МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД

“УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ”

кафедра твердотільної електроніки та інформаційної безпеки

«ЗАТВЕРДЖУЮ»
Декан фізичного факультету
_____/Лазур В.Ю./
«__30__» _____червня_____ 2023 року

Робоча програма навчальної дисципліни

СИСТЕМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

Рівень вищої освіти	другий (магістерський) рівень вищої освіти
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Освітня програма	Безпека інформаційних і комунікаційних систем
Статус дисципліни	Обов’язова
Мова навчання	Українська

Ужгород 2023

Робоча програма навчальної дисципліни «**Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки**» для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека та захист інформації** освітньої програми **Безпека інформаційних і комунікаційних систем.**

Розробник: доктор технічних наук, старший науковий співробітник Давиденко А.М.

Робочу програму розглянуто та затверджено на засіданні кафедри твердотільної електроніки та інформаційної безпеки
протокол № 9 від «15» червня 2023 р.

Завідувач кафедри _____ Різак В.М.

Схвалено науково-методичною комісією фізичного факультету
протокол № 10 від «28» червня 2023р.
Голова науково-методичної комісії _____ Карбованець М. І.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	**Розподіл годин за навчальним планом**
	Денна форма навчання
Кількість кредитів ЄКТС – **4**	Рік підготовки:
Загальна кількість годин - **120**	**1**
Кількість модулів – 2	Семестр:
Тижневих годин для денної форми навчання: аудиторних – **3** самостійної роботи студента – **4**	**1**
	Лекції:
	24
	Практичні (семінарські):
	24
Вид підсумкового контролю: **іспит**	Лабораторні:
Форма підсумкового контролю: **усна**	Самостійна робота:
	72

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки»

Мета курсу – надання студентам цілісної системи знань, умінь і навичок для оволодіння сучасними методиками безпеки інформаційних і комунікаційних систем, методикою реагування на кіберінциденти та кібератаки; формування вмінь щодо проведення розслідування та аналізу кіберінцидентів і контролю результатів навчання; розвиток у студентів здатності успішно застосовувати набуті знання та уміння у повсякденній та професійній практиці при розв'язанні ситуацій, пов'язаних з безпекою інформаційних і комунікаційних систем; розвиток у студентів здатності до самоосвіти та саморозвитку.

Завдання дисципліни «Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» – формування системи знань щодо теоретико-методологічних та методичних засад методики реагування на кіберінциденти та кібератаки, чинників та тенденцій розвитку безпеки інформаційних і комунікаційних систем в сучасних умовах, розвиток системи навичок щодо вирішення актуальних проблем кібербезпеки, інтерпретації наукових досліджень, оцінки можливостей їх застосування та можливих ризиків їх упровадження в інформаційному просторі, ознайомлення з найбільш важливими

питаннями загальних основ безпеки інформаційних і комунікаційних систем з позицій сучасного підходу.

Фокус навчальної дисципліни: зміст та матеріал навчальної дисципліни стосується аналізу теоретико-методологічних основ виявлення вразливостей і реагування на кіберінциденти та кібератаки, які орієнтують студента на актуальні питання сьогоднішнього стану забезпечення інформаційної безпеки підприємств, в рамках якої можлива подальша професійна та наукова кар'єра у галузі кібербезпеки.

Місце дисципліни в структурі освітньо-наукової програми: курс відноситься до дисциплін теоретико-практичної частини циклу професійної підготовки, за результатами яких здобувачі здають іспит та виконують навчальний процес по спеціальності 125 Кібербезпека та захист інформації.

Відповідно до освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» для другого (магістерського) рівня спеціальності 125 Кібербезпека та захист інформації, вивчення дисципліни сприяє формуванню у здобувачів другого рівня вищої освіти таких компетентностей:

Інтегральна: Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

Загальні компетентності:

1. Здатність застосовувати знання у практичних ситуаціях (КЗ-1).
2. Здатність оцінювати та забезпечувати якість виконуваних робіт (КЗ-4).
3. Здатність діяти соціально відповідально та громадсько свідомо (КЗ-5).

