ФАХОВИЙ КОЛЕДЖ
ЗАКЛАДУ ВИЩОЇ ОСВІТИ «УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»

Циклова комісія з юридичних дисциплін

ЗАТВЕРДЖЕНО
Директор Фахового коледжу
ЗВО «Університет Короля Данила»
_____Володимир ЯСЛИК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Основи кібербезпеки і управління інформаційними ресурсами»

Галузь знань : ***26 Цивільна безпека***
Спеціальність: ***262 Правоохоронна діяльність***
Освітньо-професійна програма ***«Правоохоронна діяльність»***

Освітньо-професійний ступінь – *фаховий молодший бакалавр*
Статус дисципліни – *обов'язкова*
Мова викладання, навчання та оцінювання – *українська*

Івано-Франківськ, 2025

Розробник:
КАРЧЕВСЬКИЙ Микола Віталійович – викладач циклової комісії з юридичних дисциплін Фахового коледжу ЗВО «Університет Короля Данила», спеціаліст, доктор юридичних наук, професор.

Розглянуто та схвалено на засіданні циклової комісії
з юридичних дисциплін
Протокол № 1 від «28 » серпня 2025 р.
Голова циклової комісії **Світлана ХОДАК**

Схвалено методичною радою
Фахового коледжу
ЗВО «Університет Короля Данила»
Протокол № 1 від «28» серпня 2025 р.
Голова методичної ради **Олег КЛІЩ**

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 «Основи кібербезпеки 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.

Метою вивчення дисципліни є формування у студентів системи знань і практичних навичок у сфері кібербезпеки та управління інформаційними ресурсами, необхідних для ідентифікації й аналізу кіберзагроз, захисту інформаційних активів, розробки та впровадження політик інформаційної безпеки, а також ефективного реагування на кіберінциденти у професійній діяльності правоохоронця, працівника державних і приватних структур.

Предметом дисципліни є закономірності, принципи, правові та організаційно-технічні засади забезпечення кібербезпеки, управління інформаційними ресурсами, механізми протидії кіберзагрозам і практичні інструменти захисту даних у правоохоронній, державній та приватній діяльності

Основними завданнями вивчення навчальної дисципліни є:

1. Ознайомити студентів із базовими поняттями та категоріями кібербезпеки (активи, загрози, уразливості, ризики).
2. Дати знання про класифікацію кіберзагроз, методи атак і засоби їх виявлення та запобігання.
3. Сформувати розуміння нормативно-правової бази України та міжнародних стандартів у сфері кібербезпеки.
4. Навчити застосовувати сучасні технологічні рішення для забезпечення захисту інформаційних ресурсів (шифрування, міжмережеві екрани, IDS/IPS, MFA тощо).
5. Розвинути практичні навички аналізу кіберзагроз, оцінювання ризиків та розробки політик інформаційної безпеки.
6. Ознайомити з життєвим циклом кіберінцидентів та методами ефективного реагування на них.
7. Сформувати усвідомлення ролі штучного інтелекту та великих даних у сфері кібербезпеки та пов'язаних етичних викликів.
8. Прищепити практичні навички особистої кібер-гігієни для безпечної поведінки в цифровому середовищі.

У результаті вивчення навчальної дисципліни здобувач освіти повинен **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.

У результаті вивчення навчальної дисципліни здобувачі освіти повинні **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.

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

		Денна форма	Заочна форма
Курс		**3**	**3**
Семестр		**5**	**5**
Кількість кредитів ECTS		**3**	**3**
Аудиторні навчальні заняття(год.)	**лекції**	**-**	**-**
	практичні	**30**	**6**
Самостійна робота		**60**	**84**
Форма підсумкового контролю		**залік**	

СТРУКТУРНО-ЛОГІЧНА СХЕМА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ:

Пререквізити	Постреквізити
Теорія держави і права	Практикум зі складання процесуальних документів

ЗАГАЛЬНІ ТА СПЕЦІАЛЬНІ КОМПЕТЕНТНОСТІ
Яких набувають студенти внаслідок вивчення навчальна дисципліна «Основи кібербезпеки та управління інформаційними ресурсами» згідно з освітньо-професійною програмою «Правоохоронна діяльність»

