СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Технології забезпечення безпеки безпроводових і мобільних мереж»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Гайдур Галина Іванівна, доктор технічних наук, професор.</td><td colspan="2">Контактна інформація лектора (e-mail), сторінка курсу</td><td colspan="2">e-mail: ikbdut@gmail.com;
сторінка курсу в –
https://classroom.google.com/c/NzI2MTU2Njk4MDg5?cjc=rtt62fa</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">12 Інформаційні технології</td><td colspan="2">Рівень вищої освіти</td><td colspan="2">Магістр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">Кібербезпека</td><td colspan="2">Семестр</td><td colspan="2">10</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">Інформаційна та кібернетична безпека</td><td colspan="2">Тип дисципліни</td><td colspan="2">Вибіркова компонента освітньо-наукової програми</td></tr>
<tr><td rowspan="3">Обсяг:</td><td rowspan="2">Кредитів ECTS</td><td rowspan="2">Годин</td><td colspan="5">За видами занять:</td></tr>
<tr><td>Лекцій</td><td>Семінарських занять</td><td>Практичних занять</td><td>Лабораторних занять</td><td>Самостійна підготовка</td></tr>
<tr><td>5</td><td>150</td><td>36</td><td>-</td><td>18</td><td>18</td><td>78</td></tr>
<tr><td colspan="10">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="10">Взаємозв’язок у структурно-логічній схемі</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="7">Прикладна загальна теорія систем інформаційної та кібербезпеки .
Технології виявлення уразливостей мережевих ресурсів.</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="7">Кваліфікаційна робота</td></tr>
<tr><td>Мета курсу:</td><td colspan="9">Формування знань та вмінь щодо застосування технології забезпечення кібербезпеки мобільних та безпроводових пристроїв в інформаційній системі організацій.</td></tr>
<tr><td colspan="10">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="5">Soft- skills / Загальні компетентності (ЗК)</td><td colspan="5">Hard-skills / Спеціальні компетентності (СК)</td></tr>
<tr><td colspan="5">КЗ1. Здатність застосовувати знання у практичних ситуаціях.
КЗ6. Знання та розуміння предметної області і професійної діяльності.
КЗ8. Здатність використовувати інформаційні та комунікаційні технології.
КЗ10. Здатність застосовувати кращі практики у професійній діяльності.</td><td colspan="5">КФ1. 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.
КФ2. 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.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та</td></tr>
</table>

	визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Програмні результати навчання (ПРН)

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
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.
РН23. 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.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Тема 1. Мета та основні завдання застосування технологій забезпечення безпеки мобільних та безпереводових мереж.			
Лекція 1.Основи безпеки локальних безпроводових мереж WLAN. ***Знати***: Роль і місце безпеки мобільних та безпереводових пристроїв в безпроводових локальних мереж (WLAN). Загальні принципи побудови корпоративної WLAN.Концепція використання мобільних пристроїв. Аутентифікація і шифрування. Етапи проектування безпроводової мережі. Архітектура Secure Wireless LAN. Архітектура впровадження WIPS для корпоративної безпроводової мережі. ***Формування компетенцій:*** КЗ1, КЗ6, КФ5 ***Програмні результати навчання:*** РН5, РН6 ***Рекомендовані джерела:*** 1-6	Лекція 1 2 год	1	Лекція-візуалізація

Пз1. Застосування технології забезпечення безпеки мобільних та безпереводових мереж. ***Знати:***. Роль і місце технологій забезпечення безпеки мобільних та безпереводових мереж Загальні вимоги щодо видів мобільних пристроїв в інформаційній системі організації. Види атак на безпроводову мережу корпоративної інформаційної системи. ***Формування компетенцій:*** К31, К36, КФ5 ***Програмні результати навчання:*** РН5, РН6 ***Рекомендовані джерела:*** 1-6	Практичне заняття 1 2 год	2	Усне опитування, виконання завдань на практичне застосування знань і вмінь застосування мобільних та безпроводових пристроїв згідно вимог.
Лб1. Дослідження технологій моніторингу корпоративних безпроводових мереж ***Знати:***. Роль і місце технологій забезпечення безпеки мобільних та безпереводових пристроїв. Загальні вимоги щодо видів пристроїв в інформаційній системі організації. ***Вміти:*** застосовувати сучасні мобільні та безпроводові пристрої в інформаційній системі організації. ***Формування компетенцій:*** К31, К36, КФ5 ***Програмні результати навчання:*** РН5, РН6 ***Рекомендовані джерела:*** 1-6	Лабораторне заняття 1 2 год	3	Дослідження
Основи забезпечення кібербезпеки сучасного підприємства. ***Знати:*** поняття «інформаційна система організації» як об'єкт захисту; превентивні, детективні та коректив ні заходи забезпечення кібербезпеки сучасного підприємства; поняття «подія безпеки», поняття «мобільні пристрої»; мета застосування технології забезпечення безпеки мобільних та безпереводових мереж. ***Вміти:*** застосовувати заходи забезпечення безпеки інформаційної системи організації. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 1-6	Самостійна робота 1 6 год	3	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 2. Політики безпеки застосування мобільних та безпереводових пристроїв в інформаційній системі організації			
Лекція 2. Політики безпеки застосування мобільних та безпереводових пристроїв в інформаційній системі організації	Лекція 2 2 год	1	Лекція-візуалізація

