

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ТЕХНОЛОГІЇ СТВОРЕННЯ ТА ЗАСТОСУВАННЯ КОМПЛЕКСУ ЗАСОБІВ ІНФОРМАЦІЇ ТА ОХОРОНИ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ»

| | | | | | | | |
|--|--|--|---|---|----------------------|------------------------|--------------------------|
| Лектор курсу | | Котенко Андрій Миколайович, кандидат технічних наук, доцент кафедри систем інформаційного та кібернетичного захисту | Контактна інформація лектора (e-mail), сторінка курсу в Moodle | e-mail: dutkotenko@gmail.com сторінка курсу в Moodle – http://dl.dut.edu.ua/course/view.php?id=675 | | | |
| Галузь знань | | 12 Інформаційні технології | Рівень вищої освіти | Магістри | | | |
| Спеціальність | | Кібербезпека | Семестр | 9 | | | |
| Освітня програма | | Магістр Кібербезпеки | Тип дисципліни | Професійної та практичної підготовки | | | |
| Обсяг: | Кредитів ECTS | Годин | За видами занять: | | | | |
| | | | Лекцій | Семінарських занять | Практичних занять | Лабораторних занять | Самостійна підготовка |
| | 3 | 90 | 12 | - | 12 | 12 | 54 |
| АНОТАЦІЯ КУРСУ | | | | | | | |
| Взаємозв'язок у структурно-логічній схемі | | | | | | | |
| Освітні компоненти, які передують вивченню | | Компонентна база засобів технічного захисту інформації | | | | | |
| Освітні компоненти для яких є базовою | | Написання атестаційної роботи магістра. | | | | | |
| Мета курсу: | Опанування сучасними технологіями щодо забезпечення інформаційної безпеки на об'єкті інформаційної діяльності. | | | | | | |
| Компетентності відповідно до освітньої програми | | | | | | | |
| Soft- skills / Загальні компетентності (ЗК) | | | | Hard-skills / Спеціальні компетентності (СК) | | | |
| ЗК-3. Знання інформаційних технологій – здатність використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах. ЗК-4. Навички керування проектами – здатність демонструвати своєчасність та спланованість у дослідженні, здатність до адаптації та дії в новій ситуації, здатність розробляти та управляти проектами. | | | | ФК-1. Інтегративна компетентність ФК-3. Організаційно-комунікативна компетентність ФК-4. Професійна компетентність ФК-5. Загальнонаукова компетентність ФК-6. Політехнічна компетентність ФК-7. Інженерна компетентність | | | |
| Програмні результати навчання (ПРН) | | | | | | | |

ПРН-5. Уміти розробляти логічні схеми, складати план-проспекти та технічні завдання на виконання наукових досліджень. ПРН 9. Уміти здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності.

ПРН-13. Уміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією.

ПРН-18. Уміти аналізувати існуючі технології, методи і засоби застосування шкідливого програмного забезпечення, нівелювання уразливостей мережевих та Web-ресурсів.

ПРН-22. Уміти розробляти та впроваджувати дослідницькі проекти в галузі знань «інформаційні технології» спеціальності «кібербезпека» для забезпечення безпеки мережевої інфраструктури.

ПРН-24. Уміти здійснювати науково-технічне супроводження заходів з формування і коригування програмних комплексів забезпечення безпеки та захисту інформації на об'єктах інформаційної діяльності.

ПРН-25. Уміти визначати можливості для підприємницької та громадської діяльності за напрямом захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної діяльності.

ПРН-31. Уміти проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної діяльності.

ПРН-32. Уміти обґрунтовувати раціональні шляхи щодо захисту інформації на об'єктах інформаційної діяльності та інформації, що циркулює в ІТ системах та мережах.

| ОРГАНІЗАЦІЯ НАВЧАННЯ | | | |
|--|-------------------------------|--------------------|---|
| Тема, опис теми | Вид заняття | Оцінювання за тему | Форми і методи навчання/питання до самостійної роботи |
| Змістовий модуль 1. «Загальна характеристика систем управління доступом» | | | |
| Тема 1. Інформація як об'єкт захисту <u>Знати:</u> Знати розподіл інформації за режимом правового доступу. <u>Вміти.</u> Користуватись нормативними документами щодо інформаційних ресурсів. <u>Формування компетенцій:</u> ЗК1, ФК-1. <u>Результати навчання:</u> ПРН-25. <u>Рекомендовані джерела:</u> 3-5,8. | Лекція 1 2 год. | 10 | Лекція-візуалізація |
| | Практичне заняття 1 2 год. | | Загальні положення. |
| | Лабораторна 1. 2 год. | | Кодифікація нормативних документів ТЗІ. |

