СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Савченко
Віталій Анатолійович,
доктор технічних наук, професор.</td><td colspan="2">Контактна інформація лектора (e-mail), сторінка курсу в Moodle</td><td colspan="2">e-mail: ikbdut@gmail.com;
сторінка курсу в Moodle –
http://dn.dut.edu.ua/course/view.php?id=450#section-0</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">12 Інформаційні технології</td><td colspan="2">Рівень вищої освіти</td><td colspan="2">Доктор філософії</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">Кібербезпека</td><td colspan="2">Семестр</td><td colspan="2">1</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">Доктор філософії кібербезпеки</td><td colspan="2">Тип дисципліни</td><td colspan="2">Вибіркова компонента освітньо-наукової програми</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="6">За видами занять:</td></tr>
<tr><td>Лекцій</td><td>Семінарських занять</td><td>Практичних занять</td><td>Лабораторних занять</td><td>Самостійна підготовка</td></tr>
<tr><td></td><td>3</td><td>90</td><td>18</td><td>-</td><td>18</td><td>-</td><td>54</td></tr>
<tr><td colspan="9">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="9">Взаємозв’язок у структурно-логічній схемі</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="6">Методологія наукових досліджень у кібербезпеці. Сучасні методи управління інформаційною та кібербезпекою.</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6">Кваліфікаційна робота</td></tr>
<tr><td>Мета курсу:</td><td colspan="8">Формування знань та вмінь щодо оволодіння сучасними інформаційними й безпековими технологіями, застосування методів та засобів виявлення шкідливого програмного забезпечення інформаційної системи, а також їх критичного аналізу, виявлення недоліків та протиріч для постановки та вирішення наукових завдань і проведення досліджень</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Soft- skills / Загальні компетентності (ЗК)</td><td colspan="5">Hard-skills / Спеціальні компетентності (СК)</td></tr>
<tr><td colspan="4">ЗК-3. Знання інформаційних технологій</td><td colspan="5">ФК-4. Професійна компетентність
ФК-5. Загальнонаукова компетентність
ФК-6. Політехнічна компетентність
ФК-7. Інженерна компетентність</td></tr>
<tr><td colspan="9">Програмні результати навчання (ПРН)</td></tr>
<tr><td colspan="9">ПРН-5. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
ПРН-18. Уміти аналізувати існуючі технології, методи і засоби застосування шкідливого програмного забезпечення, нівелювання уразливостей мережевих та Web-ресурсів.
ПРН-19. Уміти проектувати перспективні технології виявлення шкідливого програмного забезпечення, а також уразливостей мережевих, Web- ресурсів, Web-додатків і застосовувати їх на практиці.
ПРН-20. Уміти визначати і вирішувати етичні питання при проведенні досліджень та пошуку відмінностей у шкідливому програмному забезпеченні, уразливостях мережевих та Web-ресурсів.
ПРН-26. Уміти використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки</td></tr>
</table>

мережевої інфраструктури об’єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.
ПРН-27. Бути здатним оволодіти спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та безпековими технологіями.

ОРГАНІЗАЦІЯНАВЧАННЯ

Тема,опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
РОЗДІЛ І			
Тема: Роль і місце технологій виявлення шкідливого програмного забезпечення в інформаційній системі забезпечення кібербезпеки. ***Знати***: основні поняття щодо безпеки інформаційної системи, поняття «шкідливе програмне забезпечення», класифікація технологій виявлення вірусів, класифікація комп'ютерних вірусів, способи захисту від вірусів, особливості технологій протидії шкідливим програмам. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7. ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Лекція 1 2 год	6	Лекція-візуалізація
Тема: Шкідливе програмне забезпеченння. Технології протидії шкідливим програмам та завідомо фальшивому програмному забезпезпеченню. ***Знати***: політику безпеки, сучасні AV-технології; основні класи шкідливих програм і потенційно небажаних програм, приклади; відомі технології виявлення ознак шкідливого програмного забезпечення в інформаційній системі; технології протидії від шкідливого програмного забезпечення. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7. ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Лекція 2 2 год	6	Лекція-візуалізація