Результати навчання	Код та назва компетентності
РН3 Використовувати основні методи та засобизабезпечення правопорядку в державі, дотримуватись прав і свобод людини.	ЗК3. Здатність діяти на основі етичних міркувань (мотивів).
РН5. Здійснювати пошук необхідної для професійної діяльності інформації у різних джерелах та оцінювати її релевантність та достовірність. РН 10. Застосовувати сучасні пристрої та технології обробки інформації, засоби орієнтування на місцевості, технічні прилади та спеціальні засоби, інформаційно-пошукові системи та бази даних. РН 19. Здійснювати заходи, спрямовані на запобігання вчиненню правопорушень.	СК 1. Усвідомлення функцій держави, форм реалізації цих функцій, правових основ правоохоронної діяльності, дотримання основних принципів реалізації правоохоронної функції держави. СК3. Здатність застосовувати знання основних засад та інститутів національного права. СК 13. Здатність брати участь у забезпеченні публічної безпеки та порядку, охорони об'єктів усіх форм власності, запобіганні, виявленні та припиненні адміністративних і кримінальних правопорушень, у здійсненні заходів, спрямованих на усунення загроз життю та здоров'ю фізичних осіб.

ПОЛІТИКА КУРСУ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Відповідно до Положення про організацію освітнього процесу у Фаховому коледжі ЗВО «Університету Короля Данила», студенти зобов'язані виконувати вимоги освітньо-професійної програми, графік освітнього процесу та вимоги навчального плану.

Курс передбачає обов'язкове вивчення та виконання здобувачами усіх вимог/тем / завдань, передбачених робочою програмою навчальної дисципліни та вказаних у СДО на сторінці курсу.

ПОВЕДІНКА В АУДИТОРІЇ
Усі учасники освітнього процесу повинні дотримуватися норм і правил внутрішнього розпорядку відповідно до Статуту ЗВО “Університет Короля Данила”, Положення про Фаховий коледж та Положення про організацію освітнього процесу Фаховому коледжі ЗВО “Університету Короля Данила”.
ДОТРИМАННЯ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ
На початку вивчення курсу викладач ознайомлює студентів з основними пунктами Положення про академічну доброчесність, відповідно до якого здійснюється освітній процес. Під час виконання творчих робіт, письмових тестових або практичних завдань студенти спираються тільки на власні знання, не використовуючи інших джерел інформації, крім випадків, коли пошук додаткової інформації є умовою виконання завдання, про що попередньо повідомляє викладач.
ВІДПРАЦЮВАННЯ ПРОПУЩЕНИХ ЗАНЯТЬ
Усі пропущені заняття, а також отримані 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.
ОСКАРЖЕННЯ ПРОЦЕДУРИ ПРОВЕДЕННЯ ТА РЕЗУЛЬТАТІВ КОНТРОЛЬНИХ ЗАХОДІВ (ПІДСУМКОВОГО КОНТРОЛЮ)
Оскарження процедури проведення та результатів контрольних заходів відбувається відповідно до Положення про систему контролю та оцінювання знань здобувачів освіти Фахового коледжу.

МЕТОДИ НАВЧАННЯ ТА ДІАГНОСТИКА РЕЗУЛЬТАТІВ НАВЧАННЯ

Результати навчання	Методи навчання	Форми та методи оцінювання
Освітній компонент «Основи кібербезпеки і управління інформаційними ресурсами»		
РН3 Використовувати основні методи та засобизабезпечення правопорядку в державі, дотримуватись прав і свобод людини.	пояснювально-ілюстративний метод; інтерактивні методи навчання бесіда, бесіда-діалог, мозковий штурм, рольові і ділові ігри	Залік Поточний контроль. Усний контроль. Письмовий контроль. Тестовий контроль.
РН5. Здійснювати пошук необхідної для професійної діяльності інформації у різних джерелах та оцінювати її релевантність та достовірність.		

РН 10. Застосовувати сучасні пристрої та технології обробки інформації, засоби орієнтування на місцевості, технічні прилади та спеціальні засоби, інформаційно-пошукові системи та бази даних.		
РН 19. Здійснювати заходи, спрямовані на запобігання вчиненню правопорушень.		

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Система оцінювання результатів навчання студентів ІІІ курсу за освітньо-професійною програмою «Правоохоронна діяльність» здійснюється відповідно до «Положення про систему контролю та оцінювання знань здобувачів освіти Фахового Коледжу ЗВО «Університету Короля Данила». Кожен вид контролю передбачений з урахуванням результатів навчання.

