ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЮРИДИЧНИЙ ФАКУЛЬТЕТ

ЗАТВЕРДЖУЮ
Декан юридичного факультету
_____ Т.О. Коломоєць
(підпис)
«_____» _____2024

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
КІБЕРБЕЗПЕКА І УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ

підготовки першого (бакалаврського) освітнього ступеня
денної та заочної форм здобуття освіти

освітньо-професійна програма ПРАВООХОРОННА ДІЯЛЬНІСТЬ
спеціальності 262 ПРАВООХОРОННА ДІЯЛЬНІСТЬ
галузі знань 26 ЦИВІЛЬНА БЕЗПЕКА

ВИКЛАДАЧ: Бараннік Роман В'ячеславович, кандидат юридичних наук, доцент, доцент кафедри кримінального права та правоохоронної діяльності

Обговорено та ухвалено
на засіданні кафедри кримінального права
та правоохоронної діяльності

Протокол № 4 від "28" листопада 2024 р.
В.о. завідувача кафедри кримінального
права та правоохоронної діяльності
_____ Роман Бараннік

Погоджено
Гарант освітньо-професійної програми
_____ Г.В. Гнусов
(підпис) (ініціали, прізвище)

2024 рік

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Силабус навчальної дисципліни
Кібербезпека і управління інформаційними ресурсами

Зв`язок з викладачем (викладачами):
Сезн ЗНУ повідомлення: *https://moodle.znu.edu.ua/course/view.php?id=17279*
Телефон: *(061) 228-76-22*
Кафедра: *кафедра кримінального права та правохоронної діяльності, V корпус, ауд.106*

1. **Опис навчальної дисципліни**

Метою вивчення навчальної дисципліни *Кібербезпека і управління інформаційними ресурсами* є виховання фахівця, який:

1. **Розуміє основні принципи захисту інформації**, здатний ідентифікувати сучасні кіберзагрози та застосовувати відповідні заходи для їх нейтралізації.
2. **Орієнтується у сучасних технологіях**, таких як штучний інтелект, блокчейн, Інтернет речей (IoT) та квантові обчислення, і використовує їх для підвищення рівня кібербезпеки.
3. **Має практичні навички впровадження політик безпеки** у корпоративних та державних інформаційних системах.
4. **Здатний аналізувати великі обсяги даних** для виявлення аномалій та загроз у кіберпросторі.
5. **Володіє правовими та етичними аспектами кібербезпеки**, дотримуючись міжнародних стандартів і законодавства.
6. **Може ефективно управляти інформаційними ресурсами**, забезпечуючи їхню конфіденційність, цілісність та доступність у динамічних умовах сучасного інформаційного середовища.
7. **Готовий до роботи в команді** та розробки стратегій захисту інформаційних систем, використовуючи інноваційні технології та методики.

Цей фахівець стане ключовою ланкою у формуванні безпечного цифрового простору в сучасному інформаційному суспільстві.

Основні завдання, які переслідує дисципліна:

Сформувати у студентів необхідні компетенції для роботи в сучасному цифровому світі:

— **Навчити захищати особисті дані та інформацію.** В умовах цифровізації велика кількість персональної інформації зберігається та обробляється у мережі. Знання принципів кібербезпеки допомагає студентам захищати власні дані від: хакерських атак; фішингу; витоків конфіденційної інформації. Розуміння правових аспектів захисту інформації (наприклад, законодавства про захист персональних даних) дозволяє уникати порушень та зловживань.
— **Засвоїти основи безпеки професійної діяльності.** Більшість сучасних професій вимагає роботи з інформаційними ресурсами. Знання основ кібербезпеки дозволяє: ефективно працювати з корпоративними системами; розпізнавати потенційні загрози, пов’язані з цифровими атаками; зменшувати ризики втрати даних через дії третіх осіб чи внутрішні помилки.
— **Навчитися вправно управляти інформаційними ресурсами.** Знання принципів управління інформаційними ресурсами допомагає студентам: оптимізувати зберігання та використання даних; організовувати безпечний доступ до інформації; розробляти стратегії ефективного використання ресурсів у бізнесі чи інших організаціях.
— **Ознайомити з різноманіттям сучасних технологій.** Дисципліна знайомить студентів із основами сучасних технологій: мережевої безпеки; шифрування даних; роботи з хмарними сервісами; використання антивірусного та іншого програмного забезпечення для захисту систем. Розуміння цих технологій є ключовим для адаптації до швидких змін у сфері інформаційних технологій.

— **Провести тренування з попередження кіберзагроз.** Студенти дізнаються про види кіберзагроз: віруси, троянські програми, програми-вимагачі; атаки "відмова у наданні послуги" (DoS/DDoS); соціальна інженерія. Це допомагає їм попереджати такі ризики не лише у професійному середовищі, а й у повсякденному житті.
— **Вивчити етичний та правовий аспекти.** Вивчення правових норм та етичних принципів роботи з інформацією —дотримання авторського права; боротьба з цифровим піратством; відповідальність за розповсюдження шкідливих програм чи конфіденційної інформації — все це допомагає студентам уникати конфліктів із законом та розвивати відповідальність у роботі з цифровими ресурсами.
— **Підготуватися до цифрових викликів майбутнього.** Глобалізація та стрімкий розвиток технологій роблять кібербезпеку однією з ключових компетенцій у багатьох сферах: від права й бізнесу до медицини й освіти. Розуміння основ кібербезпеки дає конкурентну перевагу на ринку праці, адже фахівці, які знають, як управляти інформаційними ресурсами та захищати їх, високо цінуються.

Навчальна дисципліна *"Кібербезпека і управління інформаційними ресурсами"* формує знання, навички та компетенції для захисту інформаційних систем і ефективного управління даними. Вона охоплює сучасні технології, такі як штучний інтелект, блокчейн, Інтернет речей і квантові обчислення, спрямовані на протидію кіберзагрозам. Дисципліна має міждисциплінарний характер, забезпечуючи інтеграцію технічних, правових та управлінських знань.