Фахові компетенції (ФК)

1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки (КФ1).

2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки (КФ2).

3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури (КФ3).

4. 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 (КФ4).

5. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації (КФ6).

6. 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 (КФ7).

7. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації (КФ8).

А відповідно до професійного стандарту «Фахівець сфери захисту інформації» вивчення дисципліни сприяє формуванню у здобувачів другого рівня вищої освіти таких компетентностей:

Загальні компетентності (ЗК)

ЗК.01. Здатність діяти соціально відповідально та громадсько свідомо.

ЗК.02. Здатність застосовувати знання у практичних ситуаціях, розв'язувати завдання/задачі та практичні проблеми у професійній діяльності.

ЗК.05. Здатність до адаптації та дії в новій ситуації.

Професійні компетентності (за трудовою дією або групою трудових дій) згідно професійного стандарту «Фахівець сфери захисту інформації»

Д1. Здатність аналізувати, інтегрувати і використовувати кращі світові практики, стандарти при розробці нормативних документів системи технічного та криптографічного захисту інформації.

Е2. Здатність взаємодіяти із керівництвом і фахівцями технологічних та інших підрозділів підприємства/організації з технологічних та інших питань, пов'язаних із забезпеченням захисту інформації та кіберзахисту.

Е4. Здатність надавати консультативні послуги та технічну допомогу з питань технічного та криптографічного захисту інформації та кіберзахисту.

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» для другого (магістерського) рівня спеціальності 125 Кібербезпека та захист інформації**,** вивчення навчальної дисципліни повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (РН)**:**

Програмні результати навчання	
Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	РН 7
Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	РН 8
Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	РН 9
Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	РН14
Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	РН16
Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	РН18

Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	РН23
Надавати консультативні послуги та технічну допомогу з питань технічного та криптографічного захисту інформації та кіберзахисту.	РН25

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки»:

1. Демонструє здатність обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки (РН 7).
2. Демонструє вміння досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури (РН 8).
3. Має навички аналізу, розробки та супроводжування систем управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки (РН 9).
4. Має навички аналізу, розробки і супроводжування систем аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому (РН14).
5. Демонструє здатність приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень (РН16).
6. Освоїв методологію планування навчання, а також супроводжування та контролювання роботи з персоналом у напряму інформаційної безпеки та/або кібербезпеки (РН18).
7. Має навички в обґрунтуванні вибору програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації (РН23).
8. Володіє навичками надавання консультативних послуг та технічної допомоги з питань технічного та криптографічного захисту інформації та кіберзахисту (РН25).

4. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни є: **оцінювання домашніх і самостійних завдань та контрольних робіт; оцінювання завдань, виконаних студентами під час практичних занять, іспит.**

Контрольні заходи включають такі ***форми контролю та критерії оцінювання результатів навчання:*** поточний, модульний та підсумковий контроль.

Поточний контроль– оцінювання рівня знань, умінь і навичок здобувачів, що здійснюється в ході навчального процесу проведенням усного опитування, контрольної роботи, тестування, домашнього завдання тощо.

Результатом *модульного контролю* є модульна бальна оцінка, за якою підбивається підсумок роботи студентів впродовж модуля у відповідності до кредитно-трансферної системи оцінювання знань.

Підсумковий семестровий контроль проводиться у формі іспиту в обсязі навчального матеріалу, що визначений навчальною програмою, та в терміни, встановлені графіком навчального процесу. При семестровому контролі отримані здобувачем згідно кредитно-трансферної системи оцінювання знань переводяться в оцінки за національною шкалою та за шкалою ЄКТС.

