	Силабус навчальної дисципліни **«Захист інформації у комп'ютерних системах»** (назва навчальної дисципліни) **Освітньо-професійної програми: «Комп'ютерна графіка та web-дизайн»** освітньо-професійної програми) **Спеціальність:123 «Комп'ютерна інженерія»** (код та назва спеціальності) **Галузь знань:12 Інформаційні технології** (шифр та назва галузі знань)
Рівень освіти	Фахова передвища
Освітньо-професійний/ освітній ступінь	Фаховий молодший бакалавр
Статус навчальної дисципліни	Обов'язкова
Семестр	8
Обсяг дисципліни (кредити ЄКТС/загальна кількість годин)	3 кредити ЄКТС/90 годин
Мова викладання	Українська
Оригінальність навчальної дисципліни	Дисципліна «Захист інформації в комп'ютерних системах» призначена для набуття студентами здатності забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах і мережах з метою реалізації встановленої політики інформаційної безпеки. Це досягається вивченням теоретичних основ побудови і практики застосування методів та засобів захисту інформації в комп'ютерних системах з метою запобігання несанкціонованому доступи, витоку, руйнації, знищення і модифікації інформації різної категорії шляхом реалізації політики і створення комплексних корпоративних систем захисту інформації.
Мета навчальної дисципліни	Метою вивчення дисципліни «Захист інформації в інформаційних системах» є формування теоретичних знань щодо можливих небезпек і ступеня ризику втрат інформації, а також практичних навичок щодо забезпечення захисту програмної продукції. Основні завдання дисципліни «Захист інформації в інформаційних системах» – вивчення сучасних інформаційних технологій у галузі інформаційної безпеки та криптографічних методів захисту інформації; підготовка фахівців з розробки та впровадження технологій комп'ютерного захисту інформації, забезпечення цілісності даних, конфіденційності, контролю передачі інформації, ідентифікації, аутентифікації, криптографії,

	інтегрованих систем, політики безпеки, менеджменту в галузі безпеки.
Заплановані результати навчання	**Програмні результати навчання (ПРН):** ПРН1. Уміння застосовувати знання у практичних ситуаціях. ПРН2. Уміння адаптуватись до нових ситуацій. ПРН3. Уміння ефективно працювати як автономно, так і у складі команди. ПРН4. Уміння здійснювати оцінку рівня захисту інформації у комп'ютерних системах. ПРН5. Уміння застосовувати знання і розуміння для розв'язання задач синтезу та аналізу в системах, які характерні обраній спеціальності. ПРН7. Уміння використовувати інформаційні і комунікаційні технології для вирішення різних дослідницьких і професійних завдань. ПРН8. Уміння здійснювати пошук інформації в різних джерелах для розв'язання задач, щодо боротьби з недостатнім рівнем захисту інформації. ПРН13. Уміння застосовувати базові знання в області налаштування на боротьби з недостатнім рівнем захисту інформації в професійній діяльності. ПРН14. Уміння застосовувати базові знання стандартів в області інформаційних технологій при розробці та впровадженні інформаційних систем і технологій ПРН17. Уміння застосовувати комп'ютерні засоби при дослідженні режиму роботи програмного забезпечення, яке забезпечує достатній рівень захисту інформації в комп'ютерних системах. ПРН27. Знання принципів організації та основних механізмів захисту інформації у комп'ютерних системах. ПРН28. Проводити перед проектне обстеження предметної області. ПРН29. Знати, розуміти основні процеси, фази та ітерації життєвого циклу програм, що покращують та погіршують рівень захисту інформації у комп'ютерних системах.
Заплановані знання та вміння	**В результаті вивчення навчальної дисципліни здобувач фахової передвищої освіти повинен володіти такими компетентностями:** ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Здатність до адаптації та дії в новій ситуації. ЗК3. Здатність працювати в як автономно, так і в команді. ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК5. Здатність до аналізу та синтезу. ЗК6. Здатність спілкуватися державною мовою як усно, так письмово. ЗК7. Здатність спілкуватися іноземною мовою. ЗК8. Навички використання інформаційних і комунікаційних технологій. ЗК9. Здатність до пошуку, оброблення та аналізу інформації з різних

