СІЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист програмного забезпечення та даних

Рівень вищої освіти	Перший (бакалаврський)
Код та назва спеціальності **Галузь знань**	F6 Інформаційні системи та технології F.Інформаційні технології
Тип та назва освітньої програми	Освітньо-професійна програма «Прикладні інформаційні системи та технології»
Статус навчальної дисципліни	Обов'язкова компонента (ОК-12)
Курс, семестр викладання	2 курс, 1 семестр
Працемісткість навчальної дисципліни	6 кредитів ЄКТС (180 академічних годин) Денна (очна) форма навчання: лекц- 34 год., лаб. – 16 год., практ. – 16 год., самост. – 114 год. Заочна форма навчання: лекц- 12 год., лаб. – 12 год., практ. – 12 год., самост. – 144 год.
Мова викладання	Українська
Кафедра	Кібербезпеки та технічного захисту інформації
Факультет	Інформаційних технологій та кібербезпеки

Розробники / викладачі

Басов Віктор Євгенович
Старший викладач кафедри кібербезпеки та технічного захисту інформації
Кандидат технічних наук за фахом 05.12.02 – Телекомунікаційні системи та мережі
E-mail: v.y_basov@suitt.edu.ua
Консультації згідно розкладу консультацій кафедри Кібербезпеки та технічного захисту інформації

Загальна інформація про дисципліну	
Анотація до дисципліни	Навчальна дисципліна «Захист програмного забезпечення та даних» - одна із складових дисциплін у циклі підготовки за спеціальністю «Комп'ютерна інженерія». Вона визначає одну із сфер практичного застосування методів та засобів. комп'ютерної інженерії. Вивчення цієї дисципліни спрямовано на: • формування у здобувачів вищої освіти системного уявлення про необхідність підтримувати безпеку програмного забезпечення та даних протягом усього їх життєвого циклу; • розуміння основ аналізу шкідливого програмного забезпечення; • розвиток умінь застосовувати методи та засоби програмної та апаратної протидії атакам на інформаційні ресурси; • вдосконалення навичок пошуку найбільш ефективних методів та засобів задач захисту програмного забезпечення та даних;
Мета дисципліни	Формування у здобувачів вищої освіти базових теоретичних знань і практичних навичок щодо методів і засобів захисту програмного забезпечення та даних від несанкціонованого доступу, шкідливого програмного коду, атак і витоків інформації.
Компетентності, формуванню яких сприяє дисципліна	**ЗК-3.** Здатність до розуміння предметної області та професійної діяльності. **ЗК-8.** Здатність оцінювати та забезпечувати якість виконуваних робіт. **СК-1**. Здатність аналізувати об’єкт проєктування або функціонування та його предметну область. **СК-6**. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов’язків.
Програмні результати навчання	**ПРН-3.** Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп’ютерних програм мовами високого рівня із застосуванням об’єктно-орієнтованого програмування для розв’язання задач проєктування і використання інформаційних систем та технологій. **ПРН-15**. Знати методи захисту інформації, моделі безпеки інформаційних систем, використовувати ці знання при створенні безпечних інформаційних систем. **ПРН-17.** Застосовувати інформаційні технологій та засоби для створення ІТ інфраструктури та її компонентів, вміти здійснювати їх технічне обслуговування.