Паспорт навчальної дисципліни

Нормативні показники	денна форма здобуття освіти	заочна форма здобуття освіти
Статус дисципліни	**Обов'язкова**	
Семестр	2-гий	
Кількість кредитів ECTS	**3**	
Кількість годин	90	
Лекційні заняття	12	4
Лабораторні заняття	12	4
Самостійна робота	66	82
Консультації	*особисті – вівторок, четвер, з 13:00 до 14:00, V корпус, ауд. 106; дистанційні – ZOOM, за попередньою домовленістю. Запис на консультації: Moodle (приватні повідомлення)*	
Вид підсумкового семестрового контролю:	**залік**	
Посилання на електронний курс у СЕЗН ЗНУ (платформа Moodle)	*https://moodle.znu.edu.ua/course/view.php?id=17279*	

2. Методи досягнення запланованих освітньою програмою компетентностей і результатів навчання

***КОМПЕТЕНТНОСТІ* / результати навчання**	**Методи навчання**	**Форми і методи оцінювання**
● Збирати необхідну інформацію з різних джерел, аналізувати і оцінювати її; ● Здійснювати координацію діяльності суб'єктів забезпечення публічної безпеки і порядку, а також комунікацію з фізичними та юридичними особами з метою своєчасного реагування на кримінальні злочини, адміністративні правопорушення та події; ● Здійснювати пошук інформації у доступних джерелах для повного та всебічного встановлення необхідних обставин. ● 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; ● Здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя, підвищення професійної майстерності, вивчення та використання передового досвіду у сфері правоохоронної діяльності; ● Використовувати основні методи та засоби забезпечення правопорядку в державі, дотримуватись прав і свобод людини і громадянина та інших загроз національної безпеки держави (кібербезпеку, економічну та інформаційну безпеку, тощо) ● Застосовувати інформаційні системи, інформаційні технології, технології захисту даних, методи обробки, накопичення та оцінювання інформації, інформаційно аналітичної роботи, бази даних (в тому числі	**Лекційні заняття** **Мета:** Передати базові теоретичні знання, концепції та сучасні тенденції у сфері кібербезпеки. **Особливості:** Використання мультимедійних презентацій; демонстрація реальних кейсів; запрошення фахівців-практиків для обговорення сучасних викликів у сфері кібербезпеки. **Лабораторні роботи** **Мета:** Отримання практичного досвіду роботи з технологіями кіберзахисту. **Приклади завдань:** Налаштування міжмережевих екранів. Створення та перевірка криптографічних алгоритмів. Впровадження механізмів аутентифікації в середовищі Інтернету речей (IoT). **Самостійна робота** **Мета:** Сприяти формуванню здатності до самонавчання і досліджень. **Методи:** Аналіз актуальних наукових статей та матеріалів. Пошук та	Поточний контроль здійснюється систематично на практичних (лабораторних) заняттях для оцінки рівня теоретичних знань та навичок роботи з програмним забезпеченням відповідно до тематики конкретного навчального заняття або пройденого раніше навчального матеріалу в формах: вибіркове усне опитування, фронтальне письмове опитування, тестування, виконання завдань на лабораторних роботах. Проміжний контроль проводиться наприкінці кожного модуля шляхом тестування. Підсумковий контроль проводиться у формі заліку і складається із тестових завдань, у періоди визначені робочим навчальним планом. Під час

міжвідомчі та міжнародні); ● Організовувати заходи щодо режиму секретності та захисту інформації; ● Вміти оцінювати обстановку, рівень потенційних загроз та викликів, прогнозувати розвиток обстановки, дій правопорушників та противника, вживати заходів з метою запобігання, виявлення та припинення правопорушень.	систематизація інформації про новітні технології у сфері кібербезпеки. Виконання проєктів на обрані теми, наприклад, аналіз блокчейн-технологій або прогнозування ризиків у IoT.	заліку оцінюють теоретичні знання, практичні вміння та навички здобувача. При оцінці теоретичної підготовленості перевіряють знання термінології та методології.

3. Зміст навчальної дисципліни

Змістовий модуль 1. Основи кібербезпеки та інформаційної безпеки.

Поняття кібербезпеки та інформаційної безпеки. Основні принципи інформаційної безпеки. Основні характеристики інформаційної безпеки. Основні складові кібербезпеки. Загрози для кібербезпеки. Характеристики кібербезпеки. Ключові відмінності кібербезпеки та інформаційної безпеки.

Історія розвитку кібербезпеки. Ранні етапи (1940-1980-ті роки). Розвиток мереж і перші кіберзагрози (1980-1990-ті роки). Інтернет і зростання кіберзагроз (1990-2000-ті роки). Сучасні виклики та тенденції в кібербезпеці (2010-2020-ті роки). Майбутнє кібербезпеки. Вірус Creeper (1971). Комп'ютерна вірусна атака "Morris Worm" (1988). Створення першого міжмережевого екрану (1980-ті роки). Виникнення криптографії для захисту даних в Інтернеті (1990-ті роки). Атака "ILOVEYOU" (2000 рік). Атака Stuxnet (2010 рік). Розвиток програми "Global Forum on Cybersecurity" (2011 рік). Атака на Sony Pictures (2014 рік).

Класифікація загроз та актуальні загрози кібербезпеки. Кіберзлочинність. Кібершпигунство. Кібервійни. Кібертероризм. Загрози за джерелом походження. Загрози за характером атаки. Загрози за напрямком спрямованості. Віруси та шкідливі програми. Рансомвар (Ransomware). Атаки на Інтернет речей (IoT). Фішинг та соціальна інженерія. APT-атаки (Advanced Persistent Threats). DDoS-атаки (Distributed Denial of Service). Витоки даних і крадіжки персональної інформації. Порушення безпеки хмарних технологій.

Методи протидії загрозам кібербезпеки. Захист від шкідливих програм (вірусів, троянів). Антивірусні та антишкідливі програми. Фільтрація контенту та електронної пошти. Резервне копіювання даних. Методи протидії Ransomware. Програми-вимагачі. Методи протидії атакам на Інтернет речей (IoT). Заходи захисту від фішингу та соціальної інженерії. Захист від DDoS-атак. Захист даних та конфіденційної інформації від витоку. Методи протидії порушення хмарних технологій. Організаційні заходи протидії кіберзагрозам. Розробка політики кібербезпеки. Навчання та підвищення обізнаності співробітників. Розподіл обов'язків і ролей в організації. Аудит і моніторинг кібербезпеки. Регулярне резервне копіювання.

