КЛАСИЧНИЙ ПРИВАТНИЙ УНІВЕРСИТЕТ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

СИЛАБУС

навчальної дисципліни
«БЕЗПЕКА ПРОГРАМ ТА ДАНИХ»

КОНТАКТНА ІНФОРМАЦІЯ ТА ТЕХНІЧНОЇ ДОПОМОГА

(включаючи електронну пошту, робочий час / місцезнаходження тощо).

Викладач (-і)	Ковтун Володимир Андрійович
Контактний тел.	+38(096) 829-53-69 (внутр. 224)
E-mail:	kovtun.v.a.92@gmail.com
Сторінка курсу на сайті підтримки навчальних програм КПУ	http://www.zhu.edu.ua/cpu_edu/course/view.php?id=5276
Консультації	*Консультації off-line:* за графіком консультацій викладача інформаційно-комунікаційними технологіями: ZOOM - https://us02web.zoom.us/j/7844225252?pwd=Q1A1bkFPMEwxdmQvWHBhVDJjODJvZz09 Google Meet: https://meet.google.com/qgq-ncrp-yha

АНОТАЦІЯ

Навчальна дисципліна «Безпека програм та даних» є нормативною для студентів першого (бакалаврського) рівня вищої освіти галузі знань 01 Освіта/Педагогіка за спеціальністю 014 Середня освіта, освітня програма: Інформатика. Згідно з навчальним планом денної форми навчання вивчення дисципліни заплановано на 8 семестр (4 курс).

Особливістю курсу для спеціальності 014 Середня освіта освітня програма є його виражена методична спрямованість, яка передбачає не лише опанування технічних аспектів захисту даних, а й підготовку майбутнього вчителя до формування цифрової грамотності та безпечної поведінки учнів у закладах загальної середньої освіти.

Курс передбачає поєднання теоретичного навчання з аналізом реальних кейсів кіберзагроз в освітньому середовищі, вивчення законодавчих вимог щодо захисту персональних даних учасників освітнього процесу та розробку стратегій кіберзахисту для шкільних комп'ютерних класів.

Освітній процес з дисципліни здійснюється за такими формами: навчальні заняття; самостійна робота; контрольні заходи. Видами навчальних занять згідно з навчальним планом є лекції; практичні заняття, а також консультації.

Практичні заняття передбачають роботу з доступним програмним забезпеченням для шифрування, антивірусного захисту та резервного копіювання, а також моделювання ситуацій

для навчання школярів методам протидії фішингу, кібербулінгу та правилам безпечного використання хмарних сервісів у навчанні.

Самостійна робота проводиться під час аудиторних занять та в час, вільний від обов'язкових навчальних занять, без участі викладача шляхом самостійного опрацювання лекційного матеріалу, виконання індивідуальних завдань з кожного модуля курсу. Повний курс лекційного матеріалу та методичні рекомендації до виконання індивідуальних домашніх завдань розміщено на сторінках дисципліни сайту підтримки навчальних програм університету.

Консультації призначені для роз'яснення студентам теоретичних або практичних питань.

Засвоєння навчального матеріалу перевіряється за допомогою поточного контролю, який здійснюється на практичних заняттях у формі усних відповідей, самостійних робіт та перевірці виконання завдань, виконання практичних робіт. Для визначення результатів модульного та підсумкового контролю використовується система накопичення балів, яка стимулює систематичну роботу студента протягом семестру.

Підсумковий (семестровий) контроль після завершення 8 семестру здійснюється у формі екзамену.

ФОРМАТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Загальна кількість годин – 90 год., у т. ч. 42 годин аудиторних занять і 48 годин самостійної роботи студента. Кількість кредитів ECTS – 3.

