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

Освітнього рівня **першого (бакалаврського) рівня вищої освіти**

Спеціальності **125 «Кібербезпека»**

Галузь знань **12 «Інформаційні технології»**

1. Назва освітньої компоненти SIEM системи

(назва дисципліни)

2. Тип основна

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	4	120	18		18	18	66
4. Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	1. Комп'ютерні мережі 2. Теоретичні основи захищених інформаційно-комунікаційних технологій 3. Аналіз та оцінка уразливостей інформаційних систем						
Освітні компоненти для яких є базовою	1. Основи захисту конфіденційних даних 2. Програмні комплекси захисту автоматизованих систем від несанкціонованого доступу 3. Комплексні системи захисту інформації 4. Цифрова криміналістика						
5. Компетенції відповідно до ОПП та вимог роботодавців:							
Компетенції відповідно до ООП							
Знати			**Вміти**				
1. ЗК 2. Знання та розуміння предметної області та розуміння професії.			1. ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.				
			2. ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.				
			3. ПП 2. Здатність до використання інформаційно-комунікаційних				

	технологій, сучасних методів і моделей інформаційної безпеки та кібербезпеки.
	ПП 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та кібербезпеки.
	ПП 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та кібербезпеки.
	ПП 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
	ПП 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
	ПП 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та кібербезпеки.
	ПП 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки.
Компетенції відповідно до вимог роботодавців	
1. Знання принципів побудови та роботи сучасних IT-систем.	1. Впровадження та адміністрування системи моніторингу стану кібербезпеки (SIEM-система) корпоративної інформаційної системи.
2. Знання сучасних підходів, принципів та варіантів реалізації забезпечення кібербезпеки корпоративних інформаційних систем.	2. Здійснення моніторингу подій та керувати інцидентами інформаційної безпеки в корпоративній інформаційній системі.
3. Знання принципів побудови, функціонування та застосування сучасних засобів забезпечення кібербезпеки.	3. Здійснення керування правами доступу користувачів до інформаційних систем.
	4. Здійснення контролю виконання політик інформаційної безпеки в корпоративній мережі та інформаційних системах.
	5. Приймання участі в процесах розслідування інцидентів інформаційної безпеки. Здійснення аналізу інцидентів та вироблення рекомендацій по їх недопущенню.
6. Результати навчання відповідно до ОПП	
1. ПРН 11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.	
2. ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	
3. ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.	

4. ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
5. ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і кібербезпеки.
6. ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
7. ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
8. ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
9. ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
10. ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і кібербезпеки.
11. ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в ІТС та ефективності використання КЗЗ в умовах реалізації загроз різних класів.
12. ПРН 40. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
13. ПРН 43. Вирішувати задачі забезпечення неперервності бізнес процесів організації на основі встановленої системи управління інформаційною безпекою, згідно вітчизняними та міжнародними вимогами і стандартами.
14. ПРН 47. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
15. ПРН 48. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
16. ПРН 51. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

7. План вивчення освітньої компоненти

Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
Розділ 1						
	Лекція 1	Тема: Поняття безпека інформаційної технології та її значення у сучасному суспільстві.	1. Поняття безпека інформаційної технології та її значення у сучасному суспільстві.		посилання на електронний ресурс http://dl.dut.edu.ua/course/category.php?id=207	посилання на електронний ресурс http://dl.dut.edu.ua/mod/resource/view.php?id=78787