Законодавчі акти та норми в сфері кібербезпеки. Міжнародне співробітництво.

Змістовий модуль 2. Захист інформаційних систем.

Архітектура захисту інформаційних систем. Принцип мінімізації доступу. Розділення обов'язків. Верифікація та автентифікація. Журналювання. Моніторинг. Доступність. Відмова від довіри. Глибока оборонна тактика. Принцип багаторівневого захисту. Основні методи архітектури захисту.

Засоби технічного захисту інформації. Апаратні засоби технічного захисту інформації. Системи контролю доступу. Електронні замки. Біометричні сканери. Турнікети та автоматичні двері. Апаратні модулі безпеки. Генерація криптографічних ключів. Захист ключів від несанкціонованого доступу. Виконання операцій шифрування, дешифрування та підпису. Екрановані кімнати та сейфи. Сканування обличчя. Аутентифікація за допомогою голосу. Системи виявлення та запобігання вторгненням. Віртуальні приватні мережі (VPN). Міжмережеві екрани (файрволи). Аутентифікація та контроль доступу. Шифрування даних та управління ключами. Симетричне шифрування. Асиметричне шифрування. Антивірусні рішення та захист від шкідливих програм. Системи аналізу поведінки. Хмарні антивірусні сервіси. Засоби резервного копіювання та відновлення. Системи моніторингу та управління журналами. Системи виявлення та запобігання вторгненням. Системи управління інформаційною безпекою. Системи запобігання витокам інформації.

Основні цілі шифрування. Методи шифрування. Симетричне шифрування. Алгоритми симетричного шифрування. Алгоритми асиметричного шифрування. Гібридні системи. Генерація ключів. Зберігання ключів. Розподіл ключів. Ротація та оновлення ключів.

Засоби захисту від витоків інформації. Системи запобігання витокам (DLP). Шифрування даних. Аутентифікація та контроль доступу. Моніторинг і аналіз активності користувачів. Політики безпеки.

Системи виявлення вторгнень в інформаційні системи. Природа загроз та роль IDS. Основні типи систем виявлення вторгнень. Мережеві системи. Хостові системи. Системи виявлення на основі сигнатур. Системи виявлення на основі аномалій. Роль сучасних технологій у розвитку IDS.

Захист мереж. Значення захисту мереж. Атаки на основі штучного інтелекту (AI). Фішинг та соціальна інженерія. DDoS-атаки (Distributed Denial of Service). Зловмисне програмне забезпечення (Malware). Основні елементи мережевого захисту. Брандмауери (Firewall). VPN (віртуальні приватні мережі). Аутентифікація і контроль доступу. Стратегії ефективного захисту інформаційних мереж. Аудит і аналіз ризиків. Використання багатофакторної автентифікації (MFA). Навчання персоналу. Використання сегментації мережі. Регулярне оновлення програмного забезпечення.

Змістовий модуль 3. Управління доступом до інформації.

Поняття доступу до інформаційних ресурсів. Рівні доступу до інформаційних ресурсів. Вільний доступ. Обмежений доступ. Конфіденційна інформація. Спеціалізований доступ. Таємна інформація. Службова інформація. Нормативно-правові аспекти доступу до інформаційних ресурсів.

Системи управління доступом (СУД). Аутентифікація. Авторизація. Моніторинг та аудит. Адміністрування. Мандатні системи управління доступом. Рольові системи управління доступом. Атрибутивні системи управління доступом. Архітектура систем управління доступом. Моделі контролю доступу Модель Bell-LaPadula. Модель Biba.

Аутентифікація та її основні принципи. Типи аутентифікації. Процес аутентифікації. Однофакторна аутентифікація (1FA). Двофакторна аутентифікація (2FA). Багатофакторна аутентифікація (MFA). Інтернет-банкінг. Корпоративні мережі. Соціальні мережі. Авторизація. Як працює авторизація? Основні моделі авторизації. Обов'язковий контроль доступу. Атрибутний контроль доступу. Основні характеристики авторизації. Облік.

Моніторинг. Основні характеристики моніторингу. Приклади використання моніторингу. Технології моніторингу. Аудит. Основні характеристики аудиту. Приклади використання аудиту. Ключові аспекти аудиту. Технологічні інструменти для моніторингу та аудиту. Адміністрування в системі управління доступом. Основні функції адміністрування. Управління ролями та правами доступу. Забезпечення політик доступу та безпеки. Обробка запитів на доступ та управління ролями. Підтримка політики безпеки та реагування на інциденти. Характеристики адміністрування. Приклади адміністрування.

Роль людського фактору в забезпеченні інформаційної безпеки. Помилки персоналу. Фішинг та соціальна інженерія. Неналежне управління паролями. Соціальне маніпулювання. Захист від соціальної інженерії. Ефективне навчання персоналу. Культура безпеки в організаціях.

Змістовий модуль 4. Захист даних.

Юридичні та нормативні вимоги. Потенційна шкода у разі розголошення або втрати. Публічні дані. Внутрішні дані. Конфіденційні дані. Критично конфіденційні дані. Юридичне регулювання захисту даних. Конфіденційність в українському законодавстві. Відкрита інформація. Конфіденційна інформація. Таємна інформація. Службова інформація. Ідентифікація даних. Оцінка ризиків або аналіз чутливості. Встановлення категорій. Впровадження політик.

Методи шифрування даних. Історія шифрування. Класифікація методів шифрування. Симетричне шифрування. Блокове шифрування. Потокове шифрування. Дешифрування. Асиметричне шифрування. Алгоритм RSA. Основні алгоритми асиметричного шифрування. Гібридні методи шифрування. Використання методів шифрування у різних сферах. Електронна комерція. Захист персональних даних .Військова та державна безпека.