Всього кредитів	Всього годин	Аудиторних годин	У тому числі			Сам. робота
			Лекц.	Лабор.	Семін. (практ.)	
3	90	42	14	-	28	48

ОЗНАКИ ДИСЦИПЛІНИ

Курс (рік навчання)	**Семестр**	**Цикл підготовки**	**Нормативна/ вибіркова**
4	8	професійна	нормативна

МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни

Метою навчальної дисципліни є формування у майбутніх учителів інформатики системи фундаментальних знань і практичних навичок у сфері захисту програмного забезпечення та цифрових даних, що дозволить їм ефективно організовувати безпечне освітнє середовище, протидіяти сучасним кіберзагрозам та навчати учнів основам кібергігієни в умовах стрімкої цифровізації суспільства.

Завдання навчальної дисципліни

− ознайомити студентів із нормативно-правовою базою та етичними стандартами інформаційної безпеки в Україні;

− вивчити математичні та логічні основи криптографічних методів захисту інформації;

− навчити класифікувати шкідливе програмне забезпечення та розуміти механізми його розповсюдження;

− опанувати сучасні технології антивірусного захисту та методи контролю цілісності даних;

− сформувати навички розробки стратегій резервного копіювання та захисту облікових записів.

ЗАПЛАНОВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У результаті вивчення дисципліни студенти повинні знати:

- основні поняття та складові тріади інформаційної безпеки;
- принципи роботи симетричних та асиметричних алгоритмів шифрування;
- технологію функціонування електронного цифрового підпису та хешування;
- класифікацію шкідливого ПЗ та методи соціальної інженерії;
- архітектуру антивірусних пакетів та принципи роботи мережевих екранів;
- правила кібергігієни та методики забезпечення безпеки дітей в інтернеті.

Після вивчення дисципліни студенти повинні вміти:

- використовувати програмні засоби для шифрування файлів та створення захищених контейнерів;
- застосовувати електронний підпис для засвідчення автентичності цифрових документів;
- налаштовувати комплексний антивірусний захист та фаєрволи в операційних системах;
- проводити аналіз підозрілих об'єктів за допомогою онлайн-сервісів та портативних сканерів;
- конфігурувати багатофакторну автентифікацію та менеджери паролів;
- розробляти плани автоматичного резервного копіювання даних у хмарні сховища.

Відповідно до освітньо-професійної програми підготовки бакалавра галузі знань 01 Освіта/Педагогіка за спеціальністю 014 Середня освіта, освітня програма: Інформатика вивчення дисципліни «Безпека програм та даних» сприяє формуванню **компетентностей та програмних результатів навчання**:

Інтегральна компетентність:

Здатність розв’язувати складні спеціалізовані задачі у галузі середньої освіти, що передбачає застосування теоретичних знань і практичних умінь з наук предметної спеціальності, педагогіки, психології, теорії та методики навчання і характеризується комплексністю та невизначеністю умов організації освітнього процесу в закладах середньої освіти.

Загальні компетентності:

ЗК 3. Інформаційно-комунікаційна компетентність. Здатність ефективно використовувати сучасні ІКТ для пошуку, обробки, критичної оцінки та поширення інформації в освітньому та соціальному просторах.

ЗК 8. Здатність спілкуватися іноземною мовою. Здатність до комунікації іноземною мовою в професійній діяльності; здатність розуміти іншомовні фахові тексти.

Спеціальні (фахові) компетенції:

СК 10. Безпекова компетентність (Кібербезпека). Здатність проектувати та підтримувати систему кібербезпеки в освітньому середовищі, забезпечувати захист програмного забезпечення та цифрових даних, дотримуючись етичних і правових норм. Здатність формувати в учнів навички безпечної поведінки в інтернеті, знання принципів захисту персональних даних та кібергігієни.

Програмні результати навчання:

РН 11. Забезпечує безпеку програм і даних, ідентифікує кіберзагрози та впроваджує програмно-апаратні методи захисту інформації в освітній інфраструктурі; навчає учнів основам кібергігієни.

РН 16. Використовує іноземну мову для аналізу фахових джерел та технічної документації, а також для професійної комунікації у цифровому середовищі.