Комплексний показник успішності здобувача другого рівня вищої освіти, його обізнаності в предметі, що вивчається, характеризує якість його знань, систематичність, творчість, активність та самостійність. Максимальна сума балів за всі види робіт (контрольні, самостійне вивчення, практичні (семінарські) заняття) з даного курсу становить 100 балів.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота						**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	Т6	20	**60**
6	6	6	3	8	8		

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне оцінювання та самостійна робота						**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	Т6	20	**60**
6	6	6	3	8	4		

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	**Модуль 1**		**Модуль 2**	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Практичні заняття	6	40	6	40
Разом		**40**		**40**

Критерії оцінювання модульної контрольної роботи

Завдання для **модульної контрольної роботи** складається з 4 питань, кожне з яких оцінюється максимально у 5 балів. При оцінюванні кожного завдання контрольної роботив раховується обсяг і правильність виконаних завдань: оцінка "відмінно" ставиться за правильне виконання всіх завдань; оцінка "добре" ставиться за виконання 75 % усіх завдань; оцінка "задовільно" ставиться, якщо правильно виконано більше 50% запропонованих завдань; оцінка "незадовільно" ставиться, якщо завдань виконано менше від 50 %. Неявка на модульну контрольну роботу – 0 балів.

Критерії оцінювання підсумкового семестрового контролю

Усі завдання, передбачені програмою, мають бути виконані у встановлені терміни. Якщо студент/ка був/ла відсутній на заняттях, він/вона мають можливість відпрацювати навчальні питання та завдання під час самостійної підготовки та обов'язково звітують про опанування навчального матеріалу викладачу. Студенти, які пропустили більше 30% з тих занять, де було передбачено оцінювання, не відзвітували за індивідуальну та самостійну роботу, до семестрового контролю не допускаються. У разі коли студент/ка не виконав/ла умови допуску до складання семестрового контролю, завчасно, але не пізніше трьох робочих днів до складання семестрового контролю, рішенням кафедри йому/їй встановлюється індивідуальний термін ліквідації заборгованості. Якщо заборгованість неліквідована у визначений кафедрою термін, то студент/ка вважається таким/ою, що не виконав/ла вимоги робочої програми навчальної дисципліни і у відомості обліку успішності йому/їй виставляється оцінка «незараховано» за національною шкалою і FX – за шкалою ЄКТС. При повній відсутності позитивних поточних оцінок, за визначені звітності, і не ліквідації заборгованості у визначений кафедрою термін, студенту курс з навчальної дисципліни не зараховується і в графі "підсумкова оцінка", йому виставляється оцінка "недопущений" за національною шкалою і F за шкалою ЄКТС. У такому випадку студенту/ці йому пропонується пройти повний курс повторно. У разі відмови його/її відраховують з університету.

Іспит отримує студент/ка, що виявив/ла знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, ознайомлений/на з рекомендованою літературою. Підсумкова оцінка розраховується за накопичувальною системою. При цьому максимальна кількість балів встановлюється наступним чином: за змістовий модуль №1 – 100 балів; за змістовий модуль №2 – 100 балів.

При виставленні оцінки враховуються результати навчальної роботи здобувача протягом семестру.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	ОцінкаECTS	Оцінка за національною шкалою	
		Екзамен та диференційований залік	Залік
90 – 100	**A**	відмінно	Зараховано
82-89	**B**	добре	
74-81	**C**		
64-73	**D**	задовільно	
60-63	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	Не зараховано
0-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	

За бажанням студента результуюча підсумкова екзаменаційна оцінка може бути визначена як інтегрована оцінка засвоєння всіх тем дисципліни і кількісно дорівнює середньому арифметичному балів, отриманих за кожний модуль.

Результати підсумкового контролю знань заносяться до екзаменаційної відомості.

Дотримання академічної доброчесності

Під час навчання учасники освітнього процесу зобов'язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил (https://vumonline.ua/course/academic-integrity-at-the-university/), якими мають керуватися

учасники освітнього процесу з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності науково-педагогічним складом передбачає: посилання на джерела інформації у разі використання ідей, тверджень, відомостей; надання достовірної інформації про результати досліджень та власну педагогічну (науково-педагогічну, творчу) діяльність.

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, тверджень, відомостей; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності як: повторне проходження оцінювання (підсумковий модульний контроль, підготовка індивідуального завдання за іншою темою тощо).

Перевірка індивідуальних робіт здобувачів на наявність академічного плагіату проводиться викладачем або спеціально призначеним для цього працівником УжНУ за допомогою програмного продукту, що використовується в УжНУ з визначення рівня унікальності роботи.