		Предмет навчальної дисципліни.	2. Підходи до забезпечення кібербезпеки корпоративних інформаційних систем. Поняття “SIEM-система”.			
	Лекція 2	Тема: Рішення IBM QRadar Security Intelligence Platform як платформа для комплексного моніторингу стану кібербезпеки підприємства.	1. Підходи та принципи, які реалізовані в IBM QRadar Security Intelligence Platform. Рішення IBM QRadar. 2. Основні функції, які реалізовані в IBM QRadar Security Intelligence Platform.		http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Лекція 3	Тема: Склад, призначення, функції компонентів IBM QRadar SIEM та вимоги щодо їх розгортання.	1. Склад, призначення та функції компонентів IBM QRadar SIEM. 2. Вимоги щодо розгортання компонентів IBM QRadar SIEM.		http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Лекція 4	Тема: Основи адміністрування IBM QRadar SIEM. Керування користувачами.	1. Ролі користувачів. Створення, редагування та видалення ролі користувача. 2. Профілі безпеки. Облікові записи користувачів. 3. Рекомендації адміністраторові щодо зовнішньої автентифікації.		http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Лекція 5	Тема: Основи адміністрування IBM QRadar SIEM. Налаштування системи.	1. Налаштування системи. Мережева ієрархія. Безкласове адресування. Визначення мережевої ієрархії. Автоматичне оновлення. 2. Керування резервним копіюванням та відновленням. Редактор розгортання.		http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988

	Лекція 6	Тема: Основи адміністрування IBM QRadar SIEM. Керування джерелами потоків.	1. Джерела потоків. Потоки даних, що передаються по мережі, IPFIX, Sflow, J-Flow, Packeteer, файл Flowlog, інтерфейс Napatech. 2. Керування джерелами потоків.		http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Лекція 7	Тема: Основи адміністрування IBM QRadar SIEM. Керування активами.	1. Джерела даних активів. 2. Керування активами.		http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Лекція 8	Тема: Основи адміністрування IBM QRadar SIEM. Користувальницькі правила. Історична кореляція. Керування звітами.	1. Призначення користувальницьких правил. Типи користувальницьких правил. Правила виявлення аномалій. 2. Призначення історичної кореляції. Профіль історичної кореляції. 3. Призначення звітів. Типи звітів.		http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Лекція 9	Тема: Особливості рішень IBM QRadar Risc Manager та QRadar on Cloud.	1. Призначення та функції IBM QRadar Risk Manager. Монітор конфігурацій. Топологія. Монітор політики. Керування політикою. Симуляція. Керування джерелом конфігурацій. Звітність. Налаштування параметрів системи. 2. Призначення та функції IBM QRadar on Cloud. Налаштування параметрів системи.		http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Практичне	Тема: Порядок реєстрації	1. Порядок реєстрації	Порядок розгортання	http://dl.dut.edu	http://dl.dut.edu.ua/c

	заняття 1	студентів у програмі IBM Academic Initiative. Система сертифікації фахівців з кібербезпеки компанії IBM. Порядок інсталяції програмного комплексу IBM QRadar Community Edition.	студентів у програмі IBM Academic Initiative. 2. Система сертифікації фахівців з кібербезпеки компанії IBM. 3. Порядок інсталяції програмного комплексу IBM QRadar Community Edition.	SIEM-системи.	.ua/course/view .php?id=1988	ourse/view.php?id=1 988
	Практичне заняття 2	Тема: Основи адміністрування IBM QRadar SIEM. Користувальницький інтерфейс. Керування користувальницьким інтерфейсом.	1. Порядок входу до системи IBM QRadar SIEM. 2. Користувальницький інтерфейс системи IBM QRadar SIEM. Призначення користувальницького інтерфейсу. Склад користувальницького інтерфейсу. 3. Керування користувальницьким інтерфейсом системи IBM QRadar SIEM. Панелі інструментів за замовчуванням. Користувальницькі панелі інструментів.	Адміністрування SIEM-системи. Керування користувальницьким інтерфейсом.	http://dl.dut.edu .ua/course/view .php?id=1988	http://dl.dut.edu.ua/c ourse/view.php?id=1 988
	Практичне заняття 3	Тема: Основи адміністрування IBM QRadar SIEM. Керування порушеннями.	1. Розподіл пріоритетів порушень (Offense prioritization). 2. Зв’язки порушень (Offense chaining). 3. Індексування порушень (Offense indexing). 4. Утримання порушень (Offense retention). 5. Розслідування порушень (Offense investigations).	Адміністрування SIEM-системи. Керування порушеннями.	http://dl.dut.edu .ua/course/view .php?id=1988	http://dl.dut.edu.ua/c ourse/view.php?id=1 988

