Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«___» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕХНОЛОГІЇ БЕЗПЕКИ МЕРЕЖЕВОЇ ТА SMART ІНФРАСТРУКТУРИ»

для студентів

спеціальності	125 Кібербезпека та захист інформації
освітнього рівня	другого (магістерського)
освітньої програми	125.00.02 Безпека інформаційних і комунікаційних систем

2023 – 2024 навчальний рік

Розробники:

Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Соколов Володимир Юрійович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____ (підпис) _____ Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.02 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.

Керівник освітньої програми ___ (підпис) ___ Володимир СОКОЛОВ

Робочу програму перевірено

___.___. 2022 р.

Заступник декана _____ (підпис) _____ Євген ІВАНІЧЕНКО

Пролонговано:

на 2023/2024 н.р. _____ (підпис) Складанний П.І., «23» 08 2023 р., протокол № 8

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	7 / 210	
Курс	1	
Семестр	1	
Кількість змістових модулів з розподілом:	3	
Обсяг кредитів	7	
Обсяг годин, в тому числі:	210	
Аудиторні	56	
Модульний контроль	12	
Семестровий контроль	60	
Самостійна робота	82	
Форма семестрового контролю	Екзамен, курсова робота	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Технології безпеки мережевої та Smart інфраструктури» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів другого (магістерського) рівня відповідно до навчальних планів спеціальності 125 Кібербезпека та захист інформації.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Технології безпеки мережевої та Smart інфраструктури» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Технології безпеки мережевої та SMART інфраструктури» складається з 3-х змістових модулів: 1. Архітектура безпеки мережевої інфраструктури. 2. Методи забезпечення безпеки мережевої інфраструктури. 3. Захищеність SMART технології та інфраструктури. Обсяг дисципліни – 210 год (7 кредитів).

Метою викладання навчальної дисципліни «Технології безпеки мережевої та SMART інфраструктури» є формування у студентів уміння вирішувати задачі захисту інформаційно-телекомунікаційних систем, отримання компетентностей в області захисту об'єктів мережевої інфраструктури від несанкціонованого доступу до ресурсів.

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері інформаційної та кібернетичної безпеки та набуття наступних компетентностей:

Фахові компетентності

ФК-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.

ФК-3: Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

ФК-6: Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ФК-8: 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.

ФК-9: 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.

ФК(У)-11: Здатність до застосування сучасних безпекових інформаційних та SMART-технологій у сфері захисту інформації.

ФК(У)-12: Здатність до виявлення уразливостей та забезпечення безпеки телекомунікаційних технологій і SMART-інфраструктури, розслідування інцидентів інформаційної та/або кібербезпеки та протидії злоякісному програмному забезпеченню.

загальні компетентності:

КЗ-2: Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях

КЗ-3: Здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати:

- основні методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури;
- основи стратегії і політики інформаційної безпеки та/або кібербезпеки організації;
- методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах;
- завдання систем аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому;
- порядок до застосування сучасних безпекових інформаційних та SMART-технологій у сфері захисту інформації;
- методики виявлення уразливостей та забезпечення безпеки телекомунікаційних технологій і SMART-інфраструктури;

уміти:

- аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту;
- розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури;
- розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки;
- виявляти уразливості інформаційних систем та ресурсів;
- супроводжувати систему моніторингу ефективності функціонування інформаційних систем і технологій;
- аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту;

- вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик;
- обгрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації;
- проектувати захищені (з урахуванням загроз) проводові і безпроводові телекомунікаційні та SMART -системи.

та досягнути наступні ***програмні результати***:

РН 6: Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН 8: Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН 9: Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН 10: Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН 14: 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.

РН 19: Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН 20 Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН 23: Обгрунтовувати 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.