ПЛАН КУРСУ

Назва змістових модулів та тем	Лекц.	Практ (сем.)	Завдання для самостійної роботи
Змістовий модуль № 1. Основи криптографії та цілісності даних			
Тема №1. Теоретичні основи інформаційної безпеки	3	-	1. Опрацювання лекційного матеріалу, 2. Самостійне опрацювання теоретичних питань: 1) Визначення ролі складових тріади безпеки в контексті функціонування цифрового закладу освіти. 2) Аналіз основних каналів витоку персональних даних у шкільному середовищі. 3) Перелік прав та обов'язків учителів щодо захисту інформації з обмеженим доступом. 4) Оцінка правових наслідків використання неліцензійного програмного забезпечення в навчальних цілях. 3. Виконання тестового завдання на сайті підтримки навчальних програм.
Тема №2. Методи та алгоритми шифрування даних	2	7	1. Опрацювання лекційного матеріалу, 2. Самостійне опрацювання теоретичних питань: 1) Порівняння ефективності використання симетричних та асиметричних ключів для захисту інформації. 2) Обґрунтування вибору довжини ключа для гарантування стійкості шифрування до атак перебором. 3. Виконання індивідуального завдання № 1. 4. Виконання тестового завдання на сайті підтримки навчальних програм.
Тема №3. Контроль цілісності та електронний цифровий підпис	2	7	1. Опрацювання лекційного матеріалу, 2. Самостійне опрацювання теоретичних питань: 1) Алгоритм застосування хеш-функцій для виявлення несанкціонованих змін у документах. 2) Порядок перевірки статусу сертифіката відкритого ключа під час роботи з електронним підписом. 3. Виконання індивідуального завдання № 2. 4. Виконання тестового завдання на сайті підтримки навчальних програм. 5. Підготовка до модульного контролю за темами 1-3.
Змістовий модуль № 2. Захист програмного забезпечення та антивірусні технології			

Назва змістових модулів та тем	Лекц.	Практ (сем.)	Завдання для самостійної роботи
Тема №4. Класифікація та аналіз шкідливого програмного забезпечення	3	-	1. Опрацювання лекційного матеріалу, 2. Самостійне опрацювання теоретичних питань: 1) Ідентифікація специфічних симптомів активності вірусів та хробаків у операційній системі. 2) Аналіз методів маскування троянських програм під легітимне прикладне програмне забезпечення. 3) Класифікація технік соціальної інженерії за способом впливу на користувача. 4) Опис механізмів поширення програм-вимагачів у локальних та глобальних мережах. 3. Виконання тестового завдання на сайті підтримки навчальних програм.
Тема №5. Антивірусні пакети та технології захисту	2	7	1. Опрацювання лекційного матеріалу, 2. Самостійне опрацювання теоретичних питань: 1) Порівняльна характеристика можливостей сигнатурного та евристичного аналізу загроз. 2) Правила налаштування винятків та рівнів захисту в сучасних антивірусних комплексах. 3.Виконання індивідуального завдання № 3. 4. Виконання тестового завдання на сайті підтримки навчальних програм.
Тема №6. Захист даних в освітньому середовищі та кібергігієна	2	7	1. Опрацювання лекційного матеріалу, 2. Самостійне опрацювання теоретичних питань: 1) Процедура впровадження багатофакторної автентифікації для захисту корпоративної пошти вчителя. 2) Розробка графіка та вибір інструментів для автоматичного резервного копіювання навчальних баз даних. 3. Виконання індивідуального завдання № 4. 4. Виконання тестового завдання на сайті підтримки навчальних програм. 5. Підготовка до модульного контролю за темами 4-6.

ФОРМИ КОНТРОЛЮ ТА КРИТЕРІЇ ОЦІНЮВАННЯ

У процесі вивчення навчальної дисципліни «Безпека програм та даних» використовуються наступні види контролю:

1. Поточний контроль – здійснюється протягом семестру шляхом перевірки виконання тестових завдань, виконання лабораторних робіт, модульних контрольних робіт тощо. За змістом він включає перевірку ступеню засвоєння студентом навчального матеріалу, який охоплюється темою лекційного заняття, уміння самостійно опрацьовувати навчально-методичну літературу, здатність осмислювати зміст теми, уміння публічно та письмово представити певний матеріал, а також виконання завдань самостійної роботи.