			6. Дії щодо порушень (Offense actions).			
	Практичне заняття 4	Тема: Основи адміністрування IBM QRadar SIEM. Керування користувачами.	1. Ролі користувачів (User roles). 2. Профілі безпеки (Security profiles). 3. Облікові записи користувачів (User accounts).	Адміністрування SIEM-системи. Керування користувачами.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Практичне заняття 5	Тема: Основи адміністрування IBM QRadar SIEM. Дослідження подій щодо порушення.	1. Дослідження деталей події. 2. Використання фільтрів для дослідження подій. 3 Використання групування для дослідження подій. 4. Збереження пошуку. 5. Зміна збережених пошуків.	Адміністрування SIEM-системи. Дослідження подій щодо порушення.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Практичне заняття 6	Тема: Основи адміністрування IBM QRadar SIEM. Керування джерелами потоків.	1. Типи джерел потоку. 2. Додавання або редагування джерела потоку. 3. Переадресація пакетів на захоплення пакетів QRadar. 4. Увімкнення та вимкнення джерела потоку. 5. Видалення джерела потоку. 6. Псевдоніми джерела потоку.	Адміністрування SIEM-системи. Керування джерелами потоків.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Практичне заняття 7	Тема: Основи адміністрування IBM QRadar SIEM. Керування активами.	1. Джерела даних про активи. 2. Робочий процес отримання даних про активи. 3. Оновлення даних про активи. 4. Визначення відхилень приросту активів.	Адміністрування SIEM-системи. Керування активами.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988

			5. Запобігання відхиленням зростання активів. 6. Видалення даних про активи після відхилень зростання.			
	Практичне заняття 8	Тема: Основи адміністрування IBM QRadar SIEM. Користувальницькі правила. Історична кореляція. Керування звітами.	1. Кореляційні правила. 2. Типи правил. 3. Управління правилами. 4. Створення користувальницького правила. 5. Налаштування потоку або події як хибно-позитивного.	Адміністрування SIEM-системи. Користувальницькі правила. Керування звітами.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Практичне заняття 9	Тема: Основи адміністрування IBM QRadar SIEM. Інтеграція IBM X-Force. Варіант розгортання IBM QRadar SIEM для забезпечення високої доступності (High Availability).	1. Інтеграція IBM X-Force, призначення, зміст даних та правил X-Force. 2. Варіант розгортання IBM QRadar SIEM для забезпечення високої доступності (High Availability, HA).	Адміністрування SIEM-системи. Розгортання IBM QRadar SIEM для забезпечення високої доступності.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Лабораторне заняття 1	Тема: Вимоги до апаратного та програмного забезпечення для встановлення IBM QRadar SIEM. Порядок встановлення IBM QRadar SIEM.	Вимоги до апаратного та програмного забезпечення для встановлення IBM QRadar SIEM.	1. Порядок встановлення IBM QRadar SIEM. 2. Порядок встановлення IBM QRadar Community Edition.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Лабораторне заняття 2	Тема: Основи адміністрування IBM QRadar SIEM. Користувальницький інтерфейс. Керування користувальницьким інтерфейсом.	Призначення користувальницького інтерфейсу.	1. Створення інформаційної панелі. 2. Налаштування діаграм. 3. Видалення елементів Панелі інструментів. 4. Від'єднання елемента інформаційної панелі.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988

