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

	СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Кіберзахист та управління ризиками» **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	Тема «Кіберзахист та управління ризиками» є складовою навчальної дисципліни «Технології захисту інформації» та належить до циклу професійної та практичної підготовки освітньо-професійної програми спеціальності F3 «Комп'ютерні науки». Вивчення цієї теми забезпечує формування у студентів теоретичних знань і практичних умінь з питань кіберзахисту інформаційних систем, виявлення та оцінювання кіберзагроз, аналізу ризиків і вибору відповідних заходів безпеки для їх мінімізації. Зміст теми спрямований на розвиток аналітичного мислення, здатності комплексно оцінювати стан захищеності інформаційних ресурсів, приймати обґрунтовані рішення щодо управління ризиками та застосовувати сучасні підходи до забезпечення кібербезпеки в процесі експлуатації програмних і мережевих систем.
Що буде вивчатися	У межах теми «Кіберзахист та управління ризиками» студенти вивчатимуть основні принципи забезпечення кіберзахисту інформаційних систем, методи виявлення та аналізу кіберзагроз, а також підходи до оцінювання і управління ризиками інформаційної безпеки. Особлива увага приділяється формуванню системного розуміння кіберзагроз, їх впливу на функціонування інформаційних ресурсів та вибору ефективних заходів захисту. Розділ І. Основи кіберзахисту. Поняття кіберзахисту та кібербезпеки. Основні кіберзагрози та вектори атак. Об'єкти та суб'єкти кіберзахисту. Класифікація кібератак та інцидентів безпеки. Принципи побудови систем кіберзахисту. Розділ ІІ. Управління ризиками інформаційної безпеки. Поняття ризику в інформаційній та кібербезпеці. Ідентифікація загроз і вразливостей. Оцінювання та аналіз ризиків. Методи управління ризиками. Прийняття рішень щодо мінімізації ризиків. Розділ ІІІ. Засоби та методи кіберзахисту. Технічні та програмні засоби кіберзахисту. Захист мережевих і програмних систем. Системи виявлення та запобігання вторгненням. Моніторинг безпеки та реагування на інциденти. Захист розподілених і хмарних систем. Розділ ІV. Організаційні та правові аспекти кіберзахисту. Політики та процедури кібербезпеки. Організація управління кіберризиками. Нормативно-правове забезпечення кіберзахисту. Стандарти та рекомендації у сфері кібербезпеки. Основи охорони праці та безпеки життєдіяльності в умовах кіберзагроз.
Чому це цікаво/треба вивчати	Тема «Кіберзахист та управління ризиками» є актуальною та необхідною, оскільки сучасні інформаційні системи постійно зазнають кібератак і впливу різноманітних загроз. Вивчення цієї теми дозволяє зрозуміти природу кіберзагроз, причини їх виникнення та наслідки для інформаційних ресурсів, програмних і мережевих систем.