2. Підсумковий семестровий контроль – здійснюється у формі письмового екзамену відповідно до графіка освітнього процесу шляхом визначення ступеню засвоєння студентом навчальної дисципліни за результатами виконання обов'язкових завдання поточного (модульного) контролю.

Для оцінювання студентів використовується система накопичування балів. Згідно з «Положенням про організацію освітнього процесу в КПУ» підсумкова оцінка з дисципліни виставляється за 100-бальною шкалою з наступним переведенням у національну шкалу та шкалу ECTS.

Бали нараховуються за виконання завдань аудиторної роботи, практичних, лабораторних робіт, контрольних (модульних) завдань, тестів.

Результати поточного контролю здобувачів вищої освіти є складовими елементами підсумкової оцінки з дисципліни.

Оцінка рівня роботи студента протягом семестру під час навчальних занять та самостійної роботи здійснюється у межах 80 балів. Вага екзамену у підсумковій оцінці складає 20 балів.

РОЗПОДІЛ БАЛІВ ПОТОЧНОГО ТА ПІДСУМКОВОГО (СЕМЕСТРОВОГО) ОЦІНЮВАННЯ

Поточне оцінювання під час навчальних занять та самостійної роботи						Екзамен	Сума
Змістовий модуль 1			Змістовий модуль 2				
Т1	Т2	Т3	Т4	Т5	Т6	20	100
10	15	15	10	15	15		

Критерії оцінювання

Для оцінювання відповідей студентів з навчальної дисципліни «Безпека програм та даних» використовуються наступні **критерії**:

– рівню «відмінно» відповідає теоретично правильна і вичерпна відповідь на поставлене питання, у якій студент показав всебічне системне знання програмного матеріалу; засвоєння основної та додаткової літератури; чітке володіння понятійним апаратом, методами, методиками та інструментами, вивчення яких передбачене програмою дисципліни; уміння використовувати знання для аналізу життя економічного суспільства та аргументувати своє ставлення до відповідних категорій, закономірностей, випадковостей, суспільних явищ і процесів;

– рівню «добре» відповідає теоретично правильна, але не вичерпна відповідь на поставлене запитання, в цілому повне знання програмного матеріалу, успішне виконання запропонованого завдання і засвоєння матеріалу основної літератури;

– рівню «задовільно» відповідає у цілому правильна відповідь на поставлене питання, в якій студент показав достатній рівень знань з основного програмного матеріалу дисципліни, але не зміг переконливо аргументувати свою відповідь, помилився у використанні понятійного

апарату, показав недостатні знання рекомендованої літератури;

– рівню «незадовільно» відповідає неправильна або неповна відповідь на запитання, у якій студент продемонстрував значні прогалини у знаннях з основного програмного матеріалу; ухилився від аргументувань; показав незадовільні знання понятійного апарату і спеціальної літератури чи взагалі нічого не відповів.

Шкала оцінювання: 100-бальна, національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90-100	A	відмінно	зараховано
82-89	B	добре	
75-81	C		
67-74	D	задовільно	
60-66	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Підручники та навчальні посібники

1. Гнатюк С. О., Хорошко В. О., Лаптєв О. А. Захист інформації в автоматизованих системах. – К.: Видавництво НАУ, 2021. – 368 с.
2. Євсеєв С. П., Король О. Г. Криптографічний захист інформації: навчальний посібник. – Х.: ХНЕУ ім. С. Кузнеця, 2022. – 245 с.
3. Бевз О. В., Ковтун В. Ю. Кібербезпека в освітньому середовищі: посібник для вчителів. – К.: Літера, 2023. – 192 с.
4. Оксентюк В. В., Боярчук О. М. Основи кібергігієни та безпеки в Інтернеті. – Житомир: Полісся, 2020. – 210 с.