Захист даних у хмарних сховищах. Особливості хмарних середовищ. Зовнішній

доступ і контроль. Мульти-орендність. Розподілені ресурси. Типи загроз для даних у хмарних сховищах. Несанкціонований доступ. Атаки “людина посередині”. Втрата даних. Внутрішні загрози. Методи захисту даних у хмарних сховищах. GDPR (General Data Protection Regulation). HIPAA (Health Insurance Portability and Accountability Act). PCI DSS (Payment Card Industry Data Security Standard). Управління ключами в хмарах. Методи та підходи до управління ключами в хмарах. Key Management Services (KMS). Керування доступом до ключів. Ротація ключів. Шифрування в процесі. Інтеграція між платформами. Забезпечення зворотного доступу.

Захист персональних даних. Поняття персональних даних. Нормативно-правове забезпечення захисту персональних даних. Принципи захисту персональних даних. Технічні засоби захисту персональних даних. Права суб’єктів персональних даних. Ризики та виклики у сфері захисту персональних даних.

Змістовий модуль 5. Відновлення після інцидентів кібербезпеки.

Планування відновлення після інцидентів. Кіберінциденти. Наслідки інцидентів. Фінансові втрати. Репутаційні ризики. Юридичні наслідки. Операційні збої. Етапи планування відновлення. Аналіз ризиків і впливу. Розробка плану реагування. Вибір та впровадження стратегій відновлення. Комунікація. Підсумковий аналіз (Post-Incident Review). Принципи ефективного планування. Інтеграція з бізнес-процесами.

Процес реагування на інциденти кібербезпеки. Ідентифікація інциденту. Стримування загрози. Аналіз і виявлення першопричини. Відновлення систем. Підсумковий аналіз і навчання. Постійне тестування. Залучення зовнішніх експертів. Підвищення рівня обізнаності персоналу. Готовність альтернативної інфраструктури. Можливість швидкого відновлення даних. Чіткий порядок дій для команди.

Тестування планів відновлення. Види тестування планів відновлення. Настільні вправи (tabletop exercises). Симуляції (simulation testing). Пенетраційне тестування (penetration testing). Тестування резервного відновлення (випробування резервних копій). Зниження ризиків. Підвищення ефективності команд. Покращення репутації.

Страхування кіберризиків. Кіберризики. Реальні приклади використання страхування кіберризиків. Витік даних. Перерва в роботі. Вимога викупу. Основні компоненти страхування кіберризиків. Покриття втрат, пов’язаних із кіберінцидентами. Компенсація збитків клієнтам. Юридичні витрати та штрафи. Покриття втрат через простої бізнесу. Переваги страхування кіберризиків.

Довіра клієнтів і партнерів. Фінансова захищеність. Покращення управління кібербезпекою. Висока вартість страхування. Зростаюча кількість кібератак. Обмеження покриття. Як правильно вибрати кіберстрахування? Співпраця зі страховиком.

Змістовий модуль 6. Сучасні тенденції в кібербезпеці.

Штучний інтелект у кібербезпеці: нові горизонти та виклики. Класичні методи

захисту. Виявлення аномалій. Автоматизація відповіді на інциденти. Прогнозування загроз. Проблема помилкових спрацьовувань. Етичні та правові аспекти. Використання ШІ зловмисниками. Створення самонавчальних систем. Інтеграція ШІ з технологіями блокчейну. Співпраця між країнами.

Блокчейн і кібербезпека: нові межі цифрової безпеки. Ключові характеристики блокчейна. Децентралізація. Незмінність. Прозорість. Децентралізація як основа безпеки. Незмінність та прозорість даних. Анонімність та захист приватності. Виклики впровадження блокчейну в кібербезпеку. Висока вартість і складність. Загроза 51%-ї атаки. Проблеми масштабованості. Юридичні та етичні аспекти. Реальні кейси: успіхи і виклики. Майбутнє блокчейну у кібербезпеці. Смартконтракти як основа безпеки. Інтеграція з ШІ Глобальні стандарти.

Інтернет речей і кібербезпека. Уразливості систем IoT. Причини вразливостей IoT. Стандартні паролі та їх використання. Відсутність оновлень програмного забезпечення. Низький рівень шифрування. Велика кількість точок доступу. Як захистити IoT-пристрої? Використання унікальних паролів. Регулярні оновлення програмного забезпечення. Шифрування даних. Обмеження доступу.

Квантові обчислення і кібербезпека. Що таке квантові обчислення? Квантовий комп’ютер. Квантові обчислення проти сучасної криптографії. Злам банківських систем. Компрометація державних таємниць. Втрата конфіденційності у комунікаціях. Квантова криптографія. Постквантова криптографія. Кодові криптосистеми. Стандартизація нових алгоритмів. Освіта та підготовка спеціалістів.

4. Структура навчальної дисципліни

Вид заняття /роботи	**Назва теми**	**Кількість годин**		**Згідно з розкладом**
		о/д.ф.	**з.ф.**	
Лекція 1	**Основи кібербезпеки та інформаційної безпеки:** 1. Поняття кібербезпеки та інформаційної безпеки. 2. Історія розвитку кібербезпеки. 3. Класифікація загроз та актуальні загрози кібербезпеки. 4. Методи протидії загрозам кібербезпеки. 5. Законодавство в галузі кібербезпеки.	2	2	*тиждень 1*
Лабораторна робота 1	**Основи кібербезпеки та інформаційної безпеки:** 1. Ознайомлення з основними поняттями та принципами кібербезпеки та інформаційної безпеки. 2. Набуття практичних навичок з використання інструментів для забезпечення безпеки інформаційних систем. 3. Розробка простих стратегій захисту від типових кіберзагроз.	2	—	*тиждень 1*