1. Поточний контроль – усне опитування та виконання письмових завдань (тестів), виступи, презентації на практичних заняттях. Оцінювання здійснюється за національною чотирибальною шкалою – «2»; «3»; «4»; «5».

Фіксація поточного контролю здійснюється в «Електронному журналі обліку успішності академічної групи» на підставі чотирибальної шкали. У разі відсутності здобувача освіти на занятті виставляється «н». За результатами поточного контролю у Журналі автоматично обчислюється підсумкова оцінка та здійснюється підрахунок пропущених занять.

Усереднена оцінка переводиться в 100-бальну шкалу згідно нижченаведеної таблиці.

Усі пропущені заняття, а також негативні оцінки здобувачі освіти зобов'язані відпрацювати впродовж трьох наступних тижнів. У випадку недотримання цієї норми, замість «н» в журналі буде виставлено «0» (нуль балів) без права перездачі.

Здобувачі освіти повинні мати оцінки з не менше 50% аудиторних занять.

До підсумкового контролю допускаються здобувачі освіти, які за результатами поточного контролю отримали 35 балів і більше. Усі здобувачі освіти, що отримали 34 бали і менше, не допускаються до складання підсумкового контролю і на підставі укладання додаткового договору, здійснюють повторне вивчення дисципліни впродовж наступного навчального семестру.

2. Підсумковий (семестровий) контроль проводиться для встановлення рівня досягнення здобувачами освіти програмних результатів навчання з навчальної дисципліни (освітнього компонента), після завершення вивчення дисципліни.

Підсумковий контроль знань проводиться у формі заліку у вигляді захисту наскрізного проєкту.

Проєкт виконується поетапно: під час опрацювання кожної теми студенти розробляють окремі розділи політики кібербезпеки для обраної організації, установи, підприємства чи стартапу. У ході роботи студенти визначають інформаційні активи, ідентифікують кіберзагрози, аналізують уразливості, формують політики доступу, пропонують технічні та організаційні засоби захисту, а також описують процедури реагування на кіберінциденти.

Підсумковим результатом є комплексний документ – політика кібербезпеки об’єкта дослідження, що відображає знання та навички, набуті упродовж курсу.

Студенти презентують результати роботи, аргументують обрані рішення, демонструють практичні навички оцінювання ризиків, планування заходів інформаційної безпеки та застосування правових норм у сфері кібербезпеки. Оцінювання здійснюється за критеріями:

- повнота та логічність представлення матеріалу (10 балів);
- практична обґрунтованість запропонованих заходів (10 балів);
- врахування правових та етичних аспектів (10 балів);
- уміння відповідати на запитання та захищати власні висновки (10 балів).

Таким чином, наскрізний проєкт поєднує всі теми дисципліни та виступає інтегрованим підсумковим завданням курсу.

3. Оцінювання самостійної роботи проводиться як під час поточного, так і під час підсумкового контролю знань. Поточний контроль самостійної роботи передбачає усну відповідь, написання доповіді (реферат), створення презентацій, відпрацювання практичних навичок тощо.

Оцінювання самостійної роботи, яка передбачена в тематичному плані дисципліни разом з аудиторною роботою, здійснюється під час проведення практичних занять. Виставлення балів за самостійну роботу під час поточного контролю обов’язково супроводжується оцінювальними судженнями. Бали додаються до балів, які отримав здобувач освіти під час поточного контролю, але не більше, ніж кількість балів з оцінювання окремої теми заняття.

Оцінювання тем, які виносяться лише на самостійну роботу і не входять до тем аудиторних занять, контролюється під час підсумкового контролю.

Самоконтроль передбачений у формі самоперевірки засвоєних знань після заняття, яка дає можливість здобувачам освіти самостійно перевірити правильність виконання завдань та проаналізувати помилки. У разі звернень здобувачів освіти викладач під час заняття, або після нього, надає консультації щодо проблемних ситуацій чи складних питань. Завдання для самоконтролю розміщено на сторінці курсу у СДО (Система дистанційної освіти) ЗВО «Університет Короля Данила».