Тема: Стандартні антивірусні системи. Комп'ютерні віруси. Основні ознаки шкідливого програмного забезпечення. ***Знати:*** політику безпеки, класифікацію комп'ютерних вірусів, їх систематизацію; класифікацію технологій виявлення вірусів; способи захисту від вірусів. особливості технологій протидії шкідливим програмам. ***Вміти***: аналізувати прояви та ознаки шкідливого ПЗ; визначати види шкідливого ПЗ: комп'ютерний вірус, троянська програма, мережевий черв'як, руткіти; проводити моніторинг факту наявності шкідливого ПЗ. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7. ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** . 1-19.	Самостійна робота 1 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередньою лекцією.
Тема: Статистика розвитку шкідливого та руйнуючого програмного забезпечення. Фішинг ***Знати***: політику безпеки, визначення фішингу, види фішингових атак, виявлення спроби фішингу**,** основні схеми фішингових пасток; технології захисту від фішинг-атак. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7. ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Лекція 3 2 год	6	Лекція-візуалізація .
Тема: Банківські загрози Класифікації та види антивірусного програмного забезпечення. ***Знати***: найпоширеніші види антивірусного ПЗ, класифікація банківських атак; методи захисту від банківських атак; актуальні проблеми, методи "соціальної інженерії", застосування механізмів безпеки, які реалізують прийняту політику безпеки. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7. ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Лекція 4 2 год	6	Лекція-візуалізація

Тема: Особливості дослідження ознак шкідливого програмного забезпечення. Нормативно-правова база, міжнародні документи в напряму забезпечення безпеки. ***Знати:*** політику безпеки, зміст оперування понятійним апаратом щодо безпеки інформаційної системи, класифікацію технологій виявлення вірусів, особливості розслідування виявлення комп'ютерних вірусів при знаходженні в інформаційній системі шкідливого програмного забезпечення, відомі технології виявлення ознак шкідливого програмного забезпечення. ***Вміти:*** застосовувати політику безпеки, законодавчу, нормативно-правову базу щодо виявлення ознак шкідливого та руйнівного програмного забезпечення, ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Практичне заняття 1 2 год		Набуття навичок роботи з спеціалізованими програмами для дослідження технологій, які дозволяють покращити виявлення ознак шкідливого програмного забезпечення. Практичне застосування законодавчої, нормативно-правової бази щодо виявлення в інформаційній системі шкідливого програмного забезпечення.
Тема: Комп'ютерні віруси. ***Знати:*** основні поняття та визначення; комп'ютерні віруси: файлові віруси, завантажувальні віруси, резидентні віруси, поліморфні віруси, стелс-віруси, макро-віруси, Spyware, Ad-ware, Maleware, мережеві хробаки та інші види вірусів; класифікацію технологій виявлення вірусів, ***Вміти:*** визначати та виявляти ознаки різновидів комп'ютерних вірусів. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Самостійна робота 2 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекціями та практичним заняттям. Отримати навички виявлення ознак різновидів комп'ютерних вірусів.
Тема: Статичний аналіз шкідливих програм. Виявлення та елементи захисту від шкідливого програмного забезпечення. ***Знати:*** політику безпеки, методи аналізу коду, зміст **с**татичного аналізу шкідливих програм; інструменти та шаблони виявлення, що використовуються при статичному аналізу шкідливих программ, ефективні програми	Практичне заняття 2 2 год		Набуття навичок роботи з спеціалізованими програмами для практичного проведення **с**татичного аналізу шкідливих програм, які дозволяють поліпшити стан виявлення та захист від шкідливого програмного забезпечення.

боротьби з вірусами; виявлення та захист від шкідливих программ. ***Вміти:*** застосовувати **с**татичний аналіз діагностування комп'ютерних систем на наявність шкідливого програмного забезпечення. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.			
Тема: Методи підвищення достовірності антивірусного діагностування комп'ютерних систем. ***Знати:*** поширені методи діагностування, що використовуються в сучасних антивірусних програмних засобах: емулятор коду, криптоаналіз, статичний аналіз, евристичний аналізатор, мультиагентна система, поведінкове блокування та інші. ***Вміти:*** проводити діагностування комп'ютерних систем сучасними антивірусними програмними засобами. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Самостійна робота 3 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекціями та практичними заняттями. Проводити діагностування комп'ютерних систем сучасними антивірусними програмними засобами.
Тема: Динамічний аналіз шкідливих програм. ***Знати:*** політику безпеки, методи аналізу коду, зміст динамічного аналізу шкідливих програм; розширений динамічний аналіз шкідливих програм; інструменти виявлення, що використовуються при динамічному аналізу шкідливих программ, ефективні програми боротьби з вірусами; клас программ - емулюючі налагоджувачі; виявлення та захист від шкідливих программ. ***Вміти:*** застосовувати **с**татичний аналіз діагностування комп'ютерних систем на наявність шкідливого програмного забезпечення. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Практичне заняття 3 2 год		Набуття навичок роботи з спеціалізованими програмами для практичного проведення динамічного аналізу шкідливих програм, які дозволяють поліпшити стан виявлення та захист від шкідливого програмного забезпечення.