Самостійна робота	**Основи кібербезпеки та інформаційної безпеки:** Завдання для самостійної роботи розміщені на сторінці дисципліни за посиланням: *https://moodle.znu.edu.ua/course/view.php?id=17279*	11	14	*тиждень 1, 2*
Лекція 2	**Захист інформаційних систем:** 1. Архітектура захисту інформаційних систем. 2. Засоби технічного захисту інформації (ЗТЗІ). 3. Методи шифрування та управління ключами. 4. Засоби захисту від витоків інформації. 5. Системи виявлення вторгнень (СВВ). 6. Захист мереж як складова архітектури захисту інформаційних систем.	2	—	*тиждень 2*
Лабораторна робота 2	**Захист інформаційних систем:** 1. Аналіз вразливостей системи. 2. Налаштування системи виявлення вторгнень. 3. Налаштування системи запобігання вторгнень. 4. Конфігурування міжмережевого екрану. 5. Створення надійних паролів та управління доступом. 6. Шифрування даних. 7. Аналіз логів системи.	2	2	*тиждень 2*
Самостійна робота	**Захист інформаційних систем**. Завдання для самостійної роботи розміщені на сторінці дисципліни за посиланням: *https://moodle.znu.edu.ua/course/view.php?id=17279*	11	14	*тиждень 2, 3*
Лекція 3	**Управління доступом до інформації:** 1. Поняття доступу до інформаційних ресурсів та його рівні. 2. Системи управління доступом (СУД). 3. Аутентифікація, авторизація та облік в СУД. 4. Моніторинг, аудит та адміністрування в СУД. 5. Роль людського фактору в забезпеченні інформаційної безпеки.	2	2	*тиждень 3*
Лабораторна робота 3	**Управління доступом до інформації:** 1. Ознайомлення з основними методами і технологіями управління доступом до інформації. 2. Налаштування доступу в ОС Windows/Linux. 3. Використання рольової моделі доступу (RBAC). 4. Аудит доступу. 5. Моделювання політики доступу за допомогою ABAC.	2	—	*тиждень 3*
Самостійна робота	**Управління доступом до інформації**. Завдання для самостійної роботи розміщені на сторінці дисципліни за посиланням: *https://moodle.znu.edu.ua/course/view.php?id=17279*	11	14	*тиждень 3, 4*
Лекція 4	**Захист даних:** 1. Класифікація даних за рівнем конфіденційності. 2. Методи шифрування даних.	2	—	*тиждень 4*

	3. Захист даних у хмарних сховищах. 4. Захист персональних даних.			
Лабораторна робота 4	**Захист даних:** 1. Основи шифрування даних. 2. Захист передавання даних за допомогою SSL/TLS. 3. Управління доступом до даних. 4. Аналіз та усунення вразливостей.	2	2	*тиждень 4*
Самостійна робота	**Захист даних**. Завдання для самостійної роботи розміщені на сторінці дисципліни за посиланням: *https://moodle.znu.edu.ua/course/view.php?id=17279*	11	14	*пиждень 4, 5*
Лекція 5	**Відновлення після інцидентів кібербезпеки:** 1. Планування відновлення після інцидентів. 2. Процес реагування на інциденти кібербезпеки. 3. Тестування планів відновлення. 4. Страхування кіберризиків.	2	—	*Тиждень 5*
Лабораторна робота 5	**Відновлення після інцидентів кібербезпеки:** 1. Аналіз інциденту кібербезпеки 2. Усунення наслідків кіберінциденту 3. Відновлення після атаки типу Ransomware 4. Розробка політики відновлення та тестування 5. Постінцидентний аналіз та внесення змін до систем безпеки	2	—	*тиждень 5*
Самостійна робота	**Відновлення після інцидентів кібербезпеки**. Завдання для самостійної роботи розміщені на сторінці дисципліни за посиланням: *https://moodle.znu.edu.ua/course/view.php?id=17279*	11	14	*тиждень 5, 6*
Лекція 6	**Сучасні тенденції в кібербезпеці:** 1. Штучний інтелект в кібербезпеці: нові горизонти та виклики. 2. Блокчейн і кібербезпека: нові межі цифрової безпеки. 3. Інтернет речей і кібербезпека. 4. Квантові обчислення і кібербезпека.	2	—	*тиждень 6*
Лабораторна робота 6	**Сучасні тенденції в кібербезпеці:** 1. Дослідження ролі штучного інтелекту (ШІ) у виявленні та запобіганні кіберзагрозам. 2. Дослідження можливості використання блокчейн-технологій для захисту даних. 3. Аналіз загроз та методів їх запобігання у середовищі IoT. 4. Дослідження перспектив та ризиків впровадження квантових обчислень у галузі кібербезпеки.	2	—	*тиждень 6*
Самостійна робота	**Сучасні тенденції в кібербезпеці**. Завдання для самостійної роботи розміщені на сторінці дисципліни за посиланням: *https://moodle.znu.edu.ua/course/view.php?id=17279*	11	12	*тиждень 6, 7*

5. Види і зміст контрольних заходів

Вид заняття/роботи	Вид поточного контрольного заходу	Зміст контрольного заходу*	Критерії оцінювання та термін виконання*	Усього балів
1	2	3	4	5
Поточний контроль				
Лабораторна робота № 1	Складання звіту про виконання лабораторної роботи	Відповіді на теоретичні запитання та їх обґрунтування. Виконання практичних завдань, що підтверджується скріншотами екрану. Звіт прикріплюється у форматі PDF на сторінці дисципліни в Moodle	Правильна відповідь на кожне запитання викладача оцінюється в 1 бал	**7**
Самостійна робота	Тестування за підсумками першого модулю	Відповіді на тестові завдання оформлюються на сторінці дисципліни “КБіУІР” СЕЗН Moodle *https://moodle.znu.edu.ua/course/view.php?id=17279*	Правильна відповідь на кожне запитання викладача оцінюється в 0,2 бали	**2**
Лабораторна робота № 2	Складання звіту про виконання лабораторної роботи	Відповіді на теоретичні запитання та їх обґрунтування. Виконання практичних завдань, що підтверджується скріншотами екрану. Звіт прикріплюється у форматі PDF на сторінці дисципліни в Moodle	Правильна відповідь на кожне запитання викладача оцінюється в 1 бал	**8**
Самостійна робота	Тестування за підсумками першого модулю	Відповіді на тестові завдання оформлюються на сторінці дисципліни “КБіУІР” СЕЗН Moodle *https://moodle.znu.edu.ua/course/view.php?id=17279*	Правильна відповідь на кожне запитання викладача оцінюється в 0,2 бали	**2**
Лабораторна робота № 3	Складання звіту про виконання лабораторної роботи	Відповіді на теоретичні запитання та їх обґрунтування. Виконання практичних завдань, що підтверджується скріншотами екрану. Звіт прикріплюється у форматі PDF на сторінці дисципліни в Moodle	Правильна відповідь на кожне запитання викладача оцінюється в 1 бал	**8**
Самостійна робота	Тестування за підсумками першого модулю	Відповіді на тестові завдання оформлюються на сторінці дисципліни “КБіУІР” СЕЗН Moodle *https://moodle.znu.edu.ua/course/view.php?id=17279*	Правильна відповідь на кожне запитання викладача оцінюється в 0,2 бали	**2**
Лабораторна робота № 4	Складання звіту про виконання лабораторної роботи	Відповіді на теоретичні запитання та їх обґрунтування. Виконання практичних завдань, що підтверджується скріншотами екрану. Звіт прикріплюється у форматі PDF на сторінці дисципліни в Moodle	Правильна відповідь на кожне запитання викладача оцінюється в 1 бал	**8**
Самостійна робота	Тестування за підсумками першого модулю	Відповіді на тестові завдання оформлюються на сторінці дисципліни “КБіУІР” СЕЗН Moodle	Правильна відповідь на кожне запитання викладача оцінюється в 0,2 бали	**3**