КРИТЕРІЇ ОЦІНЮВАННЯ

(за 4-бальною шкалою)

Шкала в балах	Оцінка шкали ECTS	Національна шкала
90-100 балів	A	5 (« відмінно»)
83-89 балів	B	4 («дуже добре»)
75-82 бали	C	4 («добре»)
67-74 бали	D	3 («задовільно»)
60-66 балів	E	3 («достатньо»)
35-59 балів	FX	2 («незадовільно»)
0-34 бали	F	2 («неприйнятно»)

При цьому, оцінки повинні відповідати таким критеріям:

«відмінно» – здобувач освіти міцно засвоїв теоретичний матеріал, глибоко і всебічно знає зміст навчальної дисципліни, основні положення наукових першоджерел та рекомендованої літератури, логічно мислить і будує відповідь, вільно використовує набуті теоретичні знання під час аналізу практичного матеріалу, висловлює своє ставлення до тих чи інших проблем, демонструє високий рівень засвоєння практичних навичок;

«дуже добре» – здобувач освіти добре засвоїв теоретичний матеріал, володіє основними аспектами з першоджерел та рекомендованої літератури, аргументовано викладає його;

«добре» – здобувач освіти має практичні навички, висловлює свої міркування з приводу тих чи інших проблем, але припускається певних неточностей і похибок у логіці викладу теоретичного змісту або при аналізі практичного матеріалу;

«задовільно» – здобувач освіти в основному опанував теоретичні знання навчальної дисципліни, орієнтується в першоджерелах та рекомендованій літературі, але непереконливо відповідає, плутає поняття, додаткові питання викликають невпевненість або відсутність стабільних знань;

«достатньо» – здобувач освіти відповідаючи на запитання практичного характеру, виявляє неточності у знаннях, не вміє оцінювати факти та явища, пов’язувати їх із майбутньою діяльністю;

«незадовільно» – здобувач освіти не опанував навчальний матеріал дисципліни, не знає наукових фактів, визначень; майже не орієнтується в першоджерелах та рекомендованій літературі;

«неприйнятно» – здобувач освіти взагалі не орієнтується в першоджерелах та рекомендованій літературі, відсутні наукове мислення, практичні навички не сформовані.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Основи кібербезпеки та управління інформаційними ресурсами»

1. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕМА 1 Вступ до кібербезпеки
1. Кібербезпека та інформаційна безпека. 2. Основні поняття кібербезпеки: активи, загрози, уразливості, ризики. 3. Розвиток кіберзагроз: історичний аспект та сучасні тренди. 4. Нормативне регулювання кібербезпеки. 5. Міжнародні стандарти кібербезпеки: ISO/IEC 27001 (система управління інформаційною безпекою), NIST Cybersecurity Framework. 6. Діяльність CERT-UA.
ТЕМА 2. ІТ активи та їх захист
1. ІТ активи: поняття та види. 2. Дані: персональні дані, корпоративна інформація, державні реєстри. 3. Програмне забезпечення: системи управління базами даних, прикладні програми. 4. Інфраструктура: сервери, мережі, системи зберігання даних. 5. Класифікація ІТ активів за критичністю. 6. Політики управління ІТ активами.
ТЕМА 3. Кіберзагрози та методи атак
1. Визначення кіберзагроз. Класифікація кіберзагроз. 2. Методи атак та їхні характеристики. 3. Атаки із застосуванням штучного інтелекту. 4. Відповідальність і етичні аспекти. 5. Кримінальна відповідальність за правопорушення в сфері використання інформаційних технологій (ст.ст. 361 -363-1 Кримінального кодексу України). 6. Використання кіберзасобів у військових та політичних цілях. Роль етичних хакерів у забезпеченні безпеки..
ТЕМА 4. Інформаційна безпека в організації
1. Захист даних як основа довіри між компанією, клієнтами та партнерами. 2. Типові виклики в організації: людський фактор, невчасне оновлення ПЗ, відсутність чітких процедур і політик. 3. Політики інформаційної безпеки. 4. Управління доступом. 5. Ролі та відповідальності в інформаційній безпеці. 6. Резервне копіювання та відновлення. 7. Регламент реагування на інциденти кібербезпеки. 8. Важливість навчання працівників.