	джерел. ЗК10. Вміння виявляти, ставити та вирішувати проблеми. ЗК11. Базові уявлення про основи філософії, психології, педагогіки, що сприяють розвитку загальної культури й соціалізації особистості, схильності до етичних цінностей, знання вітчизняної історії, економіки й права, розуміння причинно-наслідкових зв'язків розвитку суспільства й уміння їх використовувати в професійній і соціальній діяльності. ЗК12. Здатність бути критичним і самокритичним. ЗК13. Здатність діяти на основі етичних міркувань (мотивів). ЗК14. Прагнення до збереження навколишнього середовища. ФК2. Знання закономірностей випадкових явищ і вміння застосовувати ймовірнісно-статистичні методи для вирішення професійних завдань. ФК4. Знання особливостей захисту інформації ФК5. Знання особливостей побудови утиліт, що забезпечують захист інформації у комп'ютерних системах, а також загальних принципів організації та функціонування ФК6. Знання методів боротьби, уміння використовувати сучасні засоби протидії утилітам які порушують принципи захисту інформації у комп'ютерних системах. ФК7. Здатність виконувати налаштування та оптимізацію ОС, для збереження безпеки. ФК15. Знання методів та періодичності проведення профілактичних робіт для операційних систем; від загроз пов'язаних з можливістю зараження утилітами, що негативно впливають на захист інформації у комп'ютерних системах. ***знати:*** - що собою являє політика інформаційної безпеки; - правила безпеки при роботі із комп'ютерними мережами; - мережу Інтернет та електронну пошту; - криптографічні методи захисту інформації; - будову та принципи дії комп'ютерних вірусів і шкідливих програм; ***вміти:*** - встановлювати та використовувати антивірусні програми та забезпечувати безпеку використання WWW за допомогою web-браузерів; - розробляти й вирішувати актуальні питання теорії і практики інформаційної безпеки; - застосовувати знання в практичній діяльності.
Навчальна логістика	**Зміст дисципліни:** **Т1.** Історія комп'ютерних вірусів. **Т2.** Основні види шкідливого програмного забезпечення. **Т3.** Сучасні загрози інформаційної безпеки. **Т4.** Загрози для мобільних пристроїв.

	Т5. Антивіруси: технології, індустрія, практичне застосування. **Т6.** Безпека електронних фінансів **.** **Т7.** Принципи поводження з персональною інформацією. **Т8.** Принципи безпечної роботи з мобільними пристроями. **Т9.** Безпека в умовах інформаційної війни та кібервійни. **Т10.** Технології захисту інформації. **Т11.** Основні положення теорії захисту інформації. **Т12.** Фішинг. **Т13.** Скімінг. **Т14.** Вибір антивірусу. **Т15.** Хеш-функції. **Т16.** Дослідження порушення безпеки. **Т17.** Одержання інформації про процеси. **Т18.** Шифри перестановки. Матричний шифр. **Т19.** Генерування випадковиї послідовності чисел. *Теми лабораторних робіт:* **ЛР1.** Створення і зберігання надійних паролей. **ЛР2.** Захист інформації у MICROSOFT WINDOWS. **ЛР3.** Захистінформації під час застосування ОС WINDOWS 7. **ЛР4.** Одержування інформації про процеси, що відбуваються в системі WINDOWS XP. **ЛР5.** Резервне копіювання даних в зовнішнє сховище. **ЛР6.** Шифрування даних за допомогою спеціальних програм та утиліт. (частина 1) **ЛР7.** Відновлення даних. **ЛР8.** ARMITAGE: автоматичний пошук і перевірка експлойтів у КАЛІ LINUX. **ЛР9.** Інсталяція LINUX MALWARE DETECT (LMD) в LINUX. **ЛР10.** Шифрування даних за допомогою спеціальних програм та утиліт. (частина 2). **ЛР11.** Порівняння даних за допомогою хеш-функції. **ЛР12.** Перевірка стану служб середовища WINDOWS. **ЛР13.** Систематизація матеріалу. **Види занять**: лекції,лабораторні та інші. **Методи навчання**: – словесні (лекція, пояснення, розповідь); – наочні (ілюстрація, демонстрація); – практичні(лабораторні роботи, практичні заняття); – пояснювально-ілюстративний; – метод проблемного викладу; – проблемно-пошуковий.
Тематика індивідуальних завдань	Отримується індивідуально у викладача.
Пререквізити	Дисципліна «Захист інформації в комп'ютерних системах» базується на дисциплінах: «Операційні системи»; «Комп'ютерні мережі» та «Програмування».