РН(У) 24: Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях та SMART -інфраструктурі. Вміти проектувати захищені (з урахуванням загроз) проводові і безпроводові телекомунікаційні та SMART -системи.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Архітектура безпеки мережевої інфраструктури							
Тема 1. Системи управління та забезпечення захисту інформації в АС.	28	4		6			18
Тема 2. Архітектура безпеки корпоративної мережевої інфраструктури.	28	4			6		18
Модульний контроль	4						
Разом	60	8		6	6		36
Змістовий модуль 2. Методи забезпечення безпеки мережевої інфраструктури							
Тема 3. Забезпечення безпеки Веб-додатків.	28	4		6			18
Тема 4. Методи побудови захищеної мережевої інфраструктури.	28	4			6		18
Модульний контроль	4						
Разом	60	8		6	6		36
Змістовий модуль 3. Захищеність SMART технології та інфраструктури							
Тема 5. Захищеність SMART технології та інфраструктури.	26	4		6	6		10
Модульний контроль	4						
Разом	30	4		6	6		10
Підготовка та проходження контрольних заходів	60						
Усього	**210**	**20**		**18**	**18**		**82**

5. Програма навчальної дисципліни

Змістовий модуль 1. Архітектура безпеки мережевої інфраструктури

Основні питання:

- Системи управління та забезпечення захисту інформації в АС
- Принципи побудови мереж VPN
- Створення списків управління доступом
- Архітектура безпеки корпоративної мережевої інфраструктури
- Налагодження та дослідження роботи віртуальних локальних мереж
- Налагодження та дослідження роботи віртуальних локальних мереж
- Налагодження Kali Linux на зовнішньому носії для професійної оцінки безпеки комп'ютерних систем

Змістовий модуль 2. Методи забезпечення безпеки мережевої інфраструктури

Основні питання:

- Програмні засоби виявлення SQL-ін’єкцій у Веб-додатках
- Методи перевірки і фільтрації вхідних даних у Веб-додатках

- Методи маршрутизації за протоколами OSPF, EIGRP та RIP
- Безпека міжмережевої взаємодії
- Аналіз методів SQL-ін'єкцій
- Дослідження роботи протоколу маршрутизації EIGRP, OSPF та RIP

Змістовий модуль 3. Захищеність SMART технології та інфраструктури

Основні питання:

- SMART технологія та інфраструктура
- Захищеність SMART інфраструктури інтернету речей
- Аналіз XSS-атак при різній складності експлуатації уразливостей
- Налагодження та дослідження роботи DHCP-сервера та DHCP-клієнтів
- Особливостями реалізації функції Port Security при протидії атакам MAC-Spoofing та MAC-Flooding

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен.
- *Комп'ютерного контролю:* тестові програми.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	4	4	4	4	2	2
Відвідування семінарських занять							
Відвідування практичних занять	1	3	3	3	3	3	3
Відвідування лабораторних занять	1	3	3	3	3	3	3
Робота на семінарському занятті							
Робота на практичному занятті	10	3	30	3	30	3	30
Лабораторна робота (в тому числі допуск, виконання, захист)	10	3	30	3	30	3	30
Виконання завдань для самостійної роботи	5	4	20	4	20	2	10
Виконання модульної роботи	25	1	25	1	25	1	25
Разом		-	115	-	115	-	103
Максимальна кількість балів: 333							
Розрахунок коефіцієнта: 333/60=5,55							

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Архітектура безпеки мережевої інфраструктури		36	20
1	Тема 1. Системи управління та забезпечення захисту інформації в АС..	18	10
	Лекція 1. Системи управління та забезпечення захисту інформації в АС.: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	9	5
	Лекція 2. Принципи побудови мереж VPN: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	9	5
2	Тема 2. Архітектура безпеки корпоративної мережевої інфраструктури.	18	10
	Лекція 1. Створення списків управління доступом: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	9	5
	Лекція 2. Архітектура безпеки корпоративної мережевої інфраструктури: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	9	5
Змістовий модуль 2. Методи забезпечення безпеки мережевої інфраструктури		36	20
3	Тема 3. Забезпечення безпеки Веб-додатків.	18	10
	Лекція 1. Програмні засоби виявлення SQL-ін’єкцій у Веб-додатках:	9	5