				5. Перейменування Панелі інструментів. 6. Видалення інформаційної панелі. 7. Керування сповіщеннями системи. 8. Додавання елементів для дослідження інформаційної панелі до списку Додати елементи.		
	Лабораторне заняття 3	Тема: Основи адміністрування IBM QRadar SIEM. Керування порушеннями.	1. Offense investigations (Зміст розслідування порушення (інциденту)). 2. Offense actions (Зміст дій з порушеннями (інцидентами)).	1.1. Selecting an offense to investigate. 1.2. Investigating an offense by using the summary information. 1.3. Investigating events. 1.4. Investigating flows. 2.1. Adding notes. 2.2. Hiding offenses. 2.3. Showing hidden offenses. 2.4. Closing offenses. 2.5. Exporting offenses. 2.6. Assigning offenses to users. 2.7. Sending email notifications. 2.8. Marking an offense for follow-up.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Лабораторне заняття 4	Тема: Основи адміністрування IBM QRadar SIEM. Керування користувачами.	1. Ролі користувачів (User roles). 2. Профілі безпеки (Security profiles). 3. Облікові записи користувачів (User accounts). 4. Автентифікація	1.1. Створення ролі користувача (Creating a user role). 1.2. Редагування ролі користувача (Editing a user role). 1.3. Видалення ролі	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988

			користувачів (User authentication). 5. Обмеження ресурсів.	користувача (Deleting a user role). 2.1. Права дозволу (Permission precedence). 2.2. Створення профілю безпеки (Creating a security profile). 2.3. Редагування профілю безпеки (Editing a security profile). 2.4. Дублювання профілю безпеки (Duplicating a security profile). 2.5. Видалення профілю безпеки (Deleting a security profile). 3.1. Створення облікового запису користувача (Creating a user account). 3.2. Видалення облікового запису користувача (Deleting a user account). 3.3. Відключення облікового запису користувача (Disabling a user account). 4.1. Configuring TACACS authentication. 5.1. Налаштування ресурсних обмежень.		
	Лабораторне заняття 5	Тема: Основи адміністрування IBM QRadar SIEM. Налаштування системи. Керування резервним копіюванням та	Керування резервним копіюванням та відновленням (Backup and recovery).	1. Резервне копіювання конфігурацій та даних QRadar. 2. Управління наявними архівами резервного копіювання.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988

		відновленням. Редактор розгортання		3. Відновлення конфігурацій та даних QRadar. 4. Резервне копіювання та відновлення програм.		
	Лабораторне заняття 6	Тема: Основи адміністрування IBM QRadar SIEM. Історична кореляція. Керування джерелами потоків.	1. Поняття історична кореляція. 2. Огляд історичної кореляції. 3. Джерела даних потоку.	1. Управління профілем історичної кореляції. 2. Управління джерелами потоку. 2.1. Додавання або редагування джерела потоку. 2.2. Пересилання пакетів на захоплення пакетів QRadar. 2.3. Увімкнення та вимкнення джерела потоку. 2.4. Видалення джерела потоку. 2.5. Псевдоніми джерела потоку.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Лабораторне заняття 7	Тема: Основи адміністрування IBM QRadar SIEM. Керування активами.	1. Джерела даних про активи. 2. Робочий процес отримання даних про активи. 3. Оновлення даних про активи.	1. Визначення відхилень приросту активів. 2. Запобігання відхиленням зростання активів. 3. Видалення даних про активи після відхилень зростання.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Лабораторне заняття 8	Основи адміністрування IBM QRadar SIEM. Правила виявлення аномалій. Створення правил виявлення аномалій.	1. Кореляційні правила. Правила виявлення аномалій.	1. Створення правил виявлення аномалій.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Лабораторне	Тема: Основи	1. Керування звітами (Report	1.Creating custom reports.	http://dl.dut.edu	http://dl.dut.edu.ua/c