Знати: зміст політики безпеки та визначення основних ризиків щодо використання мобільних та безпроводових пристроїв в інформаційній системі організації. ***Формування компетенцій:*** КЗ1, КЗ6, КФ5 ***Програмні результати навчання:*** РН5, РН6 ***Рекомендовані джерела:*** 1-6			
Пз2. Створення політик безпеки при застосуванні мобільних та безпроводових пристроїв в інформаційній системі організації ***Знати:***. зміст політики безпеки та визначення ризиків щодо використання мобільних та безпроводових пристроїв в інформаційній системі організації ***Вміти:*** аналізувати та оцінювати стан захищеність інформаційних систем до ризиків використання мобільних та безпроводових пристроїв. ***Формування компетенцій:*** КЗ1, КЗ6, КФ5 ***Програмні результати навчання:*** РН5, РН6 ***Рекомендовані джерела:*** 1-6	Практичне заняття 2 2год	2	Практичні навики створення політик безпки при використанні мобільних та безпроводових пристроїв в ІС організації.
Лб3. Дослідження ризиків застосування мобільних та безпроводових пристроїв в інформаційній системі організації ***Знати:***. зміст основних ризиків щодо використання мобільних та безпроводових пристроїв в інформаційній системі організації ***Вміти:*** аналізувати та оцінювати захищеність інформаційних систем до ризиків використання мобільних та безпроводових пристроїв. ***Формування компетенцій:*** КЗ1, КЗ6, КФ5 ***Програмні результати навчання:*** РН5, РН6 ***Рекомендовані джерела:*** 1-6	Лабораторне заняття 2 4 год	3	Дослідження ризиків використання мобільних та безпроводових пристроїв.
Знати: поняття «інформаційна система організації» як об’єкт захисту; превентивні, детективні та корективні заходи забезпечення кібербезпеки сучасного підприємства; поняття «політики безпеки», поняття «мобільні пристрої»; ризики застосування мобільних та безпереводових пристроїв. ***Вміти:*** застосовувати заходи забезпечення безпеки інформаційної системи організації. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27	Самостійна робота 2 6 год	3	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

Рекомендовані джерела: 1-6			
Тема 3. Концепції застосування мобільних пристроїв в інформаційній системі організації			
Лекція 3 Концепції застосування мобільних пристроїв в інформаційній системі організації. ***Знати***: основи застосування концепції використання пристроїв для забезпечення діяльності фахівців з кібербезпеки. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 1-6	Лекція 3 2 год	1	Лекція-візуалізація
Пз 3 Заходи впровадження концепції BYOD в організації ***Знати:*** основнні принципи концепції BYOD. ***Вміти:*** застосовувати на практиці основні положення концепції застосування мобільних та безпроводових пристроїв в організації. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 5, 6	Практичне заняття 3 2 год	2	Практичне застосування концепції застосування мобільних пристроїв в інформаційній системі організації.
Лб 3. Порівняння концепції застосування мобільних пристроїв в організації ***Знати****: основні принципи концепцій застосування мобільних пристроїв* **Вміти:** застосовувати на практиці основні положення концепції застосування мобільних та безпроводових пристроїв в організації. **Формування компетенцій**: ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 **Програмні результати навчання:** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 Рекомендовані джерела: 5, 6	Лабораторне заняття 3 2 год	3	Дослідження основних принципів концепцій
Знати: сучасні процеси дослідження аналізу та створення заходів забезпечення функціонування інформаційних систем організацій ***Вміти:*** вміти надавати пропозиції щодо заходів забезпечення функціонування інформаційних систем організацій. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 1-6	Самостійна робота 3 6 год	3	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

