Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського
Спеціальна кафедра № 1

СИСТЕМИ КІБЕРБЕЗПЕКИ

Робоча програма навчальної дисципліни (силабус)

Рівень вищої освіти	*Другий (магістерський)*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Освітньо-професійна програма	*Безпека державних інформаційних ресурсів*
Статус дисципліни	*Вибіркова*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*І рік підготовки, весняний семестр*
Обсяг дисципліни	*5 кредитів*
Семестровий контроль/ контрольні заходи	*Залік, модульна контрольна робота*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	
Розміщення курсу	

Київ 2023

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Навчальна дисципліна *"Системи кібербезпеки"* передбачена освітньо-професійною програмою підготовки здобувачів вищої освіти *Безпека державних інформаційних ресурсів*, *ступеня вищої освіти магістр.* Відноситься до вибіркових освітніх компонентів.

Метою навчальної дисципліни "Системи кібербезпеки" є засвоєння курсантами матеріалу щодо критичних контролів інформаційних систем, систем забезпечення кіберзахисту, здійснення моніторингу за станом інформаційної безпеки, проведення кіберрозвідки та підсилення наступних компетентностей:

КЗ-1	Здатність застосовувати знання у практичних ситуаціях.
КЗ-2	Здатність проводити дослідження на відповідному рівні.
КЗ-5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КФ3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ4	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ5	Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7	Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
КФ9	Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ11	Здатність реалізовувати технічні вимоги на основі технік оцінки рівня захищеності інформаційних систем, технологій аналізу мережевого трафіку та принципів протидії кібератакам.

Предметом навчальної дисципліни є системи аналізу шкідливого програмного забезпечення.

Виконання програми навчальної дисципліни "Технології організації та захисту державних інформаційних ресурсів" дозволяє підсилити курсантами наступні результати навчання:

РН2	Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН14	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\абокібербезпеки в цілому.
РН21	Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН24	Оцінювати стан інформаційних систем, розподіляти послуги безпеки і обирати механізми безпеки, впроваджувати технологічні рішення інноваційного характеру щодо виявлення та блокування загроз інформаційним ресурсам.

2. Пререквізити та постреквізити навчальної дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Успішне вирішення завдань навчальної дисципліни "Системи кібербезпеки" базується на засвоєні курсантами знань та умінь, сформованих у них, в результаті підготовки за ступенем вищої освіти бакалавр. Навчальна дисципліна забезпечує "Кібернавчання", а також виконання магістерської дисертації.

3. Зміст навчальної дисципліни

Семестровий (кредитний) модуль 1. Системи кібербезпеки.

Тема 1. Системи керування подіями інформаційної та кібербезпеки.

Тема 2. Оперативні центри кібербезпеки (SOC).

Тема 3. Розвідка кіберзагроз (CTI).

4. Навчальні матеріали та ресурси

Основна література.

1. P Contreras, Erickson Delgado, Betsy Page Sigman. Splunk 7 Essentials Third Edition: Packt Publishing, 2018. – 284 с.

2. Ahmad, Neven Faraj. Brave New World: NATO, the EU and the New Age of Cyberspace. MS thesis. 2020.

3. Vijayakumar, Sangavi. A Unified Data Model for Cyber Threat Intelligence in Operational Technology Networks. 2020

4. Saraf, Kundankumar Rameshwar, and P. Malathi. "Splunk-Based Threat Intelligence of Cyber-Physical System: A Case Study with Smart Healthcare." International Journal of Intelligent Systems and Applications in Engineering 11.2 (2023): 537-549.

5. Lauri Palkmets, Cosmin Ciobanu, Yonas Leguesse. Advanced artefact analysis. Advanced static analysis.: ENISA, 2018. – 122 с.

Додаткова література.

1. Travis Marlette. Splunk Best Practices. Design, implement, and publish custom Splunk applications by following best practices.: Packt Publishing, 2016. – 238 с.

2. Ashish Kumar Tulsiram Yadav. Advanced Splunk. Master the art of getting the maximum out of your machine data using Splunk.: Packt Publishing, 2016. – 348 с.

3. David Carasso. Exploring Splunk. Search Processing Language (SPL) primer and cookbook.: CITO Research, 2014. – 156 с.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчальна дисципліна “Системи кібербезпеки” вивчається курсантами на 1-ому курсі в весняному семестрі.

Видами навчальних занять є лекції, практичні та самостійна робота.