ТЕМА 5. Базові технологічні рішення кібербезпеки

1. Еволюція захисних рішень: від антивірусів до комплексних систем кіберзахисту.
2. Шифрування даних. Типи шифрування. Симетричне шифрування. Асиметричне шифрування.
3. Міжмережеві екрани. Типи міжмережевих екранів.
4. Системи виявлення та запобігання вторгненням (IDS/IPS).
5. Захист кінцевих пристроїв. Антивірусні системи: як працюють та чому важливі
6. Захист хмарних сервісів. Доступ до ресурсів з різних пристроїв і локацій. Захист від атак на API.

ТЕМА 6. Реагування на кіберінциденти

1. Мета реагування на кіберінциденти. Аналіз практичних кейсів вдалого та невдалого реагування.
2. Життєвий цикл кіберінциденту. Етапи реагування на кіберінциденти.
3. Підготовка: створення плану реагування, навчання персоналу, використання інструментів моніторингу.
4. Виявлення: методи ідентифікації інцидентів, приклади ознак інцидентів.
5. Аналіз: оцінка масштабу загрози, визначення впливу на системи та дані.
6. Локалізація: ізоляція уражених систем, запобігання поширенню загрози.
7. Усунення: видалення шкідливого програмного забезпечення, встановлення оновлень безпеки.
8. Відновлення: перевірка систем після очищення, повернення систем до нормального стану.
9. Підсумковий аналіз: висновки з інциденту, внесення змін до планів безпеки.
10. Інструменти моніторингу та аналізу.
11. Взаємодія з CERT та іншими інституціями.

ТЕМА 7. Перспективи кібербезпеки: штучний інтелект і великі дані

1. Передумови автоматизації процесів кібербезпеки.
2. ШІ у кібербезпеці. Використання машинного навчання для аналізу аномалій у трафіку. Поведінкова аналітика. Прогнозування атак.
3. 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.
4. Великі дані: аналітика загроз і прогнозування атак.
5. Crystal – система аналізу блокчейнів віртуальних активів, її використання для розслідування несанкціонованих транзакцій.
6. Баланс між безпекою та приватністю: як уникнути надмірного втручання у приватне життя громадян.
7. Zero Trust: концепція повної недовіри до будь-якої активності у мережі.

ТЕМА 8. Особиста кібер-гігієна: захист у повсякденному житті

1. Що таке особиста кібер-гігієна?
2. Правила безпеки в мережі. Як створити надійний пароль.
3. Фішинг та соціальна інженерія: як розпізнати підроблені листи, повідомлення та сайти. "Червоні прапорці" фішингу.
4. Безпека публічних Wi-Fi мереж.

5. Приватність у соціальних мережах. 6. Захист мобільних пристроїв та домашньої мережі.

Тема 9. Інформаційний портал НПУ, АРМОР
1. Відомчі інформаційні системи та обліки МВС 2. Таємниця приватного життя та розслідування кримінальних правопорушень 3. Імплементація стандартів ЄС щодо автоматизоаної обробки персональних даних у практиці МВС

2.ТЕМАТИЧНИЙ ПЛАН

Назви тем	**Денна форма навчання**			**Заочна форма навчання**		
	Всього	практичні заняття	Самостійна робота	**Всього**	практичні заняття	Самостійна робота
Тема 1. Вступ до кібербезпеки	**12**	4	8	**14**	2	12
Тема 2. ІТ активи та їх захист	**12**	4	8	**12**		12
Тема 3. Кіберзагрози та методи атак	**12**	4	8	**10**		10
Тема 4. Інформаційна безпека в організації	**12**	4	8	**14**	2	12
Тема 5. Базові технологічні рішення кібербезпеки	**12**	4	8	**12**		12
Тема 6. Реагування на кіберінциденти	**12**	4	8	**10**		10
Тема 7. Перспективи кібербезпеки: штучний інтелект і великі дані	**6**	2	4	**8**	2	6
Тема 8. Особиста кібер-гігієна: захист у повсякденному житті	**6**	2	4	**6**		6
Тема 9. Інформаційний портал НПУ, АРМОР	**6**	2	4	**4**		4

Кількість годин на вивчення дисципліни	**90**	**30**	**60**	**90**	**6**	**84**
Підсумковий контроль	**Залік**					
Всього годин	**90**	**30**	**60**	**90**	**6**	**84**