Тема: Підходи до виявлення загроз на інформаційні ресурси. ***Знати:*** методи пошуку шкідливого ПЗ за допомогою антивірусних програм; методи виявлення шкідливого ПЗ за допомогою професійних пакетів антивірусних інструментів: сканування; евристичне сканування; антивірусний моніторинг; імунізація. ***Вміти:*** проводити пошук шкідливого ПЗ за допомогою антивірусних програм; застосовувати методи виявлення ШПЗ за допомогою професійних пакетів антивірусних інструментів. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Самостійна робота 4 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь за попередніми лекціями та практичними заняттями.
Тема: Аналіз проломів в програмному забезпеченні ***Знати:*** методи доступу до уразливого програмного забезпечення, проведення аналізу експлойтів (віддалений експлойт , локальний експлойт); методи захисту програмного забезпечення, інструментальні засоби (статичні аналізатори вихідного коду програми). ***Вміти:*** проводити аналіз експлойтів (фрагментів коду, які використовують вразливості в ПЗ та ОС для здійснення атаки на систему). ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Практичне заняття 4 2 год		Набуття навичок роботи з спеціалізованими програмами для практичного проведення аналізу проломів в програмному забезпеченні, які дозволяють поліпшити стан виявлення та захист від шкідливого програмного забезпечення.
РОЗДІЛ II			

Тема: Ботнети. ***Знати:*** політику безпеки; визначення та зміст ботнетів; методи виявлення ботнет-програм; захист від ботнетів; блокування шкідливого програмного забезпечення, брандмауер. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:***1-8.	Лекція 5 2 год	6	Лекція-візуалізація
Тема: Зворотний інжиніринг x86/ARM ***Знати:*** статичний аналіз програм з використанням дизасемблера (інтерактивні, автоматичні), як зручного інструмента для дослідження програм та виявлення шкідливого контенту; додатки, що використовують основи технології дизасемблювання. ***Вміти:*** освоїти навички статичного аналізу програм з використанням дизасемблера, користуватись додатками, що використовують основи технології дизасемблювання. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Практичне заняття 5 2 год		Набуття навичок роботи з спеціалізованими програмами для практичного проведення статичного аналізу програм з використанням дизасемблера для виявлення шкідливого контенту, освоєння додатків, що використовують основи технології дизасемблювання.
Тема: Дослідження достовірності антивірусного діагностування комп'ютерних систем. Класичні комп'ютерні віруси. ***Знати:*** сучасні техніки для проведення досліджень за напрямом захисту інформації, організацію й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів; класичні комп'ютерні віруси: файлові віруси, завантажувальні віруси, макровіруси, скриптові віруси, класичні мережеві хробаки, «троянські коні»; перспективні засоби захисту. ***Вміти:*** проводити сканування для пошуку відомих	Самостійна робота 5 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекціями та практичними заняттями. Набуття навичок приймати рішення при розв'язанні практичних завдань з метою уникнення поширення ШПЗ.