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1. Зміст навчальної дисципліни

Модуль 1. ПРАВОВІ ЗАСАДИ СИСТЕМ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

Тема 1. **Вступ**

*Цілі та завдання навчальної дисципліни «*Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки*». Місце дисципліни у навчальному процесі підготовки спеціаліста з кібербезпеки. Структура, зміст тематичного плану вивчення дисципліни; навчально-методична література. Особливості вивчення дисципліни; форми контролю знань, умінь та навичок учнів. Напрями науково-дослідної роботи студентів.*

Тема 2. **Правові засади кібербезпеки України**

Правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі. Регулювання відносин щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Тема 3. **Закон України «Про захист інформації в інформаційно-комунікаційних системах»**

Правові основи організації відносин у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Порядок доступу до інформації, перелік користувачів та їх повноваження, порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимоги щодо захисту, які встановлені законом.

Тема 4. **Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»**

Правові основи організації та діяльності Державної служби спеціального зв'язку та захисту інформації України. Статус Державної служби спеціального зв'язку та захисту інформації України. Загальна структура та організація діяльності державної служби спеціального зв'язку та захисту інформації України.

Тема 5. **Закон України «Про електронні комунікації»**

Правові та організаційні основи державної політики у сферах електронних комунікацій та радіочастотного спектра, а також права, обов'язки та відповідальність фізичних і

юридичних осіб, які беруть участь у відповідній діяльності або користуються електронними комунікаційними послугами.

Розвиток ринків доступу до електронних комунікаційних мереж та ринків електронних комунікаційних послуг, що забезпечить розгортання та використання електронних комунікаційних мереж високої та надвисокої пропускної здатності, сприятиме інвестуванню в розвиток таких мереж та їх інфраструктури, розвитку конкуренції, а також сумісність електронних комунікаційних послуг, доступність, безпечність електронних комунікаційних мереж і послуг та переваги для кінцевих користувачів; створення засад для ефективного та гармонізованого користування радіочастотним спектром для забезпечення економічного, соціального, інформаційного та культурного розвитку, державної безпеки, обороноздатності, виконання міжнародних зобов'язань, а також для забезпечення і захисту інтересів держави та користувачів радіочастотного спектра; забезпечення надання на всій території України якісних, прийнятних та доступних для населення послуг шляхом забезпечення ефективної конкуренції та вибору електронних комунікаційних послуг, а також задоволення потреб і захист прав та законних інтересів кінцевих користувачів послуг, у тому числі осіб з інвалідністю, щодо доступу до електронних комунікаційних послуг на рівні з іншими споживачами.

Тема 6. **Закон України «Про основні засади забезпечення кібербезпеки України»**

Правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Модуль 2. ТЕХНІЧНІ ЗАСАДИ СИСТЕМ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

Тема 1. **Міжнародний досвід виявлення вразливостей і реагування на кіберінциденти та кібератаки**

Основи реагування на кіберінциденти. Визначення інциденту кібербезпеки. Порівняння різних типів інцидентів кібербезпеки. Реагування на інциденти ІБ. Цілі процесу реагування. Події та інциденти. Необхідність реагування на інциденти. Створення політики, плану та процедур реагування на інциденти. Елементи політики. Елементи плану. Елементи процедури. Обмін інформацією із зовнішніми сторонами.

Тема 2. **Спеціалізоване програмне забезпечення виявлення вразливостей та тестування**

Інструменти для первинного реагування (SysInternals, AVZ, Gmer, YARA). Інструменти для збирання даних (GRR Rapid Response, Forensic Toolkit, DD, Belkasoft RAM Capturer). Інструменти для аналізу потенційних загроз (Threat Lookup – Kaspersky Threat Intelligence Portal, Sandbox – Kaspersky Threat Intelligence Portal). Інструменти для аналізу дампів пам'яті. Інструменти для аналізу образів диска (Strings). Інструменти для видалення загроз (Kaspersky Virus Removal Tool, Kaspersky Rescue Disk). Спеціальні рішення Лабораторії Касперського. Аналітичні звіти Лабораторії Касперського про загрози класу APT.