	заняття 9	адміністрування IBM QRadar SIEM. Користувальницькі правила. Керування звітами.	management).	2. Editing a report. 3. Viewing generated reports. 4. Deleting generated content. 5. Manually generating a report. 6. Duplicating a report. 7. Sharing a report. 8. Branding reports. 9. Report groups.	.ua/course/view.php?id=1988	ourse/view.php?id=1988
	Самостійна робота	Тема: Поняття безпека інформаційної технології та її значення у сучасному суспільстві. Предмет навчальної дисципліни. Порядок реєстрації студентів у програмі IBM Academic Initiative. Система сертифікації фахівців з кібербезпеки компанії IBM. Вимоги до апаратного та програмного забезпечення для встановлення IBM QRadar SIEM. Порядок встановлення IBM QRadar SIEM.	1. Поняття безпека інформаційної технології та її значення у сучасному суспільстві. 2. Підходи до забезпечення кібербезпеки корпоративних інформаційних систем. Поняття “SIEM-система”. 3. Порядок інсталяції програмного комплексу IBM QRadar Community Edition.	1. Порядок встановлення IBM QRadar SIEM. 2. Порядок встановлення IBM QRadar Community Edition.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Самостійна робота	Тема: Рішення IBM QRadar Security Intelligence Platform як платформа для комплексного моніторингу стану	1. Підходи та принципи, які реалізовані в IBM QRadar Security Intelligence Platform. Рішення IBM QRadar. 2. Основні функції, які реалізовані в IBM QRadar	1. Створення інформаційної панелі. 2. Налаштування діаграм. 3. Видалення елементів Панелі інструментів. 4. Від'єднання елемента	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988

		кібербезпеки підприємства. Вхід до системи IBM Security QRadar. Користувальницький інтерфейс. Керування користувальницьким інтерфейсом.	Security Intelligence Platform.	інформаційної панелі. 5. Перейменування Панелі інструментів. 6. Видалення інформаційної панелі. 7. Керування сповіщеннями системи. 8. Додавання елементів для дослідження інформаційної панелі до списку Додати елементи.		
	Самостійна робота	Тема: Склад, призначення, функції компонентів IBM QRadar SIEM та вимоги щодо їх розгортання. Управління порушеннями в IBM QRadar SIEM.	1. Склад, призначення та функції компонентів IBM QRadar SIEM. 2. Вимоги щодо розгортання компонентів IBM QRadar SIEM.	1. Розподіл пріоритетів порушень (Offense prioritization). 2. Зв'язки порушень (Offense chaining). 3. Індексування порушень (Offense indexing). 4. Утримання порушень (Offense retention). 5. Розслідування порушень (Offense investigations). 6. Дії щодо порушень (Offense actions).	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Самостійна робота	Тема: Основи адміністрування IBM QRadar SIEM. Керування користувачами.	1. Ролі користувачів. Створення, редагування та видалення ролі користувача. 2. Профілі безпеки. Облікові записи користувачів. 3. Рекомендації адміністраторові щодо зовнішньої автентифікації.	1.1. Створення ролі користувача (Creating a user role). 1.2. Редагування ролі користувача (Editing a user role). 1.3. Видалення ролі користувача (Deleting a user role). 2.1. Права дозволу (Permission precedence). 2.2. Створення профілю	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988

				безпеки (Creating a security profile). 2.3. Редагування профілю безпеки (Editing a security profile). 2.4. Дублювання профілю безпеки (Duplicating a security profile). 2.5. Видалення профілю безпеки (Deleting a security profile). 3.1. Створення облікового запису користувача (Creating a user account). 3.2. Видалення облікового запису користувача (Deleting a user account). 3.3. Відключення облікового запису користувача (Disabling a user account). 4.1. Configuring TACACS authentication. 5.1. Налаштування ресурсних обмежень.		
	Самостійна робота	Тема: Основи адміністрування IBM QRadar SIEM. Налаштування системи. Керування резервним копіюванням та відновленням. Редактор розгортання.	1. Налаштування системи. Мережева ієрархія. Безкласове адресування. Визначення мережевої ієрархії. Автоматичне оновлення. 2. Керування резервним копіюванням та відновленням. Редактор розгортання.	1. Резервне копіювання конфігурацій та даних QRadar. 2. Управління наявними архівами резервного копіювання. 3. Відновлення конфігурацій та даних QRadar. 4. Резервне копіювання та відновлення програм.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988