Лекції є початковими заняттями в темах дисципліни. В них формуються головні завдання теми та викладаються основні напрямки його вирішення, вивчається конкретизований теоретичний матеріал.

На практичних заняттях курсанти закріплюють та поглиблюють знання, отримані на лекціях, з формуванням у них вмінь виконання окремих завдань з кібербезпеки інформаційних ресурсів, набувають практичних навичок моделюванні окремих елементів системи кібербезпеки державних інформаційних ресурсів, а також проводиться виконання практичного завдання.

Самостійна робота курсантів проводиться без керівництва викладача з метою самостійного закріплення та розширення знань.

В процесі вивчення дисципліни проводиться виховна робота зі курсантами. В процесі занять виховується наполегливість у переборенні труднощів, уміння самостійно освоювати нові засоби та методи захисту інформації.

Поточний контроль знань та вмінь курсантів реалізується індивідуальним усним або груповим письмовим опитуванням на практичних заняттях.

Підсумковий контроль здійснюється у вигляді заліку.

Структура кредитного модуля

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу		Кількість годин				
		Всього	у тому числі			
			Лекції	Практ. (семін.)	Лаборант. (комп.пр.)	СРК
Розділ 1. Системи кібербезпеки						
Тема 1.	**Системи керування подіями інформаційної та кібербезпеки**	**48,5**	**4**	**14**		**30,5**
Заняття 0/1	Вступ до дисципліни. 1. Критичні контролі (CIS 20). 2. Основні класи систем забезпечення кібербезпеки. Основна література: [2].	**5**	2			3

Заняття 1/1	Системи керування подіями інформаційної безпеки. 1. Загальна архітектура систем. 2. Джерела моніторингу. 3. Поняття події та інциденту інформаційної безпеки. Основна література: [1-4].	**5**	2			3
Заняття 1/2	Архітектура системи SPLUNK. 1. Призначення системи SIEM. 2. Функцій модуля Indexer. 3. Функції модуля Forwarder. Основна література: [1-4].	**5,5**		2		3,5
Заняття 1/3	Встановлення та базове конфігурування SPLUNK. 1. Налаштування операційної системи. 2. Встановлення SLPUNK. 3. Базове конфігурування SPLUNK. Основна література: [1-4].	**5,5**		2		3,5
Заняття 1/4	Підключення джерел до системи SPLUNK. 1. Класифікація джерел. 2. Підключення джерел SYSLOG. 3. Підключення інших видів джерел. Основна література: [1-5].	**5,5**		2		3,5
Заняття 1/5	Використання базового пошуку. 1. Структура пошукового запиту. 2. Використання часових інтервалів. 3. Збереження результатів пошуку. Основна література: [1-4].	**5,5**		2		3,5
Заняття 1/6	Використання полів пошуку. 1. Поняття поля пошуку. 2. Формування полів пошуку. Основна література: [1-4].	**5,5**		2		3,5
Заняття 1/7	Використання мови пошукових запитів SPL. 1. Синтаксис пошукового запиту. 2. Основні команди запитів. 3. Команди перетворення інформації. Основна література: [1-4].	**5,5**		2		3,5
Заняття 1/8	Використання звітів та візуалізацій. 1. Побудова звітів. 2. Побудова таблиць та візуалізацій. Основна література: [1-4].	**5,5**		2		3,5
Тема 2.	**Оперативні центри кібербезпеки (SOC)**	**49,5**	**2**	**16**		**31,5**

Заняття 2/1	Архітектура та основні принципи побудови SOC. 1. Функції та завдання. 2. Архітектура. 3. Рівень зрілості SOC. Основна література: [2].	**5,5**	2			3,5
Заняття 2/2	Використання панелей звітів та візуалізацій. 1. Побудова інформаційних панелей. 2. Створення параметричних інформаційних панелей. Основна література: [1-5].	**5,5**		2		3,5
Заняття 2/3	Моделі даних та узагальнені інформаційні моделі. 1. Моделі даних (Data models). 2. Узагальнені інформаційні моделі (Common information model). Основна література: [1-4].	**5,5**		2		3,5
Заняття 2/4	Використання пошукових запитів. 1. Створення пошукових запитів та визначень. 2. Автоматичні пошукові запити. Основна література: [1-4].	**5,5**		2		3,5
Заняття 2/5	Використання запланованих звітів та інформувань. 1. Опис та налаштування планових звітів. 2. Опис та налаштування автоматичних інформувань . 3. Створення автоматичних реакцій на події. Основна література: [1-4].	**5,5**		2		3,5
Заняття 2/6	Робота із журналами подій проксі-серверів. 1. Формат журналу подій. 2. Розроблення інформаційної панелі. 3. Налаштування автоматичних інформувань на підозрілі події. Основна література: [1-4].	**5,5**		2		3,5
Заняття 2/7	Робота із журналами події веб серверів. 1. Формат журналу подій. 2. Розроблення інформаційної панелі. 3. Налаштування автоматичних інформувань на підозрілі події. Основна література: [1-4].	**5,5**		2		3,5
Заняття 2/8	Аналіз даних із не стандартних джерел. 1. Збір та аналіз даних із SQL. 2. Збір та аналіз даних із mongoDB. Основна література: [1-4].	**5,5**		2		3,5