		https://moodle.znu.edu.ua/course/view.php?id=17279		
Лабораторна робота № 5	Складання звіту про виконання лабораторної роботи	Відповіді на теоретичні запитання та їх обґрунтування. Виконання практичних завдань, що підтверджується скріншотами екрану. Звіт прикріплюється у форматі PDF на сторінці дисципліни в Moodle	Правильна відповідь на кожне запитання викладача оцінюється в 1 бал	**8**
Самостійна робота	Тестування за підсумками першого модулю	Відповіді на тестові завдання оформлюються на сторінці дисципліни “КБіУІР” СЕЗН Moodle *https://moodle.znu.edu.ua/course/view.php?id=17279*	Правильна відповідь на кожне запитання викладача оцінюється в 0,2 бали	**2**
Лабораторна робота № 6	Складання звіту про виконання лабораторної роботи	Відповіді на теоретичні запитання та їх обґрунтування. Виконання практичних завдань, що підтверджується скріншотами екрану. Звіт прикріплюється у форматі PDF на сторінці дисципліни в Moodle	Правильна відповідь на кожне запитання викладача оцінюється в 1 бал	**7**
Самостійна робота	Тестування за підсумками першого модулю	Відповіді на тестові завдання оформлюються на сторінці дисципліни “КБіУІР” СЕЗН Moodle *https://moodle.znu.edu.ua/course/view.php?id=17279*	Правильна відповідь на кожне запитання викладача оцінюється в 0,2 бали	**3**
Усього поточний контроль	**12**			**60**
Підсумковий контроль				
Залік /Екзамен	Тестування за підсумками вивчення курсу	Тестування в СЕЗН Moodle за навчальними матеріалами до всіх тем курсу.	Кількість тестових питань — 60. Правильна відповідь на кожне запитання оцінюється у 0,5 бала.	**30**
	Теоретичне завдання передбачає усну відповідь на запитання викладача	Здобувач ґрунтовно викладає відповідь, висловлює власну позицію й переконливо її аргументує; уміє узагальнити вивчений матеріал, використовує набуті знання.	Враховується правильність, точність і повнота відповіді.	**10**
Усього підсумковий контроль				**40**

Шкала оцінювання ЗНУ: національна та ECTS

За шкалою ECTS	*За шкалою університету*	*За національною шкалою*	
		Екзамен	*Залік*
A	90 – 100 (відмінно)	5 (відмінно)	Зараховано
B	85 – 89 (дуже добре)	4 (добре)	
C	75 – 84 (добре)		
D	70 – 74 (задовільно)	3 (задовільно)	

E	60 – 69 (достатньо)		
FX	35 – 59 (незадовільно – з можливістю повторного складання)	2 (незадовільно)	Не зараховано
F	1 – 34 (незадовільно – з обов'язковим повторним курсом)		

6. Основні навчальні ресурси

Рекомендована література

Основна:

1. Білецький О. О., Черненко І. В. Основи кібербезпеки: теорія та практика. Київ: Кондор, 2021.
2. Бойко В. М., Гусак Я. П., Чопик С. В. Захист інформації в комп'ютерних системах та мережах: Львівська політехніка, 2019.
3. Бурячок А. Ю., Матюхін Ю. В. Методи та засоби інформаційної безпеки. Одеса: ОНПУ, 2018.
4. Глушко О. П., Семенченко О. А. Блокчейн-технології: принципи роботи та безпека. Київ: Наукова думка, 2021.
5. Захарченко В. І., Сидоренко Ю. В., Івженко О. В. Основи кібербезпеки: навчальний посібник. Харків: ХНУРЕ, 2021.
6. Калюжний Р. А., Поліщук В. М., Патрушева Н. С. Кібербезпека: правові аспекти. Київ: Центр учбової літератури, 2020.
7. Касич А. О., Клименко О. М. Кібербезпека та захист інформації: навчальний посібник: НАУ, Київ, 2020.
8. Коваленко Т. О. Інформаційне право України: підручник. Київ: Алерта, 2019.
9. Ковальчук І. М., Ніколенко С. М. Кіберзахист Інтернету речей. Харків: Ранок, 2020.
10. Кудрявцев С. П. Методи і засоби захисту інформації в комп'ютерних мережах: Харківський національний університет радіоелектроніки, 2019.
11. Лаврик В. І., Савченко А. С. Правовий режим інформації: підручник. Київ: Юрінком Інтер, 2020.
12. Лисенко І. В. Основи кібербезпеки: навчальний посібник: СумДУ, 2021.
13. Мартиненко А. В. Квантова криптографія та кібербезпека. Одеса: Пальміра, 2023.
14. Морозов М. О., Василенко І. В. Кіберінциденти: технічний і правовий аналіз. Київ: Вид-во "Наукова думка", 2019.
15. Романенко С. О. Технології забезпечення інформаційної безпеки. Львів: Видавництво ЛНУ, 2020.
16. Сидоренко Є. О., Горлачук В. В. Інформаційна безпека: сучасні аспекти: Техніка, Київ, 2018.
17. Станік В. Д. Інформаційна безпека: підручник. Харків: Право, 2021.
18. Шевчук А. В., Іваненко П. С. Штучний інтелект та інформаційна безпека. Львів: Магнолія, 2022.