Програма навчальної дисципліни	
Тема 1. **Вступ до дисципліни та історія питання**	- **Вступ до дисципліни. Основні поняття інформаційної безпеки.** (поняття конфіденційності, цілісності, доступності, базові моделі загроз, приклади атак). - **Історія шкідливого програмного забезпечення.** (від «CoreWars» до сучасних APT, огляд вірусів, троянців, логічних бомб, хробаків). - **Класифікація шкідливого коду та методи його виявлення.** (віруси файлові, резидентні, поліморфні, руткіти, без файлові атаки, бекдори; підходи до детекції).
Тема 2. **Архітектура атак і загроз**	- **Методологія MITREATT&CK: тактики, техніки, процедури.** (розвідка, початковий доступ, виконання). - **Системи атак: розвиток ресурсів, закріплення, привілейований доступ.** - **Бічний рух і збір інформації.** (техніки lateral movement, credential dumping, discovery). - **Ексфільтрація та вплив (exfiltration & impact).** (витік даних, шифрувальники, атаки на доступність).
Тема 3. Застосування криптографії для захисту програм та даних	- **Криптографічні основи захисту програмного забезпечення.** (симетричні та асиметричні алгоритми, властивості). - **Керування ключами та розподіл секретів.** (методи Шаміра, Блеклі, CRT-based; PKI; протоколи узгодження ключів). - **Хешування та електронні підписи.** (SHA-сімейство, стійкість до колізій, застосування у безпечному ПЗ). - **Методи криптоаналізу та їх практичне застосування.** (факторизація, методи Полларда, атаки на LFSR, secretsharing).
Тема 4. Захищене програмування	- **Принципи захищеного програмування.** (помилки в коді, SQL Injection, XSS, bufferoverflow). - **Мови та середовища програмування: уразливості та засоби захисту.**

	(C/C++, Java, Python, особливості безпеки; пам'ять та керування ресурсами). - **Захист операційних систем і середовищ виконання.** (Windows, Linux, Android; моделі прав доступу, sandboxes). - **Методи тестування безпеки ПЗ.** (static code analysis, fuzzing, penetration testing, code review).
Тема 5. Практика та сучасні тенденції захисту програмного забезпечення та даних.	- **Реверс-інжиніринг програмного забезпечення.** (IDAPro, приклади аналізу шкідливого коду на C++). - **Сучасні тенденції та перспективи у сфері безпеки ПЗ.** (кібервійна, штучний інтелект у безпеці, zerotrust, supplychainattacks).
Методи навчання	
При вивченні навчальної дисципліни використовуються наступні методи навчання:	
Інтерактивні	- Наочно-демонстраційні дидактичні комплекси до тем, що вивчаються в межах дисципліни (схеми, таблиці, графіки, діаграми; зображення, картини, зарисовки, фотографії; відеоролики; стрічки новин чи подій тощо). - Відповіді на запитання і опитування думок здобувачів освіти (дискусії). - Відпрацювання навичок та робота в групах. Організовується групова робота (2–6 осіб) і з конкретними завданнями, що виконуються спільно з взаємодопомогою, після чого результати презентуються в аудиторії для розвитку професійних і командних навичок.
Практичні	- Вправи. Різні практичні завдання, які застосовуються на будь-якому етапі навчального процесу і допомагають задіювати інтелектуальні, комунікативні та пошукові здібності здобувачів освіти. Вони можуть включати відповіді на запитання, розв'язання задач, виправлення помилок, складання порівняльних таблиць, графіків і т.п. - Творчі роботи. Мета таких робіт – розвиток творчого мислення, ерудиції, логіки, вміння комбінувати різні знання і техніки. Ці способи навчання охоплюють: проведення власних досліджень, написання рефератів, створення макетів, ілюстрацій.
Методи дистанційного навчання	- Відеоконференції в форматі лекцій або семінарів. Зв'язок здобувачів освіти з викладачем забезпечують різноманітні сучасні платформи, такі як: Zoom, Moodle, GoogleMeet та ін. - Онлайн дискусії; - Індивідуальне і групове консультування (викладач дає додаткові роз'яснення щодо виконання завдань через чати та e-mail-надсилання);

	- Відеозаписи лекцій і практичних занять.