4. ПЛАН ПРАКТИЧНИХ ЗАНЯТЬ

№ заняття	Тема заняття	Кількість годин	
		Денна форма	Заочна форма
1	Тема 1. Вступ до кібербезпеки	4	0
2	Тема 2. ІТ активи та їх захист	4	0
3	Тема 3. Кіберзагрози та методи атак	4	2
4	Тема 4. Інформаційна безпека в організації	4	0
5	Тема 5. Базові технологічні рішення кібербезпеки	4	0
6	Тема 6. Реагування на кіберінциденти	4	2
7	Тема 7. Перспективи кібербезпеки: штучний інтелект і великі дані	2	0
8	Тема 8. Особиста кібер-гігієна: захист у повсякденному житті	2	2
9	Тема 9. Інформаційний портал НПУ, АРМОР	2	0
Всього семінарських занять		**30**	6

5. САМОСТІЙНА РОБОТА

Назва теми	Зміст завдання для самостійної роботи	Денна форма	Заочна форма	Рекомендовані джерела інформації
Тема 1. Вступ до кібербезпеки	1. 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. 2. 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 3. Проаналізуйте інфографіку глобальних ризиків з матеріалів світового економічного форуму	6	12	Основні 1-8, додаткові 2,4,18

	2023 року. Які загрози можна віднести до загроз кібербезпеки. Обґрунтуйте свої бачення. 4. 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	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.	6	12	Основні 1-8, додаткові 1, 5,13
Тема 3. Кіберзагрози та методи атак	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.	6	10	
Тема 4. Інформаційна безпека в організації	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. 2. Запропонувати вдосконалення до політики інформаційної безпеки університету. 3. Наскрізний проєкт ч. 4. На підставі попередніх завдань підготувати чорнову версію	6	12	Основні 1-8, додаткові 7,9,11-19

	політики кібербезпеки Вашого проєкту.			
Тема 5. Базові технологічні рішення кібербезпеки	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..	10	12	Основні 1-8, додаткові 12,14,18
Тема 6. Реагування на кіберінциденти	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. 2. Бажано використовувати: посібник NIST "Computer Security Incident Handling Guide" (SP 800-61); огляд інструментів аналізу інцидентів від CERT-UA. 3. Наскрізний проєкт ч. 6. Деталізуйте розділ реагування на інциденти у розробленій Вами політиці кібербезпеки проєкту	8	10	Основні 1-8, додаткові 10-15
Тема 7. Перспективи кібербезпеки: штучний інтелект і великі дані	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.	8	6	Основні 1-8, додаткові 3,15
Тема 8. Особиста кібер-гігієна: захист у повсякденному житті	1. Перевірити міцність 3-5 своїх паролів за допомогою онлайн-інструментів (наприклад, https://howsecureismypassword.net/ або аналогічних). Обговорити результати: скільки часу знадобиться хакеру, щоб зламати їхні паролі, і чому.	6	6	Основні 1-8, додаткові 5,16

	2. Аналіз реальних прикладів фішингових листів (можна знайти в Інтернеті або заздалегідь підготувати імітацію). Кожен має визначити, які ознаки вказують на те, що це фішинг. 3. Відкрити свої профілі в 2-3 соціальних мережах (наприклад, Facebook, Instagram, LinkedIn) та перевірити налаштування приватності, керуючись чек-листом, який розробили самостійно. Завдання включає пошук та коригування, хто бачить їхні пости, фото, список друзів тощо. 4. Створення плану реагування на кіберінцидент "Особистий". Скласти короткий покроковий план дій на випадок, якщо їхній акаунт у соціальній мережі або електронна пошта буде зламано. План має включати: відключення від публічної мережі, зміну паролів на всіх пов'язаних сервісах, повідомлення друзів, сканування пристроїв на віруси тощо.			
Тема 9. Інформаційний портал НПУ, АРМОР	1. Інформаційне забезпечення розслідування кримінальних правопорушень. 2. Дотримання прав особи на таємницю приватного життя в процесі автоматизованої обробки персональних даних та дистанційної біометричної ідентифікації	4	4	
Всього годин самостійної роботи		60	84	

ПРОГРАМОВІ ВИМОГИ

ДЛЯ ПІДГОТОВКИ ДО ПІДСУМКОВОГО КОНТРОЛЮ

ПИТАННЯ ДЛЯ ПІДГОТОВКИ ДО ЗАЛІКУ З ДИСЦИПЛІНИ «Основи кібербезпеки і управління інформаційними ресурсами»