	• опрацювання фахових видань відповідно до теми лекції та підготовка реферату.		
	Лекція 2. Методи перевірки і фільтрації вхідних даних у Веб-додатках: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	9	5
4	Тема 4. Методи побудови захищеної мережевої інфраструктури.	18	10
	Лекція 1. Методи маршрутизації за протоколами OSPF та EIGRP: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	9	5
	Лекція 2. Безпека міжмережевої взаємодії: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	9	5
Змістовий модуль 3. Захищеність SMART технології та інфраструктури.		10	10
5	Тема 5. Захищеність SMART технології та інфраструктури.	10	10
	Лекція 1. SMART технологія та інфраструктура: • опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	5	5
	Лекція 2. Захищеність SMART інфраструктури інтернету речей: опрацювання фахових видань відповідно до теми лекції та підготовка реферату.	5	5
	Разом	82	50

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп'ютерний тест, що складається 20 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Підсумкове оцінювання у 1-му семестрі здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – комбінована. Іспит оцінюється у 40 балів за розподілом: 20 балів – комплексний тест з дисципліни; 20 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями з побудови інформаційних мереж та управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

Оцінювання практичного завдання відбувається в межах від 0 до 20 балів, згідно критеріїв оцінювання, й здійснюється з урахуванням: рівнів сформованості аналітико-синтетичних, творчих та методичних умінь необхідних для побудови захищених інформаційних та інформаційно-телекомунікаційних (автоматизованих) систем.

Бали за виконання тесту та бали за виконання практичного завдання додаються. Оцінювання результатів засвоєння теоретичних знань та оцінювання сформованості практичних навичок володіння цифровими технологіями студентами, продемонстровані на екзамені, представлене у таблиці.

Підсумкова кількість балів (max – 40)	Оцінка за 4-бальною шкалою
1 – 23	«незадовільно»
24 – 29	«задовільно»
30 – 35	«добре»
36 – 40	«відмінно»

Орієнтовний перелік питань для семестрового контролю

1. Характеристики систем управління та забезпечення захисту інформації в автоматизованих системах.
2. Характеристика підсистеми реєстрації і обліку.
3. Характеристика підсистеми забезпечення цілісності.
4. Протоколи і технології доступу до ресурсів інформаційно-комунікаційних систем.
5. Основні принципи механізмів захисту від несанкціонованого доступу до інформації в АС.
6. Віртуальні мережі. Принципи і протоколи.
7. Три основних види віртуальних приватних мереж.
8. Способи утворення захищених віртуальних каналів.
9. Рівні інформаційної інфраструктури корпоративної інформаційно-комунікаційної системи.
10. Протоколи і технології доступу до ресурсів мереж на канальному рівні.
11. Характеристика протоколу PPTP.
12. Характеристика протоколу L2TP.
13. Характеристика протоколу Secure Sockets Layer / Transport Layer Security.
14. Характеристика технології IPSec.
15. Призначення і зміст списків управління доступом.
16. Механізм реалізації списків управління доступом ACL.
17. Три основних типи профілів доступу.
18. Процес створення профілю доступу.
19. Приклад налаштування комутатора для профілю Ethernet.
20. Приклад налаштування комутатора для профілю IP.
21. Архітектура та моделі безпеки корпоративної мережевої інфраструктури.
22. Модель Захмана для корпоративної архітектури.
23. Модель SABSA для корпоративної архітектури.
24. Архітектура та моделі безпеки політики.
25. Загальні відомості застосуванн SQL-ін’єкцій у Веб-додатках.
26. Характеристика атаки SQL-ін'єкцій (SQL Injection Attacks, SQLIAs)
27. Загальні принципи атаки на інформаційну інфраструктуру.
28. Уразливості веб-додатків, які можуть експлуатуватися при застосуванні атак на ін'єкцію SQL
29. Програмні засоби виявлення SQL-ін’єкцій у Веб-додатках
30. Експлуатація вразливостей Веб-додатків.
31. Експлуатація вразливостей слабких паролів при управлінні доступом.
32. Експлуатація вразливостей інформаційної інфраструктури при здійсненні IP-спуфінгу.

