МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ХУДОЖНЬО-ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ
Відділення механіко-технологічне

	СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Технології захисту інформації» **Освітньо-професійної програми:** **«Обслуговування програмних систем і комплексів»** (назва освітньо-професійної програми) **Спеціальність F3 «Комп'ютерні науки»** (шифр та назва спеціальності) **Галузь знань: F «Інформаційні технології»** (шифр та назва галузі знань) **Освітньо-професійний ступінь:** фаховий молодший бакалавр
Циклова комісія	Комп'ютерних та землевпорядних дисциплін
Курс, семестр	IV курс, VII семестр
Обсяг	4 кредити ЄКТС – 120 годин. Аудиторні заняття: лекційні – 40 год., практичні - 35 год., самостійне опрацювання студентів – 45 год.
Мова викладання	українська
Вимоги до початку вивчення	Необхідні знання та навички з дисциплін «Алгоритмізація та програмування» «Операційні системи» «Комп'ютерні мережі» «Основи програмування»
Відповідність компетентностей та програмних результатів навчання	Загальні компетентності (ЗК): ЗК3. Здатність до абстрактного мислення, аналізу та синтезу. ЗК4. Здатність застосовувати знання у практичних ситуаціях. ЗК5. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК6. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК7. Здатність спілкуватися іноземною мовою. ЗК8. Здатність вчитися і оволодівати сучасними знаннями. ЗК9. Здатність до пошуку, оброблення та аналізу інформації з різних джерел Результати навчання (РН): РН07. Застосовувати основні механізми та методи безпеки мереж і програмних систем. РН11. Застосовувати сучасні мови програмування та технології для розробки програмного забезпечення розподілених систем. РН17. Володіти методами, засобами, стандартами захисту програмних систем і даних в умовах супроводження та експлуатації програмних систем і комплексів. РН19. Вміти аналізувати, цілеспрямовано здійснювати пошук інформації в різних джерелах, вибирати необхідні для вирішення професійних завдань в галузі комп'ютерних наук інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки. РН20. Демонструвати розуміння основних засад охорони праці та безпеки життєдіяльності і їх застосування. Спеціальні компетентності (СК) СК1. Здатність використовувати основні поняття, ідеї та методи фундаментальних наук під час розв'язання складних спеціалізованих задач з комп'ютерних наук в галузі інформаційних технологій. СК2. Здатність використовувати теоретичні та фундаментальні знання в галузі комп'ютерних наук та інформаційних технологій для вирішення різноманітних проблем. СК3. Здатність розробляти, аналізувати та застосовувати ефективні алгоритми для розв'язання конкретних професійних задач залежно від предметного середовища.

	СК7. Здатність проєктувати, розробляти та обслуговувати веб-застосунки з динамічним контентом, використовуючи веб-технології, технології комп'ютерної графіки та анімації. СК9. Здатність застосовувати знання сучасних методів і технологій створення та супроводження розподілених систем.
Місце дисципліни в освітньо-професійній програмі	Дисципліна «Технології захисту інформації» належить до циклу професійної та практичної підготовки освітньо-професійної програми спеціальності F3 «Комп'ютерні науки». Вона забезпечує формування теоретичних знань та практичних умінь у сфері захисту інформації, безпеки програмних, мережевих і розподілених систем, а також ознайомлює студентів з основними загрозами інформаційній безпеці та методами їх запобігання. Зміст навчального матеріалу дисципліни спрямований на розвиток аналітичного мислення, здатності оцінювати ризики, застосовувати методи та засоби захисту інформації, забезпечувати конфіденційність, цілісність і доступність даних у процесі експлуатації інформаційних систем. Вивчення курсу «Технології захисту інформації» є важливим етапом підготовки фахівця з комп'ютерних наук та створює підґрунтя для подальшого опанування дисциплін професійного спрямування у галузі інформаційних технологій та кібербезпеки.
Що буде вивчатися	У межах дисципліни «Технології захисту інформації» студенти вивчатимуть основи інформаційної безпеки, принципи забезпечення конфіденційності, цілісності та доступності інформації, основні загрози та ризики для інформаційних систем, а також методи і засоби їх нейтралізації. Особлива увага приділяється захисту програмних, мережевих і розподілених систем, питанням організаційного, технічного та програмного забезпечення інформаційної безпеки. Розділ І. Основи інформаційної безпеки та захисту інформації. Поняття інформації та інформаційної безпеки. Основні загрози інформаційним ресурсам. Класифікація загроз і каналів витоку інформації. Моделі порушника та оцінювання ризиків. Основні принципи та підходи до захисту інформації. Розділ ІІ. Криптографічні методи захисту інформації. Основи криптографії. Симетричні та асиметричні методи шифрування. Хеш-функції та електронний цифровий підпис. Управління криптографічними ключами та сертифікація. Застосування криптографічних засобів у програмних і мережевих системах. Розділ ІІІ. Захист програмних і мережевих систем. Методи захисту програмного забезпечення. Ідентифікація, автентифікація та контроль доступу користувачів. Захист операційних систем. Безпека комп'ютерних мереж. Основні мережеві атаки та методи протидії. Захист розподілених систем і веб-застосунків. Розділ ІV. Організаційні та правові аспекти захисту інформації. Нормативно-правове забезпечення захисту інформації. Політики інформаційної безпеки та організація захисту інформації в установах і на підприємствах. Стандарти та вимоги у сфері інформаційної безпеки. Основи охорони праці та безпеки життєдіяльності при роботі з інформаційними системами.
Чому це цікаво/треба вивчати	Дисципліна «Технології захисту інформації» є актуальною та необхідною, оскільки інформація є одним із найцінніших ресурсів сучасного суспільства, а кількість загроз інформаційній безпеці постійно зростає. Вивчення цього курсу дозволяє зрозуміти причини виникнення загроз, способи несанкціонованого доступу до інформації та методи захисту даних у програмних, мережевих і розподілених системах. Під час опанування дисципліни студенти отримують уявлення про принципи побудови безпечних інформаційних систем, використання криптографічних засобів, організацію контролю доступу та забезпечення цілісності інформації. Це дає можливість побачити, як теоретичні знання застосовуються для розв'язання практичних задач у сфері інформаційних технологій.