Додаткова:

1. Воробйов В. А. Застосування штучного інтелекту для моніторингу кіберзагроз у корпоративних мережах // Інформаційна безпека, 2022, №3, С. 45–55.
2. Головко О. А. Практика захисту інформації в Україні: проблеми та перспективи. Харків: Право, 2022.
3. Гончарук Т. М. Інтернет речей та безпека: новітні виклики для кіберпростору // Телекомунікації та інформаційні технології, 2021, №4, С. 56–68.

4. Данилюк М. І., Ковальчук С. О. Постінцидентний аналіз: методи та інструменти // Вісник НТУУ “КПІ”, 2020.
5. Журавльов Д. А., Семененко С. А. Підходи до аналізу кіберінцидентів та розробка політик відновлення // Інформаційні технології та кібербезпека, 2022.
6. Ковальчук І. В. Кіберзагрози та інформаційна безпека: виклики сьогодення // Юридична Україна. 2022. №3. С. 15-22.
7. Ковальчук І. В. Проблеми обмеження доступу до інформації: теоретичний аспект // Юридична Україна. 2022. №3. С. 17-22.
8. Ковальчук В. С., Чернов А. І. Відновлення після Ransomware-атак: аналіз методів та інструментів // Безпека інформації, 2021.
9. Литвиненко І. С. Перспективи розвитку квантових обчислень в Україні // Кібернетика та системний аналіз, 2022, №1, С. 20–30.
10. Петренко Д. О. Блокчейн як засіб забезпечення конфіденційності інформації в кіберпросторі // Вісник НТУУ “КПІ”, 2021, №2, С. 78–89.
11. Пономаренко І. М. Роль резервного копіювання у процесі відновлення після інцидентів // Комп’ютерні системи та мережі, 2020.
12. Романенко О. А. Використання протоколів SSL/TLS для захисту передачі даних // Комп’ютерні системи та мережі, 2020.
13. Семенов А. В. Автоматизація процесів реагування на кіберінциденти в організаціях // Сучасні інформаційні технології, 2019.
14. Тарасенко А. О., Ковальчук В. А. Шифрування даних: сучасні підходи та алгоритми // Інформаційні технології та захист інформації, 2021.
15. Шевченко І. Ю. Проблеми та перспективи забезпечення кібербезпеки в Україні // Збірник конференцій з кібербезпеки, 2022.
16. Шевчук С. А. Доступ до публічної інформації: правове регулювання. Київ: Науковий світ, 2018.

Нормативно-правові акти України

1. Закон України “Про доступ до публічної інформації”.
2. Закон України “Про захист персональних даних”.
3. Закон України “Про інформацію”.
4. Закон України “Про основні засади забезпечення кібербезпеки України”.
5. ДСТУ ISO/IEC 27001:2015 “Інформаційні технології. Методи управління інформаційною безпекою”. Київ: ДП “УкрНДНЦ”.
6. ДСТУ ISO/IEC 27035:2020 “Інформаційні технології. Управління інцидентами інформаційної безпеки”. Київ: ДП “УкрНДНЦ”.

7. Методичні рекомендації з кібербезпеки для державних установ України. Держспецзв’язок, 2021.
8. Національна стратегія кібербезпеки України (2021–2025).

Міжнародні стандарти та рекомендації

1. COBIT 2019 Framework. Governance and Management of Enterprise IT.
2. ISO/IEC 27001:2022 Information security management systems.
3. NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations.
4. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, GDPR).

Інформаційні ресурси

1. Державний центр кіберзахисту України (ДЦКЗ) *https://cip.gov.ua*
2. Національний координаційний центр кібербезпеки (НКЦК) *https://ncscc.gov.ua*
3. Кіберполіція України https://cyberpolice.gov.ua
4. Національний координаційний центр кібербезпеки https://ncscc.gov.ua
5. Українська асоціація штучного інтелекту (УАШІ) https://uai.org.ua

7. Регуляції і політики курсу

Відвідування занять. Регуляція пропусків.

- ✓ Відвідування усіх занять є обов'язковим, в тому чисті тих, які проводяться у дистанційній, асинхронній формі. Якщо здобувач навчається асинхронно, призначається час консультацій, відвідування яких є обов'язковим;
- ✓ активність студента під час практичних занять;
- ✓ своєчасне виконання завдань самостійної роботи;
- ✓ наявність нормативного матеріалу (допускається будь-яка форма – на паперовому, електронному носії). З цією метою дозволяється обмежене використання мобільним телефоном, планшетом чи іншими мобільними пристроями під час практичного заняття;
- ✓ відпрацювання занять, що були пропущені або не підготовлені з поважних причин відбувається шляхом самостійного вивчення матеріалу та підготовки конспекту з теми пропущеного заняття або не підготовленого заняття;
- ✓ особиста присутність здобувача освіти на заліку, екзамені є обов'язковою, незалежно від форми навчання. Якщо залік, екзамен відбувається дистанційно, або асинхронно з використанням платформи ZOOM особиста присутність здобувача також є обов'язковою.

