Інформаційний пакет освітніх компонент навчального плану
освітньо-професійної програми Інформаційна та кібернетична безпека
(назва)

Освітнього рівня третій (освітньо-науковий)

Спеціальності 125 «Кібербезпека»

Галузь знань 12 «Інформаційні технології»

1. Назва освітньої компоненти Технології виявлення уразливостей мережевих ресурсів
(назва дисципліни)

2. Тип основна, вибіркова (вказати) вибіркова

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18		18		54
4. Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	Прикладна загальна теорія систем інформаційної безпеки						
Освітні компоненти для яких є базовою	Технології забезпечення безпеки мережевої інфраструктури						
5. Компетенції відповідно до ОНП							
Компетенції відповідно до ОНП							
Знати			**Вміти**				
ПК-6. Політехнічна компетентність – знання загальних (методологічних, історичних, економічних, ергономічних тощо) питань безпекової сфери, принципів дії і будови основних функціональних органів інформаційних систем; здатність до оволодіння спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними			ПК-5. Загальнонаукова компетентність – здатність до накопичення професійних вмінь та навичок (діагностування й інтерпретування ситуацій, планування та здійснення наукових досліджень, викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційних технологій та захисту інформації); здатність до генерування нових знань з теорії захисту інформації та інформаційної				

та без пековими технологіями; здатність до застосування різноманітних, професійно профільованих знань і практичних навичок у сфері захисту інформації.	безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки; здатність до застосування нових знань у професійній діяльності (проектній, винахідницькій та раціоналізаторській роботі) тощо.
	ПК-7. Інженерна компетентність – здатність до виробничо-технологічної діяльності (розробки та впровадження інноваційних технологій інформаційної безпеки, вибору технології ІБ, устаткування та засобів, використання інформаційних технологій; розробки програм і методик випробувань систем інформаційної та кібербезпеки); здатність до організаційно-управлінської діяльності (організації процесу створення та надання інфокомунікаційних послуг); здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем, до обробки та перетворення інформації тощо.
Компетенції відповідно до вимог роботодавців	

6. Результати навчання відповідно до ОНП

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 та Web-ресурсів й застосовувати їх на практиці.

ПРН-20. Уміти визначати і вирішувати етичні питання при проведенні досліджень та пошуку відмінностей у шкідливому програмного забезпечення, уразливостях мережевих та Web-ресурсів.

ПРН-23. Бути здатним генерувати нові знання з теорії захисту інформації та інформаційної безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки.

7. План вивчення освітньої компоненти

Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
Розділ 1						
	Лекція 1	Основи забезпечення кібербезпеки сучасного підприємства. Роль і місце технологій виявлення вразливостей	1. Корпоративна інформаційна система як об’єкт захисту. Превентивні, детективні та коректівні заходи забезпечення		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479

		мережевих ресурсів у системі забезпечення кібербезпеки.	кібербезпеки підприємства. Подія безпеки. Поняття уразливості. 2. Класифікація вразливостей. Джерела даних щодо вразливостей. Прийняті позначення вразливостей.			
	Лекція 2	Основи інформаційно-аналітичної діяльності фахівців з кібербезпеки.	1. Основи інформаційно-аналітичної діяльності фахівців з кібербезпеки. Зміст інформаційно-аналітичної діяльності фахівців з кібербезпеки. 2. Методологія аналітичних досліджень кіберінцидентів. Основні методи аналітичної діяльності фахівців з кібербезпеки. Інформаційні джерела для здійснення аналітичної діяльності фахівців з кібербезпеки.		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Лекція 3	Основи технології тестування на проникнення (Penetration Testing).	1. Цілі тестування на проникнення. Види тестування на проникнення та їх зміст. Принципові відмінності тестування на проникнення та сканування вразливостей. 2. Зміст тестування рівня додатків та мережевого рівня. Зміст тестування на проникнення сегментів мережі та на предмет соціальної інженерії. 3. Звітність за результатами		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479