вірусів, що відповідають визначенню у словнику вірусів, приймати рішення з метою уникнення поширення ШПЗ. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.			
Тема: Мобільбні загрози ***Знати:*** механізми заходів безпеки на пристроях компанії Apple, додатки Apple Watchr (механізм авторизації користувачів, нова версія операційної системи тощо); принципи безпеки доступні в компанії Apple; головні загрози для мобільних пристроїв: атаки через веб-додатки та мережі; шкідливе ПЗ, аналоги класичних вірусів, троянських програм і черв'яків для мобільних; атаки з використанням соціальної інженерії; захоплення ІТ-ресурсів; витік даних та загрози цілісності даних. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:***. 1-19.	Лекція 6 2 год	6	Лекція-візуалізація
Тема: Покращене розпакування. ***Знати:*** огляд відомих способів аналізу шкідливого програмного забезпечення; систему основних міток класифікації ознак; проведення динамічного аналізу ШПЗ та статичного аналізу ШПЗ, переваги та недоліки; алгоритми машинного навчання; компоненти статичного аналізу: багаторазове сканування антивірусом; визначення типу файлу та гешування; пошук по рядкам; перевірки відомостей у PE- заголовку; аналіз дизасемблерного коду. ***Вміти:*** освоїти навички визначення наявності виконавчих файлів пакувальника для його ідентифікації. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Практичне заняття 6 2 год		Набуття навичок роботи з спеціалізованими програмами для практичного вирішення завдання виявлення наявності виконавчих файлів пакувальника для його ідентифікації.

Тема: Дослідження достовірності антивірусного діагностування комп'ютерних систем за допомогою статичного та динамічного аналізу шкідливих програм. Порівняльний аналіз. ***Знати:*** загальну структуру системи аналізу; класифікацію характерних ознак; підходи до побудови системи аналізу шкідливого програмного забезпечення; огляд відомих способів аналізу шкідливого ПЗ;; способи проведення динамічного аналізу ШПЗ та статичного аналізу ШПЗ, переваги та недоліки. ***Вміти:*** освоїти перспективні засоби виявлення шкідливого ПЗ та захисту від проникнення. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Самостійна робота 6 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекціями та практичними заняттями. Освоєння перспективних засобів виявлення шкідливого ПЗ та захисту від проникнення.
Тема: Атаки в соціальних мережах. Розвиток технологій міжмережевих екранів. Нові покоління міжмережевих екранів. ***Знати:*** політику безпеки, механізми заходів захисту від атак з використанням соціальної інженерії, план дій, рішень з безпеки і подій для виявлення та знешкодження потенційних загроз. Призначення міжмережевих екранів (Firewall, Brandmauer, брандмауер), типи міжмережевих екранів (апаратний, програмний), їх функції; види міжмережевих екранів (пакетні фільтри (packet filter), сервера прикладного рівня (application gateways); сервера рівня з'єднання (circuit gateways). ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Лекція 7 2 год	6	Лекція-візуалізація
Тема : ***Руткіти.*** ***Знати:*** огляд відомих способів аналізу шкідливого програмного забезпечення; найвідоміші руткіти і їх поширення: механізми проникнення, маскування руткітів на			

ПК та методи захисту від них, антивірус, що має функцію пошуку і руткіта, спеціальні антивірусні програми або утиліти, які сканують систему тільки на наявність руткітів. ***Вміти:*** освоїти навички виявлення наявності руткітів у системі, володіти методами захисту від них, засобами видалення руткітів. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Практичне заняття 7 2 год		Набуття навичок роботи з спеціалізованими програмами для практичного вирішення завдання виявлення наявності руткітів у системі, володіти методами захисту від них, засобами видалення руткітів.
Тема: Дослідження методів та засобів запобігання вторгнень ШПЗ. Прийняття рішень з метою уникнення поширення ШПЗ. ***Знати:*** огляд відомих способів аналізу шкідливого програмного забезпечення; механізми проникнення, методи виявлення вірусів: пошук сигнатур, евристичний аналіз, контроль незмінності об'єктів; антивірусні засоби: антивірусні сканери, антивірусні монітори, антивірусні фільтри, поліморфізм (модифікація коду вірусу), утиліти ***Вміти:*** освоїти навички виявлення наявності ШПЗ у системі, володіти методами захисту від них, засобами видалення. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Самостійна робота 7 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекціями та практичними заняттями.Набуття навичок приймати рішення при розв'язанні практичних завдань виявлення наявності ШПЗ у системі, методами захисту від вторгнень, засобами видалення.
Тема: Методи боротьби з шкідливим програмним забезпеченням засобами операційної системи. ***Знати:*** політику безпеки, методи боротьби з шкідливим програмним забезпеченням засобами операційної системи. Операційна система Ms Dos, її утиліти та команди в боротьбі проти вірусів. Внутрішні засоби Windows в боротьбі проти шкідливого програмного забезпечення. Програми сторонніх виробників. Linux-віруси. MacOSX-віруси Особливості операційних систем щодо стійкості до шкідливого програмного забезпечення.	Лекція 8 2 год	6	Лекція-візуалізація