Заняття 2/9	Робота із зовнішніми джерелами подій. 1. Налаштування збору даних із зовнішніх джерел. 2. Використання зовнішніх даних для моніторингу аномальної поведінки. 3. Модульна контрольна робота (частина 1). Основна література: [1-4].	**5,5**		2		3,5
Тема 3.	**Розвідка кіберзагроз (CTI)**	**44**	**2**	**14**		**28**
Заняття 3/1	Основні поняття та визначення CTI. 1. Призначення та основні завдання. 2. Термінологія CTI. 3. Основні мови структуризації даних. 4. Протоколи обміну та взаємодії CTI. Основна література: [2].	**5,5**	2			3,5
Заняття 3/2	Платформи кіберрозвідки (TIP). 1. Платформи опрацювання інцидентів. 2. Платформи обміну інформацією про загрози. Основна література: [5].	**5,5**		2		3,5
Заняття 3/3	Статичний аналіз артефактів. 1. Аналіз заголовків файлів. 2. Визначення пакувальників та методів захисту. 3. Пошук слів та змінних. 4. Пошук вкладених об’єктів. Основна література: [5].	**5,5**		2		3,5
Заняття 3/4	Поведінковий аналіз артефактів. 1. Моніторинг процесів. 2. Моніторинг змін реєстру. 3. Моніторинг файлових систем. Основна література: [5].	**5,5**		2		3,5
Заняття 3/5	Аналіз мережевого трафіку. 1. Засоби аналізу. 2. Аналіз протоколу HTTP. 3. Аналіз протоколу SMTP. 4. Аналіз протоколу DNS. Основна література: [5].	**5,5**		2		3,5
Заняття 3/6	Опрацювання артефактів використовуючи систему CRITS. 1. Основні домени репозиторію. 2. Використання аналітичних сервісів репозиторію. 3. Побудова зав’язків між об’єктами. Основна література: [5].	**5,5**		2		3,5

Заняття 3/7	Організація обміну інформації про індикатори кіберзагроз використовуючи MISP. 1. Формат повідомлення MISP. 2. Основні оброблювачі завдань. 3. Фільтрація та кореляція даних. Основна література: [5].	**5,5**		2		3,5
Заняття 3/8	Використання зовнішніх сервісів для збагачення даних про загрози. 1. Сервіси VT, X-Force Exchange. 2. Сервіс Passive DNS. 3. Використання зовнішніх потоків даних. 4. Модульна контрольна робота (частина 2). Основна література: [5].	**5,5**		2		3,5
Разом за розділом 1		**142**	**8**	**44**		**90**
Залік		8		2		6
Всього годин		**150**	**8**	**46**		**96**

6. Самостійна робота курсантів

Головними видами самостійної роботи курсантів є: самостійна підготовка до аудиторних занять та самостійна підготовка до заліку.

Доцільно час самостійної підготовки для поглибленого вивчення та закріплення навчального матеріалу розподілити наступним чином:

№ з/п	Назва теми та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу)	Кількість годин СР
Тема 1. Системи керування подіями інформаційної та кібербезпеки.		
1.	Поняття події та інциденту інформаційної безпеки. Функції модуля Forwarder. Базове конфігурування SPLUNK. Підключення інших видів джерел. Формування полів пошуку. Команди перетворення інформації. Побудова таблиць та візуалізацій. Основна література: [1-4]. Додаткова література: [1-3].	30,5
Тема 2. Оперативні центри кібербезпеки (SOC).		
2.	Рівень зрілості SOC. Створення параметричних інформаційних панелей. Узагальнені інформаційні моделі (Common information model). Створення автоматичних реакцій на події. Налаштування автоматичних інформувань на підозрілі події. Використання зовнішніх даних для моніторингу аномальної .поведінкиОсновна література: [1-4]. Додаткова література: [1-3].	31,5