Не допускається:

- ✓ пропуск занять без поважних причин;
- ✓ запізнення на заняття;
- ✓ користування телефонами для спілкування під час лекційних та практичних занять;
- ✓ списування та академічна недоброчесність**.**

Політика академічної доброчесності

Відповідно до Закону України "Про освіту" академічна доброчесність — це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, складання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень. Дотримання академічної доброчесності передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; дотримання норм законодавства про авторське право і суміжні права; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Прослуховуючи цей курс, здобувачі погоджуються виконувати вимоги принципів академічної доброчесності:

- ✓ вирішувати завдання самостійно, не використовуючи допомогу сторонніх осіб;
- ✓ надавати для оцінювання лише ті результати роботи, які отримані здобувачем самостійно;
- ✓ не вдаватися до кроків, що можуть у нечесний спосіб покращити власні результати навчання чи погіршити (покращити) результати інших здобувачів ступеня вищої освіти;
- ✓ ***категорично забороняється*** публікувати або іншими способом розповсюджувати відповіді на питання, що ставляться в рамках дисципліни, в тому числі відповіді на тестові питання, які містяться на платформі Moodle.
- ✓ роботи здобувачів мають містити результати їх оригінальних досліджень, роздумів, міркувань. Якщо у роботі здобувача використовуються міркування інших осіб, робота повинна містити посилання на джерело інформації. Відсутність таких посилань, фальсифікація джерел, списування, тощо є проявами академічної не доброчесності, та є підставою для її незарахуванння викладачем, незалежно від обсягу плагіату чи обману.

Жодні зазначені форми порушення академічної доброчесності не толеруються.

Використання комп'ютерів/телефонів на занятті
Використання мобільних телефонів, планшетів та інших гаджетів під час занять дозволяється виключно у навчальних цілях.
Під час виконання заходів контролю використання гаджетів заборонено. У разі порушення цієї заборони роботу буде анульовано без права перескладання.

Комунікація
Основною платформою для комунікації викладача зі здобувачами є Moodle.
Важливі повідомлення регулярно розміщуються викладачем на форумі курсу.
Для персональних запитів використовується сервіс приватних повідомлень.

ДОДАТКОВА ІНФОРМАЦІЯ

ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ 2024-2025 н. р. доступний за адресою:
https://tinyurl.com/yckze4jd

НАВЧАЛЬНИЙ ПРОЦЕС ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТИ. Перевірка набутих студентами знань, навичок та вмінь (атестації, заліки, іспити та інші форми контролю) є невід'ємною складовою системи забезпечення якості освіти і проводиться відповідно до Положення про організацію та методику проведення поточного та підсумкового семестрового контролю навчання студентів ЗНУ: https://tinyurl.com/y9tve4lk

ПОВТОРНЕ ВИВЧЕННЯ ДИСЦИПЛІН, ВІДРАХУВАННЯ. Наявність академічної заборгованості до 6 навчальних дисциплін (в тому числі проходження практики чи виконання курсової роботи) за результатами однієї екзаменаційної сесії є підставою для надання студенту права на повторне вивчення зазначених навчальних дисциплін. Порядок повторного вивчення визначається Положенням про порядок повторного вивчення навчальних дисциплін та повторного навчання у ЗНУ: https://tinyurl.com/y9pkmmp5. Підстави та процедури відрахування студентів, у тому числі за невиконання навчального плану, регламентуються Положенням про порядок переведення, відрахування та поновлення студентів у ЗНУ: https://tinyurl.com/ycds57la

ВИРІШЕННЯ КОНФЛІКТІВ. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, регламентуються Положенням про порядок і процедури вирішення конфліктних ситуацій

у ЗНУ: https://tinyurl.com/57wha734. Конфліктні ситуації, що виникають у сфері стипендіального забезпечення здобувачів вищої освіти, вирішуються стипендіальними комісіями факультетів, коледжів та університету в межах їх повноважень, відповідно до: Положення про порядок призначення і виплати академічних стипендій у ЗНУ: https://tinyurl.com/yd6bq6p9; Положення про призначення та виплату соціальних стипендій у ЗНУ: https://tinyurl.com/y9r5dpwh

ПСИХОЛОГІЧНА ДОПОМОГА. Телефон довіри практичного психолога **Марті Ірини Вадимівни** (061) 228-15-84, (099) 253-78-73 (щоденно з 9 до 21).

УПОВНОВАЖЕНА ОСОБА З ПИТАНЬ ЗАПОБІГАННЯ ТА ВИЯВЛЕННЯ КОРУПЦІЇ
Запорізького національного університету: **Банах Віктор Аркадійович**
Електронна адреса: v_banakh@znu.edu.ua
Гаряча лінія: тел. (061) 227-12-76, факс 227-12-88

РІВНІ МОЖЛИВОСТІ ТА ІНКЛЮЗИВНЕ ОСВІТНЄ СЕРЕДОВИЩЕ. Центральні входи усіх навчальних корпусів ЗНУ обладнані пандусами для забезпечення доступу осіб з інвалідністю та інших маломобільних груп населення. Допомога для здійснення входу у разі потреби надається черговими охоронцями навчальних корпусів. Якщо вам потрібна спеціалізована допомога, будь ласка, зателефонуйте (061) 228-75-11 (начальник охорони). Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення у ЗНУ:
https://tinyurl.com/ydhcsagx

РЕСУРСИ ДЛЯ НАВЧАННЯ

НАУКОВА БІБЛІОТЕКА:
http://library.znu.edu.ua
Графік роботи абонементів: понеділок-п`ятниця з 08.00 до 16.00; вихідні дні: субота і неділя.

СИСТЕМА ЕЛЕКТРОННОГО **ЗАБЕЗПЕЧЕННЯ НАВЧАННЯ (MOODLE):**
https://moodle.znu.edu.ua
Якщо забули пароль/логін, направте листа з темою «Забув пароль/логін» за адресою: moodle.znu@znu.edu.ua
У листі вкажіть: прізвище, ім'я, по-батькові українською мовою; шифр групи; електронну адресу.
Якщо ви вказували електронну адресу в профілі системи Moodle ЗНУ, то використовуйте посилання для відновлення паролю
https://moodle.znu.edu.ua/mod/page/view.php?id=133015

ЦЕНТР ІНТЕНСИВНОГО ВИВЧЕННЯ ІНОЗЕМНИХ МОВ:
http://sites.znu.edu.ua/child-advance/

ЦЕНТР НІМЕЦЬКОЇ МОВИ, ПАРТНЕР ГЕТЕ-ІНСТИТУТУ:
https://www.znu.edu.ua/ukr/edu/ocznu/nim

ШКОЛА КОНФУЦІЯ (ВИВЧЕННЯ КИТАЙСЬКОЇ МОВИ):
http://sites.znu.edu.ua/confucius