33. Способи здійснення атаки «Ін’єкція» в мережевій інфраструктурі.
34. Методи отримання вмісту бази даних за допомогою SQL-ін’єкцій.
35. Виявлення ознак наявності злоякісного програмного забезпечення системними засобами мережних інфраструктур.
36. Методи перевірки і фільтрації вхідних даних у Веб-додатках.
37. Способи фільтрації вхідних даних Validate (перевірка).
38. Способи фільтрації вхідних даних Sanitize (очищення).
39. Способи фільтрації вхідних даних Flags (прапори).
40. Методи динамічної маршрутизації
41. Побудова маршрутів за допомогою протоколів динамічної маршрутизації RIP, OSPF, EIGRP.
42. Характеристика централізованої маршрутизації.
43. Характеристика розподіленої маршрутизації.
44. Характеристика гібридної маршрутизації.
45. Математична модель ІКС.
46. Ілюстрація роботи алгоритму Беллмана-Форда.
47. Протокол маршрутизації OSPF.
48. Приклад використання алгоритмів Дійкстри та Беллмана-Форда.
49. Протокол маршрутизації EIGRP.
50. Визначення та зміст понять SMART технологія та інфраструктура.
51. Характеристика SMART критеріїв.
52. Концепція Smart інфраструктури.
53. Інфраструктура Інтернету речей.
54. Підключення облаштувань Інтернету речей.
55. Типи мереж Інтернету речей.
56. Мережі з низьким енергоспоживанням і малим діапазоном.
57. Мережі з низьким енергоспоживанням і широкою зоною охоплення (LPWAN).
58. Платформи Інтернету речей.
59. Протоколи Інтернету речей. Рівень застосувань.
60. Протоколи Інтернету речей. Рівень транспортування.
61. Протоколи Інтернету речей. Рівень мережі.
62. Проблеми забезпечення безпеки Інтернету речей.

Шкала відповідності оцінок

Рейтингова оцінка	Сума балів за всі види навчальної діяльності	Значення оцінки
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов’язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов’язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов’язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична карта дисципліни

Разом: 210 год., лекції – 20 год., практичні заняття – 18 год., лабораторні роботи – 18 год., модульний контроль – 12 год., самостійна робота – 82 год., семестровий контроль – 60 год.

Модулі (назви, бали)	**Змістовий модуль 1 Архітектура безпеки мережевої інфраструктури (115 балів)**				**Змістовий модуль 2. Методи забезпечення безпеки мережевої інфраструктури (115 бали)**				**Змістовий модуль 3. Захищеність SMART технології та інфраструктури (103 бали)**	
Лекції (теми, бали)	Системи управління та забезпечення захисту інформації в АС. (1 бал)	Принципи побудови мереж VPN (1 бал)	Створення списків управління доступом (ACL) (1 бал)	Архітектура безпеки корпоративної мережевої інфраструктури. (1 бал)	Програмні засоби виявлення SQL-ін'єкцій у Веб-додатках (1 бал)	Методи перевірки і фільтрації вхідних даних у Веб-додатках (1 бал)	Методи маршрутизації за протоколами OSPF та EIGRP (1 бал)	Безпека міжмережевої взаємодії (1 бал)	SMART технологія та інфраструктура (1 бал)	Захищеність SMART інфраструктури інтернету речей (1 бал)
Практичні, семінарські заняття (теми, бали)	Встановлення та налагодження Kali Linux на зовнішньому носії для професійної оцінки безпеки комп'ютерних систем. (33 бали)				Аналіз методів SQL-ін'єкцій (33 бали)				Аналіз XSS-атак при різній складності експлуатації уразливостей (33 бали)	
Лабораторні заняття (теми, бали)	Побудова комп'ютерних мереж на базі концентраторів, мостів, комутаторів (11 балів)	Налагодження та дослідження роботи віртуальних локальних мереж (11 балів)	Списки керування доступом ACL. (11 балів)		Дослідження роботи протоколу маршрутизації EIGRP (11 балів)	Дослідження роботи протоколу маршрутизації OSPF (11 балів)	Дослідження роботи протоколу маршрутизації RIP (11 балів)		Налагодження та дослідження роботи DHCP-сервера та DHCP-клієнтів (11 балів)	Особливостями реалізації функції Port Security при протидії атакам MAC-Spoofing та MAC-Flooding (22 бали)
Самостійна робота	Самостійна робота (20 балів)				Самостійна робота (20 балів)				Самостійна робота (10 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)				Модульна контрольна робота 2 (25 балів)				Модульна контрольна робота 3 (25 балів)	
Підсумковий контроль (вид, бали)	Курсова робота (100 балів)								Екзамен (40 балів)	