Формування компетенцій: ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.			
Тема: Аналіз шкідливого ПЗ на ОС Android. ***Знати:*** політику безпеки***,*** відомі шкідливі програми ОС Android; функції безпеки ОС Android, захист від шкідливого програмного забезпечення, фішингу та вразливостей; захисні заходи протистояння найрізноманітнішим атакам: оновлення, антивірусне ПЗ, двофакторна аутентифікація, паролі з криптозахистом; дизассемблерування. ***Вміти:*** освоїти навички в дизассемблеруванні та відлагодженні шкідливих програм для ОС Android ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Практичне заняття 8 2 год		Набуття навичок роботи з спеціалізованими програмами для практичного вирішення завдання дизассемблерування та відлагодження шкідливих програм для ОС Android
Тема: Дослідження перспективних методів та засобів забезпечення кібербезпеки інформаційної системи. ***Знати:*** політику безпеки***,*** перспективні методи виявлення вірусів, існуючі та потенційні загрози у сфері програмного захисту інформації; виявлення та ліквідацію шкідливих програм з використанням сучасних антивірусних програм; світовий досвід щодо програмного захисту інформації. ***Вміти:*** приймати рішення при розв'язанні практичних проблем забезпечення кібербезпеки інформаційної системи ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Самостійна робота 8 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекціями та практичними заняттями. Набуття навичок приймати рішення при розв'язанні практичних проблем забезпечення кібербезпеки інформаційної системи
Тема: Виявлення шкідливих програм. ***Знати***: політику безпеки***,*** основи виявлення шкідливих програм, відомі практики виявлення шкідливих програм, методи аналізу коду шкідливих програм; існуючі та			

потенційні загрози у сфері програмного захисту інформації; виявлення та ліквідацію шкідливих програм з використанням сучасних антивірусних програм; світовий досвід щодо програмного захисту інформації для його впровадження в Україні. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Лекція 9 2 год	6	Лекція-візуалізація
Тема: Збір даних в області виявлення та аналізу шкідливого ПЗ ***Знати:*** політику безпеки***,*** основи виявлення шкідливого програмного ПЗ, збір даних в області виявлення шкідливого ПЗ, відомі практики виявлення шкідливого ПЗ, методи та механізми заходів захисту від шкідливого програмного забезпечення, методи аналізу шкідливих програм; існуючі та потенційні загрози у сфері програмного захисту інформації; виявлення та ліквідацію шкідливих програм з використанням сучасних антивірусних програм; світовий досвід щодо програмного захисту інформації. ***Вміти:*** проводити дослідження та приймати рішення при розв'язанні практичних завдань виявлення шкідливих програм. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-5, ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:*** 1-19.	Практичне заняття 9 2 год		Набуття навичок роботи з спеціалізованими програмами для проведення дослідження та прийняття рішення при розв'язанні практичних завдань виявлення шкідливих програм. .
Тема: Дослідження методів виявлення та ліквідації шкідливих програм з використанням сучасних антивірусних програм. Вивчення світової практики щодо захисту вторгнень ШПЗ. ***Знати*:** політику безпеки***,*** основи виявлення шкідливих програм, відомі практики виявлення шкідливих програм, методи аналізу коду шкідливих програм; існуючі та			