Стратегія оцінювання результатів навчання	
Змістовий контент результатів навчання з дисципліни	Результати навчання з даної дисципліни, які здобувач може продемонструвати та які можна ідентифікувати, оцінити і виміряти, розглядаються у вимірах 6 рівня Національної рамки кваліфікацій, що відповідає першому циклу вищої освіти Рамки кваліфікацій Європейського простору вищої освіти, а саме: ***Знання***–очікується засвоєння базових концептуальних положень управління доступом до інформаційних ресурсів, включаючи теоретичні підходи, принципи, моделі (DAC,MAC,RBAC), етапи реалізації, а також регламенти й процедури адміністрування доступу, журналювання подій, впровадження єдиного входу (SSO) та аутентифікації. ***Уміння/навички***–формується здатність проводити дослідження та впроваджувати інноваційні рішення в управлінні доступом на основі компетентнісного підходу, розв'язувати складні задачі у сферах налаштування політик доступу, оцінювання безпеки, впровадження SSO, а також забезпечувати захист інформаційних ресурсів через аналіз ризиків і застосування сучасних технологій. ***Комунікація***–здатність ефективно спілкуватися та взаємодіяти з командою проєкту, застосовуючи сучасні методи інформаційно-комунікаційних систем та технологій; ***Відповідальність і автономія***–очікується здатність самостійно розв'язувати нестандартні ситуації вуправлінні доступом, що потребують нових стратегічних підходів.
Критерії оцінювання	Академічні успіхи здобувачів освіти в межах даної дисципліни оцінюються за бально-рейтинговою шкалою (максимальна кількість – 100 балів), що прийнята в ДУІТЗ, з обов'язковим переведенням кількості балів в оцінки за національною шкалою та за шкалою ECTS. **Відмінно (А) – від 90 до 100 балів** – здобувач у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішує усі або не менше 90% завдань, передбачених програмою навчальної дисципліни. **Дуже добре (В) – від 82 до 89 балів** – здобувач досить повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Однак під час викладання деяких питань допускаються при цьому окремі несуттєві неточності. Правильно вирішує 80-89% письмових завдань. **Добре (С) – від 74 до 81 балів –** здобувач достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань,

	використовуючи при цьому обов'язкову літературу. Однак під час викладання деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішує 74-81% письмових завдань. **Задовільно (D) – від 64 до 73 балів –** здобувач в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних та письмових відповідей, але з не зовсім глибоким та всебічним аналізом, обґрунтуванням та аргументацією, з недостатнім використанням необхідної літератури, допускаючи при цьому окремі неточності та помилки. Правильно вирішує 64-73% письмових завдань. **Задовільно (E) – від 60 до 63 балів –** здобувач в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури, допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішує 60-63% письмових завдань. **Незадовільно з можливістю повторного складання (FX) – від 35 до 59 балів –** здобувач не в повному обсязі володіє навчальним матеріалом. Фрагментарно, стисло без аргументації та обґрунтування викладає його під час усних виступів та письмових відповідей, поверхово розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності. Правильно вирішує 35-59% письмових завдань. **Незадовільно з обов'язковим повторним вивченням дисципліни(F) – від 0 до 34 балів –** Здобувач частково володіє навчальним матеріалом, не у змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішує 1-34% письмових завдань.
Форма та методи контролю навчальних досягнень	Контроль успішності навчання здобувачів освіти здійснюється на засадах відкритості та академічної доброчесності. В межах даної дисципліни передбачено два види контролю: поточний (*тематичний, рубіжний*) та підсумковий *(семестровий)*. ***Поточний контроль*** здійснюється протягом семестру під час проведення практичних занять; виконання завдань самостійної роботи; складання тематичних контрольних робіт, тестів тощо. Поточний контроль спрямований на перевірку: рівня підготовленості здобувача до занять; активності під час обговорення навчального матеріалу; якості виконання індивідуальних, практичних і тестових завдань; своєчасності та повноти виконання самостійної роботи. Результат поточного оцінювання є середньо арифметичним значенням отриманих балів за всі виконані завдання під час аудиторних (практичні, семінарські) занять та завдання, що виконуються під час самостійної роботи. До підсумкового контролю допускаються здобувачі, які за результатами поточного оцінювання набрали не менше 60 балів. ***Підсумковий контроль*** проводиться у формі екзамену, який передбачає перевірку рівня теоретичних знань, практичних умінь і навичок, а також здатності їх застосовувати у професійній діяльності.
Політика навчальної дисципліни	
Відвідування	Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни згідно академічного розкладу. Присутність на практичних, лабораторних заняттях та контрольних заходах (екзамен) є обов'язковою. Важливим є своєчасне виконання індивідуальних завдань в межах самостійної роботи, передбачених програмою дисципліни.