			тестування на проникнення. 4. Технологія проведення тестування на проникнення. 5. Приклади застосування технології тестування на проникнення для різних варіантів.			
	Лекція 4	Технології виявлення вразливостей мережевих ресурсів. Загальні положення.	1. Технологія сканування мережі. Визначення топології мережі. Розміщення сканерів уразливостей. Визначення цілей сканування. Стратегії сканування. Користувальницькі вимоги. 2. Методологія сканування: параметри розкладу активного сканування; конфігурація політики сканування; налаштування політики сканування.		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Лекція 5	Основи застосування сканера вразливостей Nessus Professional. Установки сканування та політик.	Установки сканування та політик. Basic Scan Settings. Scan Targets. Discovery Scan Settings. Assessment Scan Settings. Report Scan Settings. Advanced Scan Settings. Credentials.		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Лекція 6	Основи застосування IBM QRadar Vulnerability Manager. Призначення та можливості програмного комплексу.	1. Призначення та можливості програмного комплексу IBM QRadar Vulnerability Manager. Функціональні компоненти IBM QRadar Vulnerability Manager. 2. Види перевірок на		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479

			вразливість, які здійснюються за допомогою IBM QRadar Vulnerability Manager. 3. Порядок інсталяції та розгортання IBM QRadar Vulnerability Manager.			
	Лекція 7	Основи застосування IBM QRadar Vulnerability Manager. Налаштування сканування вразливостей та кращі практики.	1. Типи політики сканування. Тривалість сканування та сканування портів. Налаштування конфігурації пошуку активів. Сканування веб-додатків. Розміщення сканера в мережі. Динамічне сканування. Пропускна здатність мережі для одночасного сканування активів. Карти мережевого інтерфейсу на сканерах. 2. Огляд управління вразливістю. Повідомлення про сканування вразливості. Запуск сканування нових активів.		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Лекція 8	Основи застосування IBM QRadar Vulnerability Manager. Керування виявленими вразливостями.	1. Керування виявленими вразливостями. Common Vulnerability Scoring System (CVSS). Дослідження показників ризику вразливості. Конфігурування індивідуальних оцінок ризику для вразливості. 2. Дослідження даних про вразливість. Уразливості мережі. Вразливості активів.		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479

			Уразливості відкритих служб. Дослідження історії вразливості. Зменшення кількості помилково-позитивних вразливостей. Дослідження активів та вразливих груп з високим ризиком. Визначення пріоритетності вразливості шляхом застосування політики щодо ризику.			
	Лекція 9	Технологія управління вразливостями в корпоративній інформаційній системі з використанням IBM QRadar SIEM та Tenable.sc.	1. Огляд рішення Tenable.sc. 2. Додавання сканування Tenable.sc до IBM QRadar SIEM. 3. Планування сканування вразливості в IBM QRadar SIEM. 4. Перегляд стану сканування на вразливість в IBM QRadar SIEM. 5. Підтримувані сканери вразливості в IBM QRadar SIEM.		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Практичне заняття 1	Тема: Впровадження процесу управління вразливостями.		1. Процес управління вразливостями. 1.1. Мета управління вразливістю. 1.2. Ролі та обов'язки посадових осіб. 1.3. Процес управління вразливостями. 2. Застосування методики управління вразливостями: приклад. 2.1. Підготовчий етап.	http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479

				2.2. Початкове сканування вразливостей. 2.3. Визначення коригуючих дій або прийняття ризику. 2.4. Здійснення коригувальних дій. 2.5. Перевірка (Ресканування).		
	Практичне заняття 2	Тема: Стратегії сканування, які рекомендують Tenable.		1. Методологія сканування (Scanning Methodology). Параметри активного розкладу сканування (Active Scan Schedule Options). Конфігурація політики сканування (Scan Policy Configuration). Налаштування політики сканування (Scan Policy Settings). 2. Конфігурація політики сканування (Scan Policy Configuration). 3. Налаштування політики сканування (Scan Policy Settings).	http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Практичне заняття 3	Тема: Основи застосування сканера вразливостей Nessus Professional. Основи сканування.		1. Шаблони сканування та політики (Scan and Policy Templates). 2. Шаблони сканера (Scanner Templates). 3. Налаштування сканування та політики (Scan and Policy Settings).	http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Практичне	Тема: Основи			http://dl.dut.edu	http://dl.dut.edu.ua/c