Тема 3. Розвідка кіберзагроз (CTI).		
3.	Протоколи обміну та взаємодії CTI. Платформи обміну інформацією про загрози. Пошук слів та змінних. Моніторинг файлових систем. Аналіз протоколу DNS. Побудова зав'язків між об'єктами. Фільтрація та кореляція даних. Використання зовнішніх потоків даних. Основна література: [5-7]. Додаткова література: [1-3].	28
4.	Підготовка до заліку.	6
Всього годин		**96**

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Політика навчальної дисципліни визначає систему вимог, які викладач ставить перед курсантами:

Правила поведінки та відвідування навчальних занять передбачають: оволодівати теоретичними знаннями і практичними навичками за обраною спеціальністю; дотримуватися графіка навчального процесу та вимог навчального плану; відвідувати навчальні заняття і виконувати у встановлені терміни усі види завдань, передбачені цим силабусом; у разі хвороби, несення служби в наряді або у виняткових випадках курсант може бути відсутнім на заняттях (з подальшим відпрацюванням пропущеного матеріалу самостійно або на консультаціях).

По прибутті на навчальні заняття курсанти повинні відключати мобільні телефони; входити і виходити з аудиторії тільки з дозволу керівника заняття; уважно слухати пояснення керівника заняття та відповіді одногрупників; не розмовляти і не займатися сторонніми справами; виконувати всі вказівки керівника навчального заняття; підтримувати чистоту і порядок в приміщеннях, дотримуватися морально-етичних правил поведінки і спілкування.

Дотримання академічної доброчесності здобувачами освіти передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання; посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; дотримання норм законодавства про авторське право і суміжні права; надання достовірної інформації про результати власної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

У випадку запровадження обмежувальних заходів, що унеможливлюють організацію і здійснення освітнього процесу в навчальних приміщеннях у складі груп, проведення навчальних занять з даної навчальної дисципліни можна здійснювати віддалено з використанням технологій дистанційного навчання. В цьому випадку з курсантів вимагається обов'язково наявність справних відеокамери та мікрофону, які мають бути увімкнені на кожному дистанційному занятті. При проведення письмових контрольних заходів вимагається верифікація курсанта (фото з документом). Навчальна література навчальної дисципліни зазначена в розділі 4, є відкритою, не містить відомостей з обмеженим доступом і

може бути оприлюднена з використанням технологій дистанційного навчання, а сама програма не потребує коригування у випадку проведення навчальних занять у дистанційному режимі.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Видами контролю якості навчання курсантів є: поточний, календарний та семестровий контроль.

Оцінювання результатів навчання курсантів здійснюється у відповідності до Положення про систему оцінювання результатів навчання в КПІ ім. Ігоря Сікорського.

Рейтинг курсанта з навчальної дисципліни складається з балів за:

1) 4 відповіді або експрес-контролі на групових заняттях, максимальна кількість балів експрес-контролів дорівнює 4 бали × 4 експрес-контролі = 16 балів:

правильно і повністю надано всі відповіді – 4.

частково надано відповіді або наявні незначні помилки – 3.

завдання виконані з помилками – 2.

завдання не виконані – 0.

2) 15 виконаних та захищених практичних завдань, кожне з яких оцінюється у 4 бали × 15 = 60 балів:

правильно і повністю виконані всі завдання, захист без запізнень – 4.

частково виконані завдання або наявні незначні помилки – 3.

завдання виконані з помилками або із запізненням – 2.

завдання не виконані – 0.

3) модульну контрольну роботу (розділена на дві частини по 0,5 години):

максимальна кількість балів за всі частини модульної контрольної роботи 10 балів × 2 = 20 балів:

правильно і повністю виконані всі завдання – 10.

частково виконані завдання або наявні незначні помилки – 8-9.

завдання виконані з помилками – 6-7.

завдання не виконані – 0.

4) ведення конспекту лекції – 4 бали:

конспект повний (в т.ч. питання, що виносяться на самопідготовку) – 4.

конспект не повний – 0.

5) штрафні та заохочувальні бали за:

невчасно здані практичні завдання, пасивність на заняттях та несистематична самостійна робота протягом семестру -1… -10.

активність на заняттях та систематична самостійна робота протягом семестру, участь на олімпіадах та наукових конференціях +1…+ 10.