	Самостійна робота	Тема: Основи адміністрування IBM QRadar SIEM. Керування джерелами потоків.	1. Джерела потоків. Потоки даних, що передаються по мережі, IPFIX, Sflow, J-Flow, Packeteer, файл Flowlog, інтерфейс Napatech. 2. Керування джерелами потоків.	1. Управління профілем історичної кореляції. 2. Управління джерелами потоку. 2.1. Додавання або редагування джерела потоку. 2.2. Пересилання пакетів на захоплення пакетів QRadar. 2.3. Увімкнення та вимкнення джерела потоку. 2.4. Видалення джерела потоку. 2.5. Псевдоніми джерела потоку.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Самостійна робота	Тема: Основи адміністрування IBM QRadar SIEM. Керування активами.	1. Джерела даних активів. 2. Керування активами.	1. Визначення відхилень приросту активів. 2. Запобігання відхиленням зростання активів. 3. Видалення даних про активи після відхилень зростання.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
	Самостійна робота	Тема: Основи адміністрування IBM QRadar SIEM. Користувальницькі правила. Історична кореляція. Керування звітами.	1. Призначення користувальницьких правил. Типи користувальницьких правил. Правила виявлення аномалій. 2. Призначення історичної кореляції. Профіль історичної кореляції. 3. Призначення звітів. Типи звітів.	1.Creating custom reports. 2. Editing a report. 3. Viewing generated reports. 4. Deleting generated content. 5. Manually generating a report. 6. Duplicating a report. 7. Sharing a report. 8. Branding reports. 9. Report groups.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988

	Самостійна робота	Тема: Особливості адміністрування IBM QRadar Risc Manager та QRadar on Cloud.	1. Призначення та функції IBM QRadar Risk Manager. Монітор конфігурацій. Топологія. Монітор політики. Керування політикою. Симуляція. Керування джерелом конфігурацій. Звітність. Налаштування параметрів системи. 2. Призначення та функції IBM QRadar on Cloud. Налаштування параметрів системи.	1. Налаштування параметрів системи IBM QRadar Risc Manager. 2. Налаштування параметрів системи IBM QRadar on Cloud.	http://dl.dut.edu.ua/course/view.php?id=1988	http://dl.dut.edu.ua/course/view.php?id=1988
Розділ 2						
	…	…				
Розділ …						
	…	…				

8. Мова вивчення освітньої компоненти

(українська, англійська, розділи, що викладаються англійською мовою)

українська

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

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. MITRE. Ten Strategies of a World-Class Cybersecurity Operations Center. /Carson Zimmerman –The MITRE Corporation, 2014. – 346 p.
6. IBM Security QRadar. Version 7.3.2. Installation Guide [Електронний ресурс] – Режим доступу: https://www.ibm.com/support/knowledgecenter/ru/SS42VS_7.3.2/com.ibm.qradar.doc/b_siem_inst.pdf?view=kc.
7. IBM QRadar Security Intelligence Platform. Actionable intelligence for enterprise security using the IBM QRadar Sense Analytics Engine. [Електронний ресурс]. Режим доступу: http://www.ibmjournal.com/hubfs/Security_content/IBMjournal_QRadar_WP.pdf?t=1479226713412.
8. 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.
9. 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.

10. 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.
11. 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.
12. 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.
13. The Advantages of TACACS+ for Administrator Authentication. [Електронний ресурс]. Режим доступу: http://tacacs.net/docs/TACACS_Advantages.pdf.
14. 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.

Інформаційний ресурс
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

10. Методи оцінювання, підсумкові звітності за освітньою компонентою
(заліки, екзамени, курсові проекти, тестування)
залік
11. Матеріально-технічне забезпечення освітньої компоненти
лабораторія «Кіберполігон» із системою управління подіями та інцидентами кібербезпеки IBM Security QRadar SIEM