потенційні загрози у сфері програмного захисту інформації; виявлення та ліквідацію шкідливих програм з використанням сучасних антивірусних програм; світову практику щодо захисту вторгнень ШПЗ. ***Вміти:*** проводити дослідження та приймати рішення при розв'язанні практичних проблем виявлення та ліквідації шкідливих програм з використанням сучасних антивірусних програм. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7. ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27. ***Рекомендовані джерела:***. 1-19.	Самостійна робота 9 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям. Набуття навичок роботи з спеціалізованими програмами для проведення дослідження та прийняття рішення при розв'язанні практичних завдань виявлення та ліквідації шкідливих програм з використанням сучасних антивірусних програм.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп'ютерне обладнання, мережа Інтернет, ауд. 420 - центр компетенцій IBM (Кіберполігон), система управління подіями та інцидентами кібербезпеки IBM Security QRadar SIEM: набір серверів ServerDellPER530Ю, програмні комплекси Nessus Professional, Tenable.sc, IBM QRadar SIEM та IBM QRadar Vulnerability Manager.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. .Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів – Київ: ДУТ ННІЗІ, 2020. – 167 с.
2. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
3. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний, Н.В. Лукова-Чуйко/ – К. : ДУТ – КНУ, 2016. – 178 с.
4. Богуш В.М., Довидьков О.А. Теоретичні основи захищених інформаційних технологій - К.: ДУІКТ, 2006. - 508 с.
5. Бурячок В. Л. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем / В. Л. Бурячок, О. Г. Корченко, Л. В. Бурячок // Захист інформації. – 2012. – № 4(57). – С. 5–12
6. Мінаєв С.А. Принципи організації протидії шкідливим програмам в інформаційно-телекомунікаційних системах на основі оптимізації їх функціонування / В. А. Мінаєв, С. В. Скриль // Радіосистеми. – Вип. 47 «Радіотехнічні і інформаційні системи охорони і безпеки». – Радіотехніка. – 2013. – №9. – С. 71-72.
7. Technical Guide to Information Security Testing and Assessment. Recommendations of the National Institute of Standards and Technology. Karen Scarfone. Murugiah Souppaya. Amanda Cody. Angela Orebaugh. NIST Special Publication 800-115. (Sep. 2008). 80 p. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
8. Park Foreman. Vulnerability Management. Second Edition. CRC Press Taylor & Francis Group, 2019. 330 p
9. Drapkin S. Application Securityin .NET Succinctly Syncfusion, 2017. – 103 p.
10. ISO/IEC 27001:2013. InformationTechnology. SecurityTechniques. InformationSecurityManagementSystems. Requirement
11. ISO/IEC 27035:2011«Information technology. Securitytechniques. Informationsecurityincidentmanagement.
12. ApplicationSecurityVerification Standard 4:.0 https://www.owasp.org/images/d/d4/OWASP_Application_Security_Verification_Standard_4.0-en.pdf
13. NationalInstituteofStandardsandTechnology: https://nvd.nist.gov/vuln-metrics/cvss

14. MITRE CommonWeaknessEnumeration: http://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html
15. OpenWebApplicationSecurity Project: https://www.owasp.org/index.php/Category: OWASP_Code_Review_Project
16. Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. Paul Cichonski. Tom Millar. Tim Grance. Karen Scarfone. Special Publication 800-61 Revision 2 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
17. Tom Palmaers. Implementing a vulnerability management process. SANS Institute. Accepted: 03/23/2013. 24 p. https://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180
18. IBM QRadar Vulnerability Manager 7.4.0. User Guide. 152 p. https://www.ibm.com/docs/en/SS42VS_7.4/pdf/b_qvm_ug.pdf.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо аспірант відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації аспірант повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату аспірант отримує за завдання 0 балів.
- Аспірант, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни аспірант видаляється з заняття, за заняття отримує 0 балів.

* КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання аспірантом 54 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,5 бала
	• звіт про виконання практичного завдання	за кожен звіт максимум 1 бал
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	Звільняється від заліку
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Залік проходить у письмовій формі.	46 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	Критерії оцінювання	Рівень компетентності	Оцінка /*запис в екзаменаційній відомості*
90-100	Аспірант демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або аспірант проявляє невпевненість в	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції аспіранта в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні питань, що відносяться до дисципліни, яка вивчається	Відмінно / Зараховано (А)

	тлумаченні теоретичних положень чи складних практичних завдань.		
82-89	Аспірант демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналізможливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення	**Достатній** Забезпечує аспіранту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно зприкладами, що розглянуті при вивченні дисципліни	Добре / Зараховано (B)
75-81	Аспірант в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
64-74	Аспірант засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє зміст стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Аспірант має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, аспірант з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	.Аспірант може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни аспірант виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у аспіранта відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX), *в залікову книжку не проставляється*
1-34	Аспірант повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Аспірант не допущений до здачі заліку.	**Незадовільний** Аспірант не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F), в *залікову книжку не проставляється*