	заняття 4	застосування сканера вразливостей Nessus Professional. Налаштування сканування та політики.			.ua/course/view.php?id=479	ourse/view.php?id=479
	Практичне заняття 5	Тема: Основи застосування сканера вразливостей Nessus Professional. Налаштування сканування оцінки.			http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Практичне заняття 6	Тема: Основи застосування сканера вразливостей Nessus Professional. Аналіз результатів сканування.			http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Практичне заняття 7	Тема: Основи застосування IBM QRadar Vulnerability Manager. Налаштування сканування вразливостей та кращі практики.			http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Практичне заняття 8	Тема: Основи застосування IBM QRadar Vulnerability Manager. Керування вразливостями.			http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479

	Практичне заняття 9	Тема: Основи застосування IBM QRadar Vulnerability Manager. Інтеграція зі сканерами Tenable.io та Tenable.sc.			http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Самостійна робота 1	Основи забезпечення кібербезпеки сучасного підприємства. Роль і місце технологій виявлення вразливостей мережевих ресурсів у системі забезпечення кібербезпеки.	1. Корпоративна інформаційна система як об’єкт захисту. Превентивні, детективні та коректівні заходи забезпечення кібербезпеки підприємства. Подія безпеки. Поняття уразливості. 2. Класифікація вразливостей. Джерела даних щодо вразливостей. Прийняті позначення вразливостей.	1. Здійснення інформаційно-аналітичної діяльності фахівців з кібербезпеки. 2. Методологія аналітичних досліджень кіберінцидентів. Основні методи аналітичної діяльності фахівців з кібербезпеки. Інформаційні джерела для здійснення аналітичної діяльності фахівців з кібербезпеки.	http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Самостійна робота 2	Основи інформаційно-аналітичної діяльності фахівців з кібербезпеки.	1. Основи інформаційно-аналітичної діяльності фахівців з кібербезпеки. Зміст інформаційно-аналітичної діяльності фахівців з кібербезпеки. 2. Методологія аналітичних досліджень кіберінцидентів. Основні методи аналітичної діяльності фахівців з кібербезпеки. Інформаційні джерела для здійснення аналітичної діяльності		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479

			фахівців з кібербезпеки.			
	Самостійна робота 3	Основи технології тестування на проникнення (Penetration Testing).	1. Цілі тестування на проникнення. Види тестування на проникнення та їх зміст. Принципові відмінності тестування на проникнення та сканування вразливостей. 2. Зміст тестування рівня додатків та мережевого рівня. Зміст тестування на проникнення сегментів мережі та на предмет соціальної інженерії. 3. Звітність за результатами тестування на проникнення. 4. Технологія проведення тестування на проникнення. 5. Приклади застосування технології тестування на проникнення для різних варіантів.	1. Шаблони сканування та політики (Scan and Policy Templates). 2. Шаблони сканера (Scanner Templates). 3. Налаштування сканування та політики (Scan and Policy Settings).	http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Самостійна робота 4	Технології виявлення вразливостей мережевих ресурсів. Загальні положення.	1. Технологія сканування мережі. Визначення топології мережі. Розміщення сканерів уразливостей. Визначення цілей сканування. Стратегії сканування. Користувальницькі вимоги. 2. Методологія сканування: параметри розкладу активного сканування; конфігурація політики сканування; налаштування політики сканування.		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479

	Самостійна робота 5	Основи застосування сканера вразливостей Nessus Professional. Установки сканування та політик.	Установки сканування та політик. Basic Scan Settings. Scan Targets. Discovery Scan Settings. Assessment Scan Settings. Report Scan Settings. Advanced Scan Settings. Credentials.		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Самостійна робота 6	Основи застосування IBM QRadar Vulnerability Manager. Призначення та можливості програмного комплексу.	1. Призначення та можливості програмного комплексу IBM QRadar Vulnerability Manager. Функціональні компоненти IBM QRadar Vulnerability Manager. 2. Види перевірок на вразливість, які здійснюються за допомогою IBM QRadar Vulnerability Manager. 3. Порядок інсталяції та розгортання IBM QRadar Vulnerability Manager.		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Самостійна робота 7	Основи застосування IBM QRadar Vulnerability Manager. Налаштування сканування вразливостей та кращі практики.	1. Типи політики сканування. Тривалість сканування та сканування портів. Налаштування конфігурації пошуку активів. Сканування веб-додатків. Розміщення сканера в мережі. Динамічне сканування. Пропускна здатність мережі для одночасного сканування активів. Карти мережевого інтерфейсу на сканерах. 2. Огляд управління		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479