1. Дайте визначення понять: актив, загроза, вразливість, ризик. Наведіть приклади для кожного.
2. Які основні чинники визначають значення кібербезпеки для держави, бізнесу та громадян?
3. Поясніть відмінність між інформаційною безпекою та кібербезпекою.
4. Опишіть історію та наслідки атаки Morris Worm.
5. Які сучасні кіберзагрози пов’язані з використанням штучного інтелекту?
6. Які існують види IT-активів? Наведіть приклади.
7. За якими критеріями здійснюється класифікація IT-активів за критичністю?
8. Що таке політика управління IT-активами та які її основні елементи?
9. Порівняйте вимоги GDPR та Закону України «Про захист персональних даних».
10. Які ролі виділяють у процесі управління IT-активами?
11. Які основні групи кіберзагроз за джерелами можна виділити?
12. Дайте характеристику атаки DDoS та поясніть механізм її проведення.
13. Що таке SQL-ін’єкція та які наслідки вона може мати?
14. Опишіть сутність програм-вимагачів (ransomware) та приклади їх впливу.
15. Яка кримінальна відповідальність передбачена за правопорушення у сфері використання інформаційних технологій згідно з КК України?
16. Які основні компоненти політики інформаційної безпеки?
17. Опишіть моделі управління доступом: DAC, RBAC, ABAC.
18. Що таке багатофакторна автентифікація (MFA) і які приклади її застосування ви знаєте?
19. У чому полягає політика «3-2-1» у резервному копіюванні?
20. Які ключові ролі й відповідальності існують у сфері інформаційної безпеки організації?
21. У чому різниця між симетричним та асиметричним шифруванням?
22. Для чого використовується SSL/TLS і як перевірити сертифікат сайту?
23. Які завдання виконують системи IDS та IPS? Наведіть приклади.
24. Які особливості захисту хмарних сервісів у контексті кібербезпеки?
25. Які основні можливості надають сучасні антивірусні системи?
26. Опишіть етапи життєвого циклу кіберінциденту.
27. Яку роль відіграють SIEM-системи? Наведіть приклади таких рішень.
28. Які функції виконує CERT-UA у системі кібербезпеки України?
29. У чому полягає відмінність між інструментами «пісочниця» (sandbox) та мережевим аналізатором Wireshark?
30. Які основні уроки організація може винести після завершення інциденту?

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Бурячок В. Л., Киричок Р. В., Складанний П. М. Основи інформаційної та кібернетичної безпеки: навч. посібник. – Київ: Київ. ун-т ім. Б. Грінченка, 2019. – 320 с. URL: : https://elibrary.kubg.edu.ua/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf
2. Бурячок В.Л., Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки, підручник, Київ.; ПВП «Задруга», 2014. - 222 с
3. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібер-оборони: підручник. – 2-ге вид., перероб. і доп. – Одеса: ОНАЗ ім. О. С. Попова, 2019. – 320 с.
4. Інформаційна безпека та кібербезпека держави : навчальний посібник / Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська ; під заг. ред. Н. М. Титова. Київ : Ліра-К, 2024. – 224 с.
5. Лісовська, Ю. П. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2021. – 268 с.
6. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. / [автори: В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін]. Київ : Ліра-К, 2022. - 553 с.
7. Сілін Є.С., Кадубовський О.А. Основи кібербезпеки : навч.посіб. Дніпро, 2023. – 200 с. URL: : https://ddpu.edu.ua/fmk/publications/manuals/manual_18.pdf
8. Технології захисту інформації [Текст] : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король ; під заг. ред. С. Е. Остапова. – Київ : Новий світ-2000, 2020. – 500 с.