Тема 4. Роль і місце технології управління мобільними пристроями (MDM) в інфраструктурі організацій.			
Лекція 4. Роль і місце технології управління мобільними пристроями (MDM) в інфраструктурі організацій. ***Знати***: основи прикладного і спеціалізованого програмного забезпечення управління мобільними пристроями (MDM) в інфраструктурі організацій. ***Вміти***: використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 1-6	Лекція 4 2 год	1	Лекція-візуалізація
Пз 4. Аналаз проблеми щодо використання мобільних пристроїв в інформаційній системі організації. ***Знати***: основи прикладного і спеціалізованого програмного забезпечення управління мобільними пристроями (MDM) в інфраструктурі організацій. ***Вміти***: використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки.	Практичне заняття 4 2 год	2	Практичне навики використання (MDM) в інфраструктурі організацій
Тема 4. Роль і місце технології управління мобільними пристроями (MDM) в інфраструктурі організацій. ***Лб 4. Дослідження методів та засобів управління мобільними пристроями в інформаційній системі організації.*** ***Знати***: основи прикладного і спеціалізованого програмного забезпечення управління мобільними пристроями (MDM) в інфраструктурі організацій. ***Вміти***: аналізувати, контролювати та забезпечувати систему управління мобільними пристроями для забезпечення доступу до інформаційних ресурсів згідно встановленої стратегії.	Лабораторне заняття 4 2 год	3	Дослідження методів та засобів

Знати: основи прикладного і спеціалізованого програмного забезпечення управління мобільними пристроями (MDM) в інфраструктурі організацій. ***Вміти***: аналізувати, контролювати та забезпечувати систему управління мобільними пристроями для забезпечення доступу до інформаційних ресурсів згідно встановленої стратегії.	Самостійна робота 4 6 год	3	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 5. Технологія управління мобільними пристроями організації			
Лекція 5 Огляд MaaS360 *Знати:* Можливості, типи розгортання, програми реєстрації та методи автентифікації, необхідні для керування пристроями організації	Лекція 5 2 год	1	Лекція-візуалізація
Пз5 Початок роботи з MAAS360 ***Знати***: ключові компоненти, які допомагають управляти всіма пристроями організації. ***Вміти***: застосовувати основні принципи щодо управління мобільними пристроями для забезпечення доступу до інформаційних ресурсів згідно встановленої стратегії.	Практичне заняття 5 2 год	2	Практичне застосування технології управління мобільними пристроями MAAS360.
Пз5 Початок роботи з MAAS360 **Вміти:** Застосовувати навігацію домашньою сторінкою порталу адміністратора Maas360, використання довідки та покрокових інструкцій, розуміти призначення служби підтримки IBM MaaS360, налаштувати реєстрації Apple, налаштувати реєстрації Android Enterprise, додавати пристрої	Лабораторне заняття 5 2 год	3	Виконання індивідуального завдання
Тема 5. Технологія управління мобільними пристроями організації **Лекція 5 Огляд MaaS360** ***Знати:*** Можливості, типи розгортання, програми реєстрації та методи автентифікації, необхідні для керування пристроями організації **Вміти** Застосовувати навігацію домашньою сторінкою порталу.	Самостійна робота 5 6 год	3	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Лекція 6. Огляд можливостей і функціональності MaaS360 **Знати:** базові знання з управління мобільнимим пристроями, знати стратегію розгортання технології MDM MAAS360, **Вміти:** застосовувати можливості і функції MaaS360	Лекція 6 2 год	1	Лекція-візуалізація