Постреквізити	В результаті вивчення дисципліни «Захист інформації в комп'ютерних системах» студенти здобувають навики кваліфікованих спеціалістів з комп'ютерних систем та їх захисту.
Рекомендовані навчально-методичні матеріали для вивчення навчальної дисципліни	**Рекомендовані навчально-методичні матеріали:** ***Основні джерела:*** 1. Величко В.В. Передача данных в сетях мобильной связи третьего поколения / В.В.Величко. – М.: Радио и связь, Горячая линия-Телеком, 2005. – 332с. 2. Горбенко І.Д., Горбенко Ю.І., Прикладна криптологія. Теорія. Практика. Застосування: монографія. – Х.:Видавництво «Форт», 2012. – 870с. 3. Захист інформації в комп'ютерних системах та мережах : навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251с. 4. Єжова Л.Ф. Алгоритмізація і програмування процедур обробки інформації. – К.: КНЕУ, 2000. – 152с. 5. Хорошко В.А., Чекатков А.А. Захист інформації в комп'ютерних системах та мережах. Підручник. К.: BHV, 2005. ***Допоміжні джерела:*** 6. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – К.: Укр. НДІССІ, 1997. – 11с. 7. Гуржій А.М., Коряк С.Ф., Самсонов В.В., Скляров О.Я. Контроль та керування корпоративними комп'ютерними мережами: Інструментальні засоби та технології: Навч. посібник. – Харків: СМІТ, 2004 – 544с. 8. Єжова Л.Ф. Алгоритмізація і програмування процедур обробки інформації. – К.: КНЕУ, 2000. – 152с. 9. Жураковський Ю.П., Полторак В.П. Теорія інформації та кодування: Підручник. – Київ: Вищ. шк., 2001. – 255с. 10. Новиков О.М., Грайворонський М.В., Основи захисту інформації в автоматизованих системах. Навч. пос. – К.: Академія, 2003. ***Електронні ресурси:*** електронний варіант лекцій, електронні презентації, будь-який електронний освітній контент (підручники, інтерактивні плакати, тести, завдання тощо).
Матеріально-технічне забезпечення	Навчально-методичний комплекс дисципліни, особистий конспект лекцій, презентації, методичні рекомендації до проведення лабораторних робіт, методичні рекомендації до виконання самостійних робіт.
Семестровий контроль, критерії оцінювання	**Форма семестрового контролю** – іспит. **Критерії оцінювання:** Оцінки **"ВІДМІННО"** заслуговує здобувач освіти, який дав повні і правильні відповіді на теоретичні питання щодо функціонування, побудови програм, що покращують та погіршують рівень захисту інформації у комп'ютерних системах ; виявив уміння

	логічно і послідовно обґрунтувати свої думки і висновки щодо вибору інструментів аналізу, вміє застосовувати теоретичні знання для розв'язування задач професійної направленості, вільно працює з технічною документацією, використовує знання з інших фахових дисциплін. Оцінки **"ДОБРЕ"** заслуговує здобувач освіти, який дав відповіді на всі теоретичні питання щодо захисту інформації у комп'ютерних системах, правильно використовує наукову термінологію, щодо захисту інформації у комп'ютерних системах операційних систем, але допустив при цьому помилки і недостатньо обґрунтував або пояснив вибір програмних засобів покращення рівня захисту інформації у комп'ютерних системах. Оцінку **"ЗАДОВІЛЬНО"** отримує здобувач освіти, який виявив знання програмного матеріалу, щодо захисту інформації в комп'ютерних системах в обсязі, необхідному для подальшого навчання, але виконав завдання на рівні репродуктивного відображення, допустив грубі помилки, не ув'язує свою відповідь з раніш отриманими даними, знаннями з інших предметів, при вирішенні практичних робіт використовує отримані знання поверхово. Оцінку **"НЕЗАДОВІЛЬНО"** отримує здобувач освіти, який допустив принципові помилки при відповіді на запитання, щодо захисту інформації в комп'ютерних системах; виявив серйозні вади в засвоєнні програмного матеріалу; дав відповіді на рівні нижче репродуктивного відображення, не виконав більше половини запропонованих завдань.
	Під час виконання лабораторних робіт та індивідуальних науково-дослідних завдань, проведення контрольних заходів здобувачі повинні дотримуватися правил академічної доброчесності, які визначено Кодексом доброчесності ВСП «Первомайський фаховий коледж НУК ім. адм. Макарова». Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Жодні форми порушення академічної доброчесності не толеруються. Виявлення ознак академічної недоброчесності в письмовій роботі здобувача є підставою для її незарахування викладачем, незалежно від масштабів плагіату
Циклова комісія	Циклова комісія «Комп'ютерних технологій».