Дотримка академічної доброчесності	Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати різні програмні засоби.
Умови зарахування пропущених занять	Відпрацювання академічної заборгованості з дисципліни можливо до початку екзаменаційної сесії. Процедура узгоджується з викладачем, згідно його розкладу консультацій.
Інші умови	Навчально-методичні матеріали дисципліни розміщені на платформі Moodle.
Рекомендовані джерела інформації	
Базові підручники та навчальні посібники	Stallings, W., & Brown, L. Computer Security: Principles and Practice. 5th ed. Pearson, 2021, 816 p. Bishop, M. Computer Security: Art and Science. 2nd ed. Addison-Wesley, 2019, 1296 p. Viega, J., & McGraw, G. Building Secure Software: How to Avoid Security Problems the Right Way. Updated Edition. Addison-Wesley, 2020, 512 p. Northcutt, S. Inside Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems. Pearson IT Certification, 2021, 624 p. Попов, С. М., та ін. Кібербезпека та захист інформації: навчальний посібник. Київ: КНЕУ, 2022, 342 с. Литвиненко, В. В., Колесніков, А. О. Методичні рекомендації до вивчення дисципліни «Захист інформаційних систем». Харків: ХНУРЕ, 2021, 45 с. Ткаченко, П. М., Дьяконов, І. М. Методичні рекомендації з виконання практичних завдань з кібербезпеки. Київ: ДУІКТ, 2023, 52 с. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection. Information Security Management Systems. International Organization for Standardization, 2022, 40 p. ENISA. Good Practices for Secure Software Development Lifecycle. – European Union Agency for Cybersecurity, 2021, 58 p..
Методичні рекомендації та розробки викладачів дисципліни	Корчинський В.В., Бєлова Ю.В. Теорія інформації та кодування: методичні вказівки до лабораторних та практичних занять для підготовки бакалаврів. Спец.: 125 – Кібербезпека та захист інформації, Одеса, ДУІТЗ, 2023, 83 с. Басов В.Є. Безпека розробки та підтримки додатків. Посібник до проведення лабораторних робіт. Спец.: 125 – Кібербезпека та захист інформації, Одеса, ДУІТЗ, 2021, 44 с
Інформаційні ресурси	НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. К.: Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ, 1999. – 28 с. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. К.: Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ, 1999. – 64 с. PhishTank: URL: https://www.phishtank.com/ (дата звернення: 01.05.2025). GeoIP: URL: https://www.maxmind.com/en/geoip-demo (дата звернення: 01.05.2025). WhoIs: URL: https://www.whois.com/whois/ (дата звернення: 01.05.2025).

	MITRE ATT&CK. Enterprise matrix: URL: https://attack.mitre.org/matrices/enterprise/ (дата звернення: 01.05.2025). MITRE ATT&CK Mobile Matrix: URL: https://attack.mitre.org/matrices/mobile/ (дата звернення: 01.05.2025). MITRE ATT&CK ICS Matrix–URL: https://attack.mitre.org/matrices/ics/ (дата звернення: 01.05.2025). Virus Total (Електронний ресурс) –URL: https://www.virustotal.com/gui/home/upload (дата звернення: 01.05.2025).

Рік введення силабусу – 2025 р.	Затверджено рішенням кафедри Інформаційних та комп'ютерних систем (Протокол від 26 серпня 2025 р. № 1) Завідувач кафедр Володимир КОРЧИНСЬКИЙ Гарант освітньої програми Роман ЦАРЬОВ Викладач: Віктор БАСОВ