Календарна атестація курсантів проводиться за окремим розпорядженням КПІ ім. Ігоря Сікорського за результатами поточного рейтингу курсанта на час атестації. Якщо значення цього рейтингу не менше 50 % від максимально можливого на час атестації, курсант вважається атестованим.

Розрахунок шкали (R) рейтингу:

Сума вагових балів контрольних заходів складає R = 16+60+20+4 = 100 балів.

Умовою допуску до заліку є отримання курсантом позитивних оцінок з контрольних робіт та виконання всіх практичних завдань.

Курсанти, які набрали протягом семестру рейтинг з кредитного модуля менше $0{,}6R$, зобов'язані виконувати залікову контрольну роботу.

Курсанти, які набрали протягом семестру необхідну кількість балів ($RD \geq 0{,}6R$), мають можливості:

1) за рішенням викладача застосовується жорстка РСО – попередній рейтинг курсанта з дисципліни скасовується і він отримує оцінку тільки за результатами залікової контрольної роботи, яка оцінюється в 100 балів. Цей варіант змушує курсанта критично оцінити рівень своєї підготовки та ретельно готуватися до заліку.

На заліку курсант виконує залікову письмову контрольну роботу. В кожному варіанті залікової контрольної роботи три питання: перше та друге теоретичне, максимум по 25 балів; третє практичне, максимум 50 балів. Відповідно максимальний бал за залік 100 балів.

Критерії нарахування балів за відповідь на кожне теоретичне питання:

– "відмінно" – повна відповідь (не менше 90% потрібної інформації) – 24 - 25 балів;

– "добре" – достатньо повна (не менше 75% потрібної інформації) або повна відповідь з незначними неточностями – 19 – 23 бали;

– "задовільно" – неповна відповідь (не менше 60% потрібної інформації) та має незначні помилки – 15 – 18 балів;

– "незадовільно" – відповідь не відповідає вимогам для оцінювання на "задовільно" – 0 балів.

Критерії нарахування балів за виконння завдання з практичного питання:

– "відмінно" – повна відповідь (не менше 90% потрібної інформації) – 48 - 50 балів;

– "добре" – достатньо повна (не менше 75% потрібної інформації) або повна відповідь з незначними неточностями –38 – 47 бали;

– "задовільно" – неповна відповідь (не менше 60% потрібної інформації) та має незначні помилки – 30 – 37 балів;

– "незадовільно" – відповідь не відповідає вимогам для оцінювання на "задовільно" – 0 балів.

Сума балів за кожне питання складає рейтинг, який визначає оцінку за дисципліну, є остаточним і вноситься в залікову відомість.

2) за рішенням викладача отримати залікову оцінку (залік) так званим "автоматом" відповідно до набраного рейтингу R.

Вважається, що курсант успішно виконав програму навчальної дисципліни, якщо він отримав позитивну загальну рейтингову оцінку $RD \geq 60$.

Рейтингова оцінка трансформується до університетської системи оцінювання згідно з таблицею:

Кількість балів	Оцінка
95-100	Відмінно
85-94	Дуже добре
75-84	Добре
65-74	Задовільно
60-64	Достатньо
менше 60	Незадовільно

Заохочувальні та штрафні бали застосовуються вибірково та мають на меті підвищення мотивації курсантів до активної, відповідальної, системної роботи на заняттях протягом семестру.

9. Додаткова інформація з навчальної дисципліни

Приклад питань, що виносяться на залікову контрольні роботу:

1. Основні класи систем забезпечення кібербезпеки.
2. Загальна архітектура систем.
3. Критичні контролі (CIS 20).
4. Поняття події та інциденту.
5. Компоненти SPL.
6. Розвідка кіберзагроз, класифікація та завдання.
7. Внутрішні джерела даних Threat Intelligence.
8. Завдання Threat Intelligence. Типи даних Threat Intelligence.
9. Зовнішні джерела даних Threat Intelligence.
10. Дослідити мережу лабораторії (комп’ютерного класу), виявити всі активні вузли засобоми TimeStamp Request, Information Request, Netmask Request.
11. Дослідити мережу лабораторії (комп'ютерного класу), виявите всі активні вузли методом TCP Ping, з використанням TCP-пакетів з різним поєднанням прапорів.
12. Дослідити відповіді різних ОС на сканування методами Stealth scanning. Занести в таблицю результати для різних способами перевірки та станів TCP-порту (порт відкритий, порт закритий, порт відкритий і фільтрується, порт закритий і фільтрується).