ПЗ 6 Огляд можливостей і функціональності MaaS360 **Вміти:** Керувати мобільною робочою силою та забезпечувати захист організації MAAS360, застосовувати можливості і функції MaaS360	Практичне заняття 6 2 год	2	Практичне застосування технології управління мобільними пристроями MAAS360.
Лб 6 Огляд можливостей і функціональності MaaS360 **Вміти:** Керувати мобільною робочою силою та забезпечувати захист організації MAAS360, застосовувати можливості і функції MaaS360	Лабораторне заняття 6 2 год	3	Самостійне виконання завдання щодо застосування технології управління мобільними пристроями MAAS360.
Огляд можливостей і функціональності MaaS360, керування кінцевими точками до вбудованої безпеки з MaaS360. **Знати:** базові знання з управління мобільнимим пристроями, знати стратегію розгортання технології MDM MAAS360, **Вміти:** застосовувати можливості і функції MaaS360	Самостійна робота 6 6 год	3	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Лекція 7 Стратегії розгортання **Знати:** знати стратегію розгортання технології MDM MAAS360, поняття облікових записів, режими автентифікації користувачів та адміністраторів.	Лекція 7 2 год	1	Лекція-візуалізація
Пз 7 Стратегії розгортання **Знати:** знати стратегію розгортання технології MDM MAAS360, поняття облікових записів, режими автентифікації користувачів та адміністраторів **Вміти:** практично застосовувати знання методів та засобів управління мобільними пристроями в організації на базі рішення MAAS360	Практичне заняття 7 2 год	2	Тестування
Лб 7. Стратегії розгортання **Знати:** знати стратегію розгортання технології MDM MAAS360, поняття облікових записів, режими автентифікації користувачів та адміністраторів **Вміти:** практично застосовувати знання методів та засобів управління мобільними пристроями в організації на базі рішення MAAS360	Лабораторне заняття 5 2 год	3	Практичне застосування стратегії розгортання MAAS360
Описувати можливості продукту MaaS360 та архітектуру SaaS Пояснювати ключові компоненти MaaS360, які використовуються для інтеграції мобільних пристроїв із корпоративними та хмарними ресурсами Знати ключову інформацію та завдання, необхідні для планування розгортання корпоративної мобільності IBM MaaS360.	Самостійна робота 7 6 год	3	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

Оцінювати стратегію розгортання IBM MaaS360. Реєстрація та керуйте мобільними пристроями Android та iOS за допомогою MaaS360 https://learn.ibm.com/course/view.php?id=13935			
Лекція 8. MaaS360: Планування реалізації **Знати:** знати стратегію розгортання технології MDM MAAS360, поняття облікових записів, режими автентифікації користувачів та адміністраторів **Вміти:** практично застосовувати знання методів та засобів управління мобільними пристроями в організації на базі рішення MAAS360	Лекція 8 2 год	1	Лекція-візуалізація
Пз8. Стратегія аутентифікації на прикладі MaaS360. **Знати:** знати стратегію розгортання технології MDM MAAS360, поняття облікових записів, режими автентифікації користувачів та адміністраторів **Вміти:** практично застосовувати знання методів та засобів управління мобільними пристроями в організації на базі рішення MAAS360	Практичне заняття 8 2 год	2	Практичне застосування методики управління мобільними пристроями
Лб 8. Стратегія аутентифікації на прикладі MaaS360. **Знати:** знати стратегію розгортання технології MDM MAAS360, поняття облікових записів, режими автентифікації користувачів та адміністраторів **Вміти:** практично застосовувати знання методів та засобів управління мобільними пристроями в організації на базі рішення MAAS360	Лабораторне заняття 8 2 год	3	Практичне застосування стратегії аутентифікації в MAAS360
Тема 5. Технологія управління мобільними пристроями організації Оцінювати стратегію розгортання IBM MaaS360. Стратегія аутентифікації мобільнимих пристроїв Android та iOS за допомогою MaaS360	Самостійна робота 8 6 год	3	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 6. Тенденції та майбутні перспективи застосування технології управління мобільними пристроями **Знати:** знати обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технологі **Вміти:** практично обирати програмне забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень кібербезпеки на основі сучасних знань.	Лекція 9 2 год	1	Пояснювально-ілюстративний, лекція-візуалізація
	Практичне заняття 7 2 год	2	Усне опитування, виконання завдань на практичне застосування знань і вмінь

	Лабораторне заняття 5 2 год	3	Дослідження
	Самостійна робота 9 6 год	3	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп‘ютерне обладнання, мережа Інтернет, програмний комплекс IBM QRadar SIEM , програмний комплекс ESET PROTECT, демо версія IBM MAAS360