Тема 3. **Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA**

Моделі команд. Вибір моделі команди. Персонал реагування на інциденти. Залежності всередині організацій. Служби групи реагування на інциденти. Координація. Координаційні відносини. Угоди про спільне використання та вимоги до звітності. Методи обміну

інформацією (спеціальні, частково автоматизовані). Питання безпеки. Обмін детальною інформацією. Інформація про вплив на бізнес. Технічна інформація. Рекомендації.

Тема 4. **Виявлення і реагування на кібератаки на рівні робочих та серверних станцій**

Розвідка та збір даних (Reconnaissance). Вибір способу атаки (Weaponization). Доставка (Delivery). Експлуатація (Exploitation). Закріплення (Installation). Виконання команд (Command and Control). Досягнення мети (Actions on Objective)

Тема 5. **Збір телеметрії інформаційно-комунікаційних систем, поняття активного сенсору**

Підготовка. Підготовка до врегулювання інцидентів. Запобігання інцидентам. Виявлення та аналіз. Вектори атаки. Ознаки події. Джерела прекурсорів та індикатори. Аналіз інцидентів. Документація про інцидент. Пріоритизація інцидентів. Повідомлення про інцидент. Стримування, викорінення та відновлення. Вибір стратегії стримування. Збір та обробка доказів. Ідентифікація атакуючих хостів. Викорінення та відновлення. Події після інциденту. Використання зібраних даних про інциденти. Зберігання доказів. Контрольний перелік обробки інцидентів.

Тема 6. **Моделювання та аналіз кібератак**

Інструменти для первинного реагування (SysInternals, AVZ, Gmer, YARA). Інструменти для збирання даних (GRR Rapid Response, Forensic Toolkit, DD, Belkasoft RAM Capturer). Інструменти для аналізу потенційних загроз (Threat Lookup – Kaspersky Threat Intelligence Portal, Sandbox – Kaspersky Threat Intelligence Portal). Інструменти для аналізу дампів пам'яті. Інструменти для аналізу образів диска (Strings). Інструменти для видалення загроз (Kaspersky Virus Removal Tool, Kaspersky Rescue Disk). Спеціальні рішення Лабораторії Касперського. Аналітичні звіти Лабораторії Касперського про загрози класу APT.

5.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Форма навчання - денна:					
	Усього	у тому числі				
		лекції	практичні (семінарські)	Практичні (лабораторні)	індивідуальна робота	Самостійна робота
Модуль 1						
Тема 1. **Вступ**	10	2		2		6
Тема 2. **Правові засади кібербезпеки України**	8	2				6
Тема 3. **Закон України «Про захист інформації в інформаційно-комунікаційних системах»**	10	2		2		6

Тема 4. **Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»**	10	2		2		6
Тема 5. **Закон України «Про електронні комунікації»**	10	2		2		6
Тема 6. **Закон України «Про основні засади забезпечення кібербезпеки України»**	10	2		2		6
Модульна контрольна робота	2			2		
Разом за І модуль	60	12		12		36
Модуль 2						
Тема 1. **Міжнародний досвід виявлення вразливостей і реагування на кіберінциденти та кібератаки**	10	2		2		6
Тема 2. **Спеціалізоване програмне забезпечення виявлення вразливостей та тестування**	8	2				6
Тема 3. **Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA**	10	2		2		6
Тема 4. **Виявлення і реагування на кібератаки на рівні робочих та серверних станцій**	10	2		2		6
Тема 5. **Збір телеметрії інформаційно-комунікаційних систем, поняття активного сенсору**	10	2		2		6
Тема 6. **Моделювання та аналіз кібератак**	10	2		2		6
Модульна контрольна робота	2			2		
Разом за ІІ модуль	60	12		12		36
Разом за 1 семестр	120	24		24		72

5.3. Теми практичних (семінарських) занять

№ з/п	Назва теми	Кількість годин
1	**Обробка інформації, історія та основні поняття**	2
2	**Закон України «Про інформацію». Поняття інформації з обмеженим доступом**	2
3	**Поняття тріади К Ц Д**	2