			вразливістю. Повідомлення про сканування вразливості. Запуск сканування нових активів.			
	Самостійна робота 8	Основи застосування IBM QRadar Vulnerability Manager. Керування виявленими вразливостями.	1. Керування виявленими вразливостями. Common Vulnerability Scoring System (CVSS). Дослідження показників ризику вразливості. Конфігурування індивідуальних оцінок ризику для вразливості. 2. Дослідження даних про вразливість. Уразливості мережі. Вразливості активів. Уразливості відкритих служб. Дослідження історії вразливості. Зменшення кількості помилково-позитивних вразливостей. Дослідження активів та вразливих груп з високим ризиком. Визначення пріоритетності вразливості шляхом застосування політики щодо ризику.		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479
	Самостійна робота 9	Технологія управління вразливостями в корпоративній інформаційній системі з використанням IBM QRadar SIEM та Tenable.sc.	1. Огляд рішення Tenable.sc. 2. Додавання сканування Tenable.sc до IBM QRadar SIEM. 3. Планування сканування вразливості в IBM QRadar SIEM. 4. Перегляд стану сканування на вразливість в IBM QRadar SIEM.		http://dl.dut.edu.ua/course/view.php?id=479	http://dl.dut.edu.ua/course/view.php?id=479

			5. Підтримувані сканери вразливості в IBM QRadar SIEM.			
Розділ 2						
	…	…				
Розділ …						
	…	…				
8. Мова вивчення освітньої компоненти						
(українська, англійська, розділи, що викладаються англійською мовою)						
українська, англійська						
9. Інформаційне забезпечення освітньої компоненти						
Рекомендовані джерела та інші навчальні ресурси: вказати підручники, навчальні посібники не пізніше 2010 року видання, які є у нас у бібліотеці на державній мові; електронні ресурси, посилання, електронна бібліотека ДУТ, іншомовні джерела						
Основна						
1. Бурячок В.Л. 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.						
2. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2011. – 31 с.						
3. Рибка С.В. Кіберпростір, управління інфраструктурою, кібербезпека / С.В. Рибка, Є.В. Кільчицький, О.М. Післегін // Стратегічна панорама. – 2015. – № 1. – С. 126–134.						
4. MITRE. Ten Strategies of a World-Class Cybersecurity Operations Center. /Carson Zimmerman -The MITRE Corporation, 2014. – 346 p.						
5. Захарова В. І. Основи інформаційно-аналітичної діяльності [текст]: навч. посіб. / Захарова В. І., Філіпова Л. Я. – К.: «Центр учбової літератури», 2013. – 336 с.						
6. Варенко В.М. Інформаційно-аналітична діяльність: Навч. посіб. / В.М. Варенко. – К.: Університет «Україна», 2014. – 417 с.						
7. Бондарев В.В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства : учебное пособие / В. В. Бондарев. – Москва : Издательство МГТУ им. Н. Э. Баумана, 2017. – 225, [3] с. : ил.						
8. Руководство по реагированию на инциденты информационной безопасности. Управление технологических решений. Версия 1.0 (07.02.2017) [Електронний ресурс]. Режим доступу: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2017/08/21181001/Incident_Response_Guide_rus.pdf.						
9. Michael J. Chapple, David Seid. CompTIA Cybersecurity Analyst (CSA+) Study Guide: Exam CS0-001. Sybex, 2017 – 552 p.						
10. Information Supplement: Penetration Testing Guidance. Penetration Test Guidance Special Interest GroupPCI Security Standards Council. 2015. –						

43p.

11. 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. [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.

12. 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 [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

13. IBM QRadar Version 7.3. Planning and Installation Guide. January 2018 [Електронний ресурс] – Режим доступу: http://www.redbooks.ibm.com/redbooks/pdfs/sg248412.pdf.

14. IBM Security QRadar.Version 7.3.2. Administration Guide. [Електронний ресурс]. Режим доступу: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_admin_guide.pdf?view=kc.

15. IBM Security QRadar. Version 7.3.2. Architecture and Deployment Guide [Електронний ресурс] – Режим доступу: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/b_siem_deployment.pdf?view=kc.