	Актуальність курсу зумовлена високим попитом на фахівців, які володіють знаннями та навичками із захисту інформації. Набуті компетентності є важливою складовою професійної підготовки фахівця з комп'ютерних наук та створюють основу для подальшого професійного розвитку у сфері інформаційної безпеки та кіберзахисту.
Чому можна навчатися	У процесі вивчення дисципліни «Технології захисту інформації» студенти набудуть знань і практичних умінь, необхідних для забезпечення захисту інформації в програмних, мережевих та інформаційних системах. Отримані компетентності дозволять аналізувати загрози інформаційній безпеці, обирати та застосовувати відповідні методи і засоби захисту інформаційних ресурсів. Студенти навчаться використовувати основні криптографічні методи захисту інформації, реалізовувати механізми контролю доступу, забезпечувати безпеку програмного забезпечення та комп'ютерних мереж, а також здійснювати захист даних у процесі експлуатації інформаційних систем. Особлива увага приділяється практичному застосуванню засобів захисту інформації та дотриманню вимог стандартів і нормативно-правових актів. Набуті знання можуть бути використані під час розробки, супроводження та адміністрування інформаційних систем, у професійній діяльності фахівців з комп'ютерних наук, а також для подальшого навчання і професійного розвитку у сфері інформаційної безпеки та кіберзахисту.
Як користуватися набутими знаннями\уміннями	Набуті під час вивчення дисципліни «Технології захисту інформації» знання та вміння можуть бути використані під час розробки, експлуатації та супроводження програмних, мережевих і інформаційних систем з метою забезпечення захисту інформації. Студенти зможуть застосовувати методи та засоби захисту для забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів. Отримані знання дозволяють здійснювати аналіз загроз і вразливостей, обирати та впроваджувати відповідні технічні, програмні й організаційні заходи захисту інформації, використовувати криптографічні засоби, механізми контролю доступу та засоби захисту мереж і програмних систем. Практичне використання набутих знань є важливою складовою професійної діяльності фахівця з комп'ютерних наук та сприяє підвищенню рівня інформаційної безпеки під час роботи з інформаційними системами в умовах їх супроводження та експлуатації.
Заняття	Лекційні заняття: формування теоретичних знань щодо основ інформаційної безпеки, загроз і методів захисту інформації, ознайомлення з криптографічними, програмними та організаційними засобами захисту інформації з використанням мультимедійних матеріалів та аналізу практичних прикладів. Практичні заняття: закріплення теоретичного матеріалу та формування практичних умінь із застосування методів і засобів захисту інформації, аналізу загроз, реалізації механізмів контролю доступу, використання криптографічних засобів та забезпечення безпеки програмних і мережевих систем. Лабораторні заняття: виконання практичних завдань із використанням комп'ютерних технологій, спрямованих на налаштування та застосування засобів захисту інформації, аналіз рівня захищеності інформаційних систем і відпрацювання практичних навичок забезпечення інформаційної безпеки. Інтерактивні заняття: використання навчальних платформ та онлайн-інструментів (наприклад, Google Classroom, Kahoot, Quizlet) для проведення інтерактивних вправ, тестування знань, обговорення результатів виконаних завдань і здійснення поточного контролю навчальних досягнень студентів.
Інформаційне забезпечення	Рекомендовані джерела інформації: Шаньгін В. Ф. Захист інформації в комп'ютерних системах і мережах : навч. посібник. — К. : Діалектика, 2019.

	Бурячок В. Л., Хорошко В. О. Основи інформаційної та кібербезпеки : навч. посібник. — К. : КПІ ім. Ігоря Сікорського, 2020. Столінгс В. Криптографія та безпека мереж : принципи та практика. — К. : Вільямс, 2018. Документація та стандарти з інформаційної безпеки (ISO/IEC 27001, ISO/IEC 27002). Офіційні ресурси та нормативно-правові акти України у сфері захисту інформації. Допоміжна література: Соммервілл І. Інженерія програмного забезпечення. — К. : Вільямс. Офіційна технічна документація операційних систем і мережевих платформ. Онлайн-ресурси та освітні платформи з інформаційної безпеки та кіберзахисту.
Поточний контроль	Поточний контроль здійснюється викладачем у формі усного опитування, письмового та тестового контролю і спрямований на перевірку рівня засвоєння навчального матеріалу, а також сформованості практичних умінь і навичок із захисту інформації. Контрольні заходи включають виконання практичних і лабораторних завдань за комп'ютером, розв'язання навчальних задач, самостійні роботи, підготовку доповідей і презентацій, тестування, а також оцінювання результатів індивідуальної та групової роботи студентів.
Семестровий контроль	Підсумковий контроль здійснюється у формі екзамену