4	**Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу**	2
5	**Вивчення сайту Державної служби спеціального зв'язку та захисту інформації України**	2
6	**Модульна контрольна робота**	2
7	**ISO/IEC 27001 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»**	2
8	**Вивчення сайту CERT-UA**	2
9	**Збір та кореляція подій безпеки, включаючи збір мережевої телеметрії з детальною інформацією про мережеві потоки та сесії**	2
10	**Проведення моніторингу електронного комунікаційного трафіку з метою виявлення кібератак та кіберінцидентів**	2
11	**Виявлення та аналіз зловмисного програмного забезпечення, включаючи відстеження та запобігання спробам його поширення на мережевому рівні**	2
12	**Модульна контрольна робота**	2
	Разом	24

5.4. Самостійна робота

Самостійна робота магістра є одним із засобів оволодіння навчальним матеріалом у час, вільний від обов'язкових навчальних занять, і є невід'ємною складовою процесу вивчення цієї дисципліни. Основними напрямками самостійної роботи магістрів з навчальної дисципліни «Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» є опрацювання рекомендованої літератури, а також вивчення окремих питань, винесених на самостійне опрацювання.

№	Назва роботи	Кількість годин
1	Проробка лекційного матеріалу	24
2	Підготовка до практичних занять	24
3	Проробка питань програми, які не викладались на лекціях	24
	Разом	**72**

6. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

У процесі вивчення дисципліни використовується система інформаційних ресурсів: дидактичні, програмні, інтернет-мережа, бібліографічні, бібліотечні. Серед них нормативно-правова база (закони, постанови, положення, накази): сайти Міністерства

освіти і науки України, інтернет-ресурси, періодичні видання, наукові праці професорсько-викладацького складу, тези та матеріали наукових конференцій.

Наочні засоби: мультимедійні презентації у програмі Microsoft Office Power Point; відеоматеріали з каналу Youtube; зразки друкованих медіа джерел, схематизованих навчально-методичних матеріалів і довідкових статей; роздавальні матеріали – табличні й схематичні основи, інфографіка тощо.

Технічні засоби: лекційний курс передбачає використання технічних засобів навчання, комп'ютерних проекторів.

Для дистанційного навчання використовується Moodle(e-learn.uzhnu.edu.ua) та Google Meet.

7. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. /[КорченкоО.Г.,ГнатюкС.О., КазмірчукС.В.та ін.]. – Київ: Центр навч.-наук. та наук.-пр.виданьНАСБ України, 2014. – 190с. URL: https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf

2. Якименко Ю. М. Аналіз стану використання методичних підходів до оцінки рівня економічної безпеки підприємства.- / Ю. М. Якименко, Т.М. Мужанова // Економіка. Менеджмент. Бізнес.– № 1(31). – К.: ДУТ, 2020. – С. 64-6 9. URL: http://journals.dut.edu.ua/index.php/emb/article/view/2377/2277

3. 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. — Київ : ДУТ, 2015.— 288 с.

4. Якименко Ю. М. Системний аналіз методологічних підходів до управління підприємством у сфері інформаційних технологій. // II Міжнародна науковопрактична конференції «Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку», 11лютого 2021 року. — Київ: ДУТ, 2021. - С. 279-282. URL: http://www.dut.edu.ua/uploads/n_9074_59003267.pdf

5. Якименко Ю. М. Особливості використання методичних заходів захисту інформації підприємства від сучасних видів загроз, кібератак і ризиків // Матеріали: Всеукраїнська наукова конференція, Актуальні проблеми кібербезпеки, 27 жовтня 2021. Тези доповідей — Київ: ДУТ, 2021. - С.173-176. URL: http://www.dut.edu.ua/uploads/p_2099_79407917.pdf

6. Суворова О.Р. Керування механізмами захисту. Міжнародні стандарти інформаційної безпеки. Урок №12. URL: https://naurok.com.ua/keruvannyamehanizmami-zahistu-mizhnarodni-standarti-informaciyno-bezpeki-104726.html