	Під час опанування теми студенти отримують уявлення про підходи до організації кіберзахисту, методи оцінювання ризиків та принципи прийняття рішень щодо їх мінімізації. Це сприяє формуванню системного бачення безпеки інформаційних систем і розуміння взаємозв'язку між технічними, організаційними та правовими заходами кіберзахисту. Актуальність теми зумовлена зростанням кількості кіберінцидентів і потребою у фахівцях, здатних оцінювати рівень захищеності інформаційних систем та управляти ризиками. Набуті знання є важливою складовою професійної підготовки фахівця з комп'ютерних наук і створюють основу для подальшого розвитку у сфері кібербезпеки.
Чому можна навчатися	У процесі вивчення теми «Кіберзахист та управління ризиками» студенти набудуть знань і практичних умінь, необхідних для забезпечення кіберзахисту інформаційних систем та управління ризиками інформаційної безпеки. Отримані компетентності дозволяють аналізувати кіберзагрози, оцінювати рівень ризиків і обирати ефективні заходи для їх зменшення. Студенти навчаться ідентифікувати загрози та вразливості, застосовувати методи аналізу ризиків, використовувати технічні та організаційні засоби кіберзахисту, а також брати участь у процесах реагування на кіберінциденти. Особлива увага приділяється формуванню навичок прийняття обґрунтованих рішень у сфері кібербезпеки. Набуті знання можуть бути використані під час проєктування, експлуатації та супроводження інформаційних систем, у професійній діяльності фахівців з комп'ютерних наук, а також для подальшого навчання і професійного розвитку у сфері кіберзахисту та управління ризиками.
Як користуватися набутими знаннями\уміннями	Набуті в межах теми «Кіберзахист та управління ризиками» знання та вміння можуть бути використані під час розробки, експлуатації та супроводження інформаційних систем для забезпечення їх кіберзахисту. Студенти зможуть застосовувати методи і засоби захисту інформації для запобігання кіберзагрозам та зменшення впливу кіберінцидентів. Отримані навички дозволяють оцінювати рівень ризиків інформаційної безпеки, виявляти вразливості інформаційних систем і приймати обґрунтовані рішення щодо вибору заходів кіберзахисту. Застосування методів управління ризиками сприяє підвищенню надійності та безпеки програмних і мережевих систем. Практичне використання набутих знань є важливою складовою професійної діяльності фахівця з комп'ютерних наук та дозволяє ефективно застосовувати сучасні підходи до кіберзахисту та управління ризиками у реальних умовах.
Заняття	Лекційні заняття: формування теоретичних знань з основ кіберзахисту та управління ризиками, вивчення видів кіберзагроз, методів аналізу ризиків, принципів побудови систем кібербезпеки та організації процесів управління ризиками з використанням мультимедійних матеріалів і прикладів із практики. Практичні заняття: закріплення теоретичного матеріалу та формування практичних умінь з ідентифікації кіберзагроз і вразливостей, оцінювання ризиків, вибору та застосування технічних і організаційних заходів кіберзахисту, аналізу кіберінцидентів і прийняття рішень щодо реагування на них. Лабораторні заняття: виконання практичних завдань із використанням програмних і технічних засобів кіберзахисту, налаштування засобів моніторингу безпеки, відпрацювання навичок виявлення та реагування на кіберінциденти, оцінювання рівня захищеності інформаційних систем. 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:

	Бурячок В. Л., Хорошко В. О. Кібербезпека та захист інформації : навчальний посібник. — К. : КПІ ім. Ігоря Сікорського, 2020. Шаньгін В. Ф. Захист інформації в комп'ютерних системах і мережах : навчальний посібник. — К. : Діалектика, 2019. Столінгс В. Безпека комп'ютерних мереж і кіберзахист. — К. : Вільямс, 2018. ISO/IEC 27001 Information Security Management Systems. ISO/IEC 27005 Information Security Risk Management. Нормативно-правові акти України у сфері кібербезпеки та захисту інформації. Допоміжна література: Соммервілл І. Інженерія програмного забезпечення. — К. : Вільямс. Офіційна технічна документація операційних систем, мережевого обладнання та засобів кіберзахисту. Онлайн-ресурси та освітні платформи з кібербезпеки та управління ризиками.
Поточний контроль	Поточний контроль здійснюється викладачем з метою перевірки рівня засвоєння студентами навчального матеріалу, сформованості теоретичних знань і практичних умінь з кіберзахисту та управління ризиками. Контрольні заходи включають усне опитування, виконання практичних і лабораторних завдань за комп'ютером, розв'язання навчальних задач, тестування, самостійні роботи, підготовку доповідей і презентацій, а також оцінювання результатів індивідуальної та групової роботи студентів. Результати поточного контролю враховуються під час підсумкового оцінювання та дозволяють оцінити динаміку навчальних досягнень студентів і рівень їх готовності до практичного застосування набутих знань у сфері кіберзахисту.
Семестровий контроль	Підсумковий контроль здійснюється у формі екзамену