16. IBM Security QRadar. Version 7.3.2. User Guide [Електронний ресурс]. Режим доступу: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_users_guide.pdf?view=kc.

17. IBM QRadar Vulnerability Manager. Version 7.3.2. User Guide [Електронний ресурс]. Режим доступу: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/b_qvm_ug.pdf?view=kc.

18. IBM QRadar Vulnerability Assessment Configuration Guide. August 2019 [Електронний ресурс]. Режим доступу: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/com.ibm.dsm.doc/b_vuln.pdf?view=kc&origURL=SS42VS_DSM/b_vuln.pdf

19. Nessus 8.6.x User Guide. Last Updated: August 27, 2019. Tenable. 432 p. [Електронний ресурс]. Режим доступу: https://docs.tenable.com/nessus/8_6/Content/Resources/PDF/Nessus_8_6.pdf.

20. Tenable Scan Strategy. Tenable Professional Services. Last Revised: April 07, 2019. Tenable. 22 p. [Електронний ресурс]. Режим доступу: https://docs.tenable.com/other/nessus/Tenable_ProServ_Scan_Strategy_Guide.pdf.

21. Tenable.sc 5.13.x User Guide. Last Revised: December 30, 2019 Електронний ресурс]. Режим доступу: https://docs.tenable.com/sccv/5_13/Content/PDF/Tenablesc_UserGuide.pdf.

22. IBM QRadar Vulnerability Assessment Configuration Guide. January 2020 [Електронний ресурс]. Режим доступу: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/com.ibm.dsm.doc/b_vuln.pdf?view=kc&origURL=SS42VS_DSM/b_vuln.pdf

23. Tom Palmaers. Implementing a vulnerability management process. SANS Institute. Accepted: 03/23/2013. 24 p. [Електронний ресурс]. Режим доступу: https://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180

Інформаційні ресурси

1. IBM Knowledge Center. IBM QRadar Security Intelligence Platform 7.3.2. IBM Security QRadar SIEM V7.3.2 documentation [Електронний ресурс]. Режим доступу: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/c_qradar_pdfs.html.
2. Tenable. Documentation for Nessus [Електронний ресурс]. Режим доступу: https://docs.tenable.com/Nessus.htm.

(заліки, екзамени, курсові проекти, тестування)

іспит

11. Матеріально-технічне забезпечення освітньої компоненти

Навчальна лабораторія № 420
«Академічний центр компетенцій IBM (Кіберполігон)»

1. комп'ютери DellOptiPlex 3050/Corei5 7500T – 14 шт. (2017 рік).
2. Проектор ViewSonicPJD 7720 HD (2018) – 1 шт.
3. Система управління подіями та інцидентами кібербезпеки IBMSecurityQRadarSIEM:
4. набір серверів ServerDellPER530– 3шт.
5. робочі станції DellPrecisionTower 3620 i7 - 14 шт. Dell OptiPlex 3050 i5;
6. Маршрутизатор Mikrotik CSS326-24G-2S+RM. - 1 шт.
7. комутатор MikrotikCSS326-24G-2S+ RM – 1шт.

Lubuntu 16/04 , Ubuntu 16/04 server, MatLab, Security Appscan Standart 9.0.3.12, VirtualBox 6.0.12 Build 133076, ESET Security Management Center, Kali Linux 2019.3., IBM QRadar SIEM v.7.3.2, IBM QRadar Community Edition v.7.3.1, IBM i2 Analyst's Notebook, Tenable Nessus Professional.

проведення практичного навчання з питань :

набуття навичок роботи з спеціалізованими програмами для побудови та функціонування систем управління даними та подіями щодо кібербезпеки;

вивчення технологій, впровадження та керування рішеннями щодо запобігання подіям та інцидентам безпеки;

проведення моніторингу, налаштуванню, детального аналізу подій безпеки, розслідування подій, кореляція та визначення їх тенденцій для інформаційних систем.

Дана лабораторія забезпечує проведення наукових досліджень з розслідування кіберінцидентів та методів пошуку загроз, автоматизації процесів управління доступом користувачів інформаційних систем, з пошуку та класифікації вразливостей, проводити автоматизований аналіз для швидкого пошуку та класифікації вразливості інформації.

Інформаційний пакет освітньої компоненти, яка викладається англійською мовою, додатково розміщується на сторінці кафедри на англійській мові