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Park Foreman. Vulnerability Management. Second Edition. CRC Press Taylor & Francis Group, 2019. 330 p.
2. Technical Guide to Information Security Testing and Assessment. Recommendations of the National Institute of Standards and Technology. Karen Scarfone. Murugiah Souppaya. Amanda Cody. Angela Orebaugh. NIST Special Publication 800-115. (Sep. 2008). 80 p. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.
3. 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 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.
4. Tom Palmaers. Implementing a vulnerability management process. SANS Institute. Accepted: 03/23/2013. 24 p. https://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180.
5. NIST SP 800-124 Rev. 1 https://doi.org/10.6028/NIST.SP.800-124r1
6. MaaS360 Overview - IBM Training - Global. (2024, March 01). Retrieved from https://www.ibm.com/training/course/maas360-overview-SLA5619
7. MaaS360 Features and Functionality Review - IBM Training - Global. (2024, March 01). Retrieved from https://www.ibm.com/training/course/maas360-features-and-functionality-review-SLA6005
8. Гайдур Г. І., Шулімова Д. Д., Бойко А. О., Постніков Є. І. Модель забезпечення кібербезпеки інтернету речей. Телекомунікаційні та інформаційні технології. № 2 (2024). С 4-13. DOI: 10.31673/2412-4338.2024.020515
9. Гайдур, Г. І., Гахов, С. О., Марченко, В. В., & Гайдур, К. В. (2024). Концептуальна модель виявлення фішингових атак на основі використання методів опорних векторів. Сучасний захист інформації, 2(58), 24–33. https://doi.org/10.31673/2409-7292.2024.020003
10. Скибун,О. Ж., Гайдур,Г. І., & Гахов С. О. (2024). Аналіз використання концепції BYOD в корпоративних інформаційних системах. Сучасний захист інформації, 1(57), 50–56. https://doi.org/10.31673/2409-7292.2024.010006 .
11. Легомінова, С.В., Гайдур Г.І. Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм. Кібербезпека: освіта, наука, техніка. – 2023. - №2(22). – С. 564-67. DOI 10.28925/2663-4023.2023.22.5467
12. Ганченко М.І., Гайдур Г.І., Гахов С.О., Дмітрієв В.Є. “Актуальність та перспектива розвитку Privileged Access Management рішень.” Зв’язок. 2022. №1 (2022). С. 3-9. DOI: 10.31673/2412-9070.2022.010310 Доступ: https://con.dut.edu.ua/index.php/communication/article/view/2578
13. Гайдур Г. І., Гахов С. О., Бригинець А. А. Виявлення мережевих аномалій з використанням алгоритмів нейронних мереж. Телекомунікаційні та інформаційні технології. № 1 (2023). С. 61-73. DOI: 10.31673/2412-4338.2023.016173
14. Гайдур Г. І. Гахов С. О, Сич М. В., Дмітрієв В. Є. Аналіз загроз мережевого трафіку рівнів моделі OSI для динамічного розрахунку RTO в контексті боротьби з DDOS атаками. Телекомунікаційні та інформаційні технології. № 3 (2023). С. 12-21. DOI: 10.31673/2412-4338.2023.031221

15. Haidur, H. The Method of Increasing the Efficiency of Signal Processing Due to the Use of Harmonic Operators // Zamrii, I., Haidur, H., Sobchuk, A., Zinchenko, K., Polovinkin, I. // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory, ATIT 2022 - Proceedings, 2022, pp. 138–141.(Scopus)
16. Гайдур Г.І., Гахов С.О., Марченко В.В. Метод побудови динамічної моделі логічного об'єкта інформаційної системи та визначення закону його функціонування. Radioelectronic and Computer Systems, 2022, no. 1(101). С. 129-140. doi: 10.32620/reks.2022.1.10. (Категорія А, Scopus).
17.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо аспірант відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації аспірант повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату аспірант отримує за завдання 0 балів.
- Аспірант, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни аспірант видаляється з заняття, за заняття отримує 0 балів.

*** КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання аспірантом 60 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 1 бала
	• звіт про виконання практичного завдання	за кожен звіт максимум 1 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	10-15 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Залік проходить у письмовій формі.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Аспірант демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції	Відмінно / Зараховано (А)

	співставляти дані об‘єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов’язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об’єму матеріалу, передбаченого робочою програмою, або аспірант проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	аспіранта в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	
82-89	Аспірант демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує аспіранту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	Добре / Зараховано (B)
75-81	Аспірант в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
64-74	Аспірант засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Аспірант має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, аспірант з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв’язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Аспірант може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни аспірант виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у аспіранта відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не

			зараховано (FX) *В залікову книжку не проставляється*
1-34	Аспірант повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Аспірант не допущений до здачі заліку.	**Незадовільний** Аспірант не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*