (Splunk, QRadar). Прогнозування атак.

Проблемні аспекти використання ШІ у кібербезпеці. Помилкові спрацьовування. Використання ШІ зловмисниками. Автоматизація фішингових атак. Генерація deepfake для соціальної інженерії. Використання ШІ для автоматизації сканування вразливостей.

Великі дані: аналітика загроз і прогнозування атак. Джерела великих даних: логи систем, дані про трафік, інформація з соціальних мереж. Технології аналізу. Інструменти візуалізації (Tableau, GoogleLooker).

Кейси: Crystal – система аналізу блокчейнів віртуальних активів, її використання для розслідування несанкціонованих транзакцій. Як великі дані допомогли виявити складні APT-угруповання.

Етичні аспекти та кібербезпека майбутнього. Використання штучного інтелекту для масового спостереження. Генеративні моделі для атак. Баланс між безпекою та приватністю: як уникнути надмірного втручання у приватне життя громадян.

Zero Trust: концепція повної недовіри до будь-якої активності у мережі. Колективна безпека: важливість міжнародної співпраці для подолання глобальних загроз.

Завдання для семінарського заняття.

1. *Знайти реальний приклад використання ШІ або великих даних для забезпечення кібербезпеки та підготувати короткий звіт.*
2. *Наскрізний кейс ч. 7. Презентуйте політику інформаційної безпеки Вашого проєкту ураховуючи такі тренди як штучний інтелект та великі дані.*

Зміст самостійної роботи студентів

Розподіл годин, виділених на вивчення дисципліни «Кібербезпека і управління інформаційними ресурсами»

Найменування видів робіт	**Розподіл годин**	
	денна форма	**заочна форма**
Самостійна робота, год, у т.ч.:	48	-
Опрацювання матеріалу, викладеного на лекціях	14	-
Підготовка до практичних занять та контрольних заходів	12	-
Підготовка звітів з практичних робіт	-	-
Підготовка до поточного контролю	10	-
Опрацювання матеріалу, винесеного на самостійне вивчення	12	-

ПОЛІТИКА КУРСУ

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. “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.

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, окрім виробничої необхідності. 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

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 права.

Програмний результат навчання	**Метод навчання**	**Метод оцінювання**
ПРН3. Збирати необхідну інформацію з різних джерел, аналізувати і оцінювати її.	словесні методи (лекція, розповідь пояснення); наочні методи (ілюстрування, комп’ютерні і мультимедійні методи);	усний контроль, поточний контроль, програмований контроль

	інтерактивні методи (Case study, дискусія, мозковий штурм, робота в команді (групах))	
ПРН9. Користуватись державною системою урядового зв'язку, Національною системою конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку.	словесні методи (лекція, розповідь пояснення); наочні методи (ілюстрування, комп'ютерні і мультимедійні методи); інтерактивні методи (дискусія, мозковий штурм, робота в команді (групах)).	усний контроль, поточний контроль, програмований контроль
ПРН3. Збирати необхідну інформацію з різних джерел, аналізувати і оцінювати її.	словесні методи (лекція, розповідь пояснення); наочні методи (ілюстрування, комп'ютерні і мультимедійні методи); інтерактивні методи (Case study, дискусія, мозковий штурм, робота в команді (групах)	усний контроль, поточний контроль, програмований контроль

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Вид	**Зміст**	**% від загальної оцінки**	**Бал**	
			min	**max**
Поточні контрольні заходи	всього	60	35	60
Підсумкові контрольні заходи	екзамен	40	24	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.

Критерії оцінювання:

«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.

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».

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 залік без поважних причин, вважаються такими, що одержали незадовільну оцінку.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна література

1. Холод О.М. Комунікаційні технології: Підручник. К.: ЦНЛ, 2013.- 212с.

2. Томашевський О.М., Цегелик Г.Г., Вітер М.Б., Дубук В.І. Інформаційні технології та моделювання: Навч.посібник. К.: ЦУЛ, 2012.

296 с.

3. Буйницька О.П. Інформаційні технології та технічні засоби навчання: Навч.посібник. К.: ЦУЛ, 2012. 240 с.

Електронні інформаційні ресурси

4. Швачич Г. Г. Сучасні інформаційно-комунікаційні технології : навч. посіб. Г. Г. Швачич, В. В.Толстой, Л. М. Петречук [та ін.]. – Дніпро: НМетАУ, 2017. 230 с. URL: https://nmetau.edu.ua/file/ikt_tutor.pdf (дата звернення: 25.08. 2024).

5. Інформаційно-комунікаційні технології в бізнесі : навч. посіб. уклад. М. О. Чупріна. – К.: КПІ ім. Ігоря Сікорського, 2020. 116 с. URL: https://ela.kpi.ua/bitstream/123456789/33703/1/Infor_tech.pdf (дата звернення: 25.08. 2024).

6. Гуревич Р. С. Інформаційно-комунікаційні технології в професійній освіті : монографія. Р. С. Гуревич, М. Ю. Кадемія, М. М. Козяр; за ред. Р. С. Гуревича. Львів : Льв. держ. ун-т безпеки життєдіяльності, 2012. 506 с. URL: http://ito.vspu.net/repozitariy/Kademiia/stati/15last/7_15zIKT.pdf (дата звернення: 25.08. 2024).