Додаткова література

1. Перлрос, Н. Ось таким, як мені кажуть, буде кінець світу: перегони кіберозброєнь [Текст]: [монографія] / Н. Перлрос – Харків : Фоліо, 2024. – 576с.
2. Ромашко, І. Правила з кібербезпеки [Текст] / І. Ромашко // Управління освітою. – 2020. – № 2, лютий. - С. 50-56.
3. Когут, Ю. Кібервійна та безпека об’єктів критичної інфраструктури [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2021. – 332с.
4. Когут, Ю. Кібервійни, кібертероризм, кіберзлочинність. Концепції, стратегії, технології [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2022. – 284с.
5. Когут, Ю. Кібертероризм. Історія, цілі, об’єкти [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2021. – 304с.
6. Когут, Ю. Цифрова трансформація економіки та проблеми кібербезпеки [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2021. – 368с.
7. Когут, Ю. Штучний інтелект і безпека [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2024. – 294с.
8. Ланде, Д. OSINT у кібербезпеці [Текст] : навчальний посібник / Д. Ланде – Київ : ТОВ «Інжиніринг», 2024. – 552с.
9. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ – Київ : Видавництво НА СБ України, 2020. 256 с.
10. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. – Київ: НІСД, 2014. – 328 с.
11. Іванюк, К. Обережність та обачність [Текст] : соціалізація і кіберсоціалізація підлітків як соціально-педагогічне явище / К. Іванюк // Соціальний педагог. – 2020. – № 6, червень. – С. 10-15.

12. Богуш В.М., Довидьков О.А. Проектування захищених комп'ютерних систем та мереж, навчальний посібник, -К.; ДУІКТ, 2008. – 500 с.
13. Бугайчук, А. Кіберсоціалізація [Текст] : життя в новій віртуальній реальності / А. Бугайчук // Управління освітою. – 2020. – № 2, лютий. – С. 24-44.
14. Alam, Shahid. Cybersecurity: Past, Present and Future. – arXiv preprint, 2022. https://arxiv.org/abs/2207.01227
15. Cyber Security. Simply. Make it Happen. : Monograph / edit. Abolhassan. – Springer International Publishing, 2017. – ISBN 978- 3-319-46528-9 (print) ; 978-3-319-46529-6 (online). 127 p.
16. Cyber-Physical Security : Monograph / edit. Clark. – Springer International Publishing, 2017. – ISBN 978-3-319-32822-5 (print) ; 978-3-319-32824-9 (online). 299 p.
17. Enterprise Security : Monograph / edit. Chang. – Springer International Publishing, 2017. – ISBN 978-3-319-54379-6 (print) ; 978-3-319-54380-2 (online). 277 p.
18. Mashima, D., Chen, Y., Roomi, M. M., Lakshminarayana, S., Chen, D. Cybersecurity for Modern Smart Grid against Emerging Threats. – arXiv monograph, 2024. https://arxiv.org/abs/2404.04466
19. Pavlovic, D., Seidel, P.-M. Security Science (SecSci), Basic Concepts and Mathematical Foundations. – Open-access lecture notes/textbook (Oxford, Royal Holloway, Hawaii), 2025. https://arxiv.org/abs/2504.16617v1

Електронні інформаційні ресурси

1. Офіційний веб-сайт Президента України – http://www.president.gov.ua.
2. Офіційний веб-сайт Верховної Ради України – http://www.portal.rada.gov.ua.
3. Офіційний веб-сайт Кабінету Міністрів України – http://www.kmu.gov.ua.
4. Офіційний веб-сайт Міністерства внутрішніх справ України – http://www.mvs.gov.ua.
5. Офіційний веб-сайт Офісу Генерального прокурора – http://www.gp.gov.ua.
6. Офіційний веб-сайт Міністерства юстиції України – http://www.minjust.gov.ua.
7. Єдиний реєстр судових рішень в Україні – http://www.reyestr.court.gov.ua.
8. Національна бібліотека України ім. В. І. Вернадського – http://www.nbuv.gov.ua.
9. Національна парламентська бібліотека України – http://www.catalogue.nplu.org.
10. **Журнал "Кібербезпека"**, аналітичний дайджест — щомісячне видання від НАН України та НБУВ, охоплює актуальні погляди й новини сфери. https://ippi.org.ua/kiberbezpeka-v-informatsiinomu-suspilstvi
11. **CERT-UA**, офіційний сайт Державного центру кібербезпеки України (CERT-UA) — нормативна база, кейси реагування, аналітика. https://cert.gov.ua/
12. **Journal of Cybersecurity** (Oxford University Press) — відкритий академічний журнал із міждисциплінарним підходом до кібербезпеки. https://academic.oup.com/cybersecurity/issue?login=false