8. Рекомендовані джерела

Основна

1. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К.: МК-Прес, 2005. – 432 с.
2. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
3. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.
4. Демида Б.А. Обельовська К.М., Яковина В.С. Основи адміністрування LAN у середовищі MS Windows: навч. посіб. Львів : Видавництво Львівської політехніки, 2013. 488 с.
5. Ємельянов С.Л. Основи інформаційної безпеки. – Одеса: Фенікс, 2014.– 357 с.
6. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 5 липня 1994 року № 80/94-ВР, Відомості Верховної Ради України (ВВР), 1994, № 31. – с.286
7. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу»
8. Пороло Є. Застосування концепції Data Bank в мережі хмарного IoT / Євгеній Пороло // ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНОТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА СИСТЕМ / Євгеній Пороло. –м. Київ, Україна: ISSN (print)2663-502X, ISSN (online) 2664-3057, 2020. –С. 368.
9. Пороло Є. Удосконалена архітектура мережі для хмарного Інтернету речей / Є. Пороло, В. Курдеча // ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ / Є. Пороло, В. Курдеча. –м. Київ, Україна: ISSN(print) 2663-502X, ISSN(online) 2664-3057, 2020. –С. 219–221.
10. Фролов А. В. Бази даних в Мережі інтернет: Практичний посібник по створенню Webдодатків з базами даних / А. В. Фролов., 2000. – 448 с.
11. Яковина В.С. Основи безпеки комп’ютерних мереж: Навчальний посібник. Львів: НВФ "Українські технології", 2008. – 396 с.

Додаткова

1. Dac-Nhuong Le IoT: Security and Privacy Paradigm / Dac-Nhuong Le, Souvik Pal : CRC Press, 2020. – 399 p.
2. Fei Hu Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations / Fei Hu : CRC Press, 2016. – 604 p.
3. ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management.
4. ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements.
5. ISO/IEC TR 27035:2011. Information technology − Security techniques − Information security incident management.
6. ISO/IEC 20000:2011. Information technology. Service management. Part 2: Code of practice.
7. Defining Incident Management Processes for CSIRTs: A Work in Progress // CMU/SEI-2004-TR-015: ESC-TR-2004-015 Chris Alberts, Audrey Dorofee, Georgia Killcrece October 2004 Networked Systems Survivability Program.

9. Інформаційні ресурси

1. Staying Ahead of Privacy and Security Risks in Internet of Things. [Електронний ресурс] // – Режимдоступу: https://www.natlawreview.com/article/staying-ahead-privacy-and-security-risks-internet-things
2. SpiegelmockM.IoT Security Through Open Certification. [Електронний ресурс] //– Режимдоступу:

http://www.sfbayisoc.org/2017/06/21/iot-security-through-open-certification/
3. Lisa Goeke, Security Challenges of the Internet of Things [Електронний ресурс]. – Режим доступу: https://www.theseus.fi/bitstream/handle/10024/128420/Goeke_Lisa.pdf?sequence=1
4. Kateryna Savchenko, Vladislav Vyshnovskiy. System bezpieczeństwa inteligentnego domu //Materiały konferencyjne. Konferencja studenckich kół naukowych Pionu Hutniczego [Електронний ресурс] – Режим доступу: http://www.kolanaukowe.agh.edu.pl/ph/dzialalnosc//
5. Flynn D. IoT considerations —cloud services —IaaS, PaaS, SaaS, build your own [Електронний ресурс] / Des Flynn. –2015. –Режим доступу до ресурсу: https://medium.com/lattice-research/iot-considerations-server-sideiaas-paas-saas-1f55afc03185.