Статті у наукових фахових виданнях

1. Мельник А. М. Методи виявлення шкідливого програмного забезпечення на основі поведінкового аналізу. – К.: Кібербезпека: освіта, наука, техніка, 2024. №1 (21). – С. 45–58.
2. Коваленко О. І. Застосування хмарних антивірусних технологій у закладах середньої освіти. – Суми: Вісник СумДУ, 2021. №3. – С. 112–120.
3. Сидоренко В. П. Криптографічні методи захисту персональних даних учасників освітнього процесу. – Одеса: Інформатика та математичні методи в моделюванні, 2022. Том 12, №2. – С. 88–96.
4. Іванчук Ю. В. Електронний цифровий підпис як інструмент діджиталізації сучасної школи. – К.: Наукові записки НаУКМА. Комп'ютерні науки, 2023. Том 6. – С. 34–41.

Автореферати дисертацій

1. Ткачук Р. Л. Методи та засоби оцінки цілісності даних у розподілених системах: автореф. дис. канд. техн. наук: 05.13.05. – Львів, 2021. – 20 с.
2. Василенко М. О. Моделі захисту програмного забезпечення від несанкціонованого копіювання: автореф. дис. канд. техн. наук: 05.13.06. – Харків, 2020. – 22 с.
3. Петренко С. В. Побудова систем антивірусного моніторингу в корпоративних мережах: автореф. дис. канд. техн. наук: 05.12.02. – К., 2022. – 24 с.
4. Дмитрук Л. В. Захист інформації в хмарно-орієнтованих освітніх системах: автореф. дис. канд. пед. наук (інформаційні технології): 13.00.10. – К., 2023. – 21 с.

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

Українські освітні ресурси

1. Дія.Освіта: osvita.diia.gov.ua – державна платформа з освітніми серіалами про кібергігієну та захист персональних даних для громадян.
2. Кіберполіція України: cyberpolice.gov.ua – офіційний ресурс із рекомендаціями щодо протидії інтернет-шахрайству та актуальними новинами про кіберзагрози.
3. НКЦК (Національний координаційний центр кібербезпеки): ncck.gov.ua – ресурс РНБО з аналітичними звітами та порадами щодо захисту національного кіберпростору.
4. Stop Sexting: stop-sexting.in.ua – провідний український портал про безпеку дітей в інтернеті та захист від онлайн-насильства.

Програмне забезпечення та документація

1. VeraCrypt: veracrypt.fr – відкрите програмне забезпечення для створення зашифрованих дисків та контейнерів із підтримкою AES.
2. VirusTotal: https://www.google.com/search?q=virustotal.com – онлайн-сервіс для миттєвої перевірки підозрілих файлів та посилань за допомогою десятків антивірусних двигунів.
3. KeepassXC: keepassxc.org – менеджер паролів із відкритим вихідним кодом, що дозволяє безпечно зберігати облікові дані локально.
4. Windows Security Documentation: learn.microsoft.com – офіційна документація з налаштування вбудованих засобів захисту Windows Defender та брандмауера.

Електронні підручники та освітні платформи

1. Coursera (Cybersecurity Specialization): coursera.org – міжнародна платформа з курсами від провідних університетів світу з основ безпеки програм.
2. Prometheus: prometheus.org.ua – українська платформа з безкоштовним курсом «Основи інформаційної безпеки» для широкого кола користувачів.
3. Cisco Networking Academy: netacad.com – професійні курси з мережевої безпеки та захисту від кіберзагроз із практичними симуляціями.
4. Електронна бібліотека НАПН України: lib.iitta.gov.ua – репозиторій наукових праць та підручників з інформатизації освіти та безпечного використання ІТ.

Фахові спільноти та ресурси

1. DOU (Розділ Security): dou.ua – найбільша спільнота програмістів України з експертними статтями про актуальні вразливості та методи захисту ПЗ.
2. OWASP (Open Web Application Security Project): owasp.org – глобальна спільнота, що фокусується на безпеці програмного забезпечення та стандартах захисту вебдодатків.
3. Infosecurity.ua: infosecurity.ua – спеціалізований інформаційний ресурс про ринок інформаційної безпеки в Україні та світі.
4. Facebook-спільнота «Кіберпедагоги»: facebook.com – об’єднання вчителів інформатики для обміну досвідом викладання безпечної поведінки в інтернеті.