7. Рой Я.В., Мазур Н.П., Складанній П.М.Аудит інформаційної безпеки –основа ефективного захисту підприємств./ Кібербезпека: освіта, наука, техніка №1(1) - Київ: Київський університет імені Бориса Грінченка, 2018 с.87-93. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/23

8. Якименко Ю. М. Методологічні аспекти впровадження системного аналізу в побудові системи управління інформаційною безпекою.- Професійний розвиток фахівців у системі освіти дорослих: історія, теорія,технології: програма IУ-ої Всеукраїнської Інтернет-конференції 16 жовтня 2019 р., м. Київ.-/за наук. ред. В.В. Сидоренко; упорядкування Я.Л. Швень, М.І. Скрипник. К.: Агроосвіта, 2019. - С.41-43.

Допоміжна література

1. Якименко Ю. М. Аналіз стану використання методичних підходів до оцінки рівня економічної безпеки підприємства.- / Ю. М. Якименко, Т.М. Мужанова // Економіка. Менеджмент. Бізнес. – №1 – К.: ДУТ, 2020. – С. 64-69. URL: http://journals.dut.edu.ua/index.php/emb/article/view/2386

2. Якименко Ю. М. Методичні піходи системного аналізу до вирішення проблем управління інформаційною безпекою в системі національної безпеки держави / Ю.М. Якименко // Актуальні проблеми управління інформаційною безпекою держави: XII Всеукраїнська науково-практична конференція. Збірник тез наукових доповідей. Електронне видання — Київ: Нац. акад. СБУ, 2021. - С. 162-164. URL: http://academy.ssu.gov.ua/upload/file/%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D1%96%D1%8F%2026.03.2021.p df

3. Якименко Ю. М. Управління інцидентами інформаційної безпеки в організації системи забезпечення кіберстійкості підприємства. Матеріали Всеукраїнської НПК Інтернет-конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу», 25 лютого 2021 року. Тези доповідей – Київ: ННІЗІ ДУТ, 2021.- С.24-25. URL: http://www.dut.edu.ua/uploads/l_2173_91341086.pdf.

4. Yakymenko, Y., Muzhanova, T., & Lehominova, S. (2021). СИСТЕМНИЙ АНАЛІЗ ТЕХНІЧНИХ СИСТЕМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ВІД КОМПАНІЇ FIREEYE. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 4(12), 36-50. URL: https://doi.org/10.28925/2663-4023.2021.12.3650

5. ДСТУ ISO/IEC 27001:2015 (Ідентичний до міжнародного ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements).

6. ДСТУ ISO/IEC 27002:2015 (Ідентичний до міжнародного ISO/IEC 27002:2013 Cor 1:2014). Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.

7. ДСТУ ISO/IEC 27031:2015 (ISO/IEC 27031:2011, IDT). Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу

8. ДСТУ ISO/IEC 27035-1:2018 (ISO/IEC 27035-1:2016, IDT). Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами.

9. ДСТУ ISO/IEC 27035-2:2018 (ISO/IEC 27035-2:2016, IDT). Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти.

10. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements.

11. ISO/IEC 27002:2013 Technologies de l’information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l’information

12. ДСТУ ISO/IEC 27007:2018 (ISO/IEC 27007:2017, IDT). Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою

13. ДСТУ ISO 19011:2019 (ISO 19011:2018, IDT). Настанови щодо проведення аудитів систем управління

14. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с. URL: https://dut.edu.ua/uploads/l_2230_88161692.pdf .

Корисні Інтернет ресурси.

1. https://www.armoredpenguin.com/crossword/ – Середовище для створення кросвордів
2. https://learningapps.org – Створення вправ
3. https://worditout.com – Створення хмар
4. https://jamboard.google.com – Jamboard
5. https://uk.wikipedia.org/wiki – Wiki сервіс
6. https://wordart.com – WordArt
7. http://disted.edu.vn.ua/media/bp/html/etusivu.htm – Онляндія

8. https://www.blogger.com – Блогер (для створення блогів)
9. https://www.google.com – Форми (для створення опитування)
10. https://go.playposit.com – Play posit