| | | | |
|--|---------------------------------|----|--|
| | Самостійна робота | | УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". від 28 грудня 2021 року № 685/2021. |
| <p>Тема 2. <i>Захист акустичної інформації</i></p> <p>Знати: Загрози акустичній інформації. Методи захисту акустичної інформації.</p> <p>Вміти: Реалізовувати системи захисту акустичної інформації на об'єктах інформаційної діяльності, здійснювати вибір методів і засобів захисту акустичної інформації, здійснювати пошук закладних пристроїв.</p> <p>Формування компетенцій:ЗК1, ФК-4, ФК-5</p> <p>Результати навчання:ПРН-13, ПРН-17.</p> <p>Рекомендовані джерела: 1,3-7,8,</p> | Лекція 2 2 год | 10 | Лекція-візуалізація |
| | Практичне заняття 2 2 год | | Засоби захисту акустичної інформації: генератор просторового зашумлення, нелінійний локатор, скануючий приймач, детектор електромагнітного поля. |
| | Лабораторн а 2. 2 год. | | Пошук радіо закладних пристроїв. |
| | Самостійна робота | | Методи та засоби захисту акустичної інформації. Генератор просторового зашумлення, нелінійний локатор, скануючий приймач, детектор електромагнітного поля. |
| <p>Тема 3. <i>Загрози інформації в автоматизованих системах</i></p> <p>Знати: Загрози інформації в автоматизованих системах, причини їх виникнення.</p> <p>Вміти: обґрунтовувати та реалізовувати систему захисту від витоку на об'єкти інформаційної діяльності, інформації через ПЕМВН, здійснювати вибір методів і засобів для захисту інформації в АС від витоку технічними каналами.</p> <p>Формування компетенцій:ЗК1, ФК-1, ФК-4,</p> <p>Результати навчання: ПРН-17, ПРН-24.</p> <p>Рекомендовані джерела: 1,3-</p> | Лекція 3 2 год | 7 | Лекція-візуалізація |
| | Практичне заняття 3 2 год | | Засоби захисту інформації від витоку технічними каналами |
| | Лабораторн а 3. 2 год. | | Дослідження генератору просторового зашумлення. |

| | | | |
|---|-------------------------------|----|--|
| | Самостійна робота | | Галузь використання. Класифікація пристроїв захисту інформації в АС від витоку технічними каналами. |
| <p>Тема 4. <i>Електричні канали витоку інформації.</i> Знати: Причини виникнення електричних каналів витоку інформації. Вміти: обґрунтовувати та реалізовувати системи захисту інформації від витоку електричним каналом на об'єктах інформаційної діяльності, здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності від витоку електричним каналом. Формування компетенцій:ЗК1, ФК-4, ФК-7. Результати навчання:ПРН-13, ПРН-25. Рекомендовані джерела: 7 ,8</p> | Лекція 4 2 год | 7 | Лекція-візуалізація |
| | Практичне заняття 4 2 год | | Пристрої захисту інформації від витоку електричними каналами. |
| | Лабораторна 4. 2 год. | | Дослідження генератору лінійного зашумлення. |
| | Самостійна робота | | Пристрої захисту інформації від витоку електричними каналами. |
| <p>Тема 5 <i>Склад та призначення систем відеоспостереження</i> Знати: Склад системи відеоспостереження. Її роль у системі захисту інформації. Вміти: Проектувати систему відео спостереження на ОІД. Формування компетенцій:ЗК1, ЗК3, ФК-1, ФК-8 Результати навчання: ПРН-5, ПРН-24, ПРН-32 Рекомендовані джерела: 1,10.</p> | Лекція 5 2 год. | 10 | Лекція-візуалізація |
| | Практичне заняття 5 2 год. | | Практичне ознайомлення со складом системи відео спостереження. |
| | Лабораторна 5. 2 год. | | Дослідження відеокамер системи відео спостереження. |
| | Самостійна робота | | Підсилена аутентифікація та ідентифікація. Адміністрування і система збору статистики. Існуючі структури СКУД. Мережевий контролер СКУД. |

| | | | |
|--|------------------------------|----|---|
| <p>Тема 6. <i>Проектування системи захисту інформації на ОІД.</i> <u>Знати:</u> Існуючі системи захисту інформації (КТЗІ, КСЗІ) <u>Вміти:</u> Застосовувати знання при практичному проектування систем захисту інформації. <u>Формування компетенцій:</u>ЗК1, ФК-1,ФК-6, ФК-8 <u>Результати навчання:</u>ПРН-5, ПРН13, ПРН-17, ПРН-22, ПРН-24, ПРН-32, <u>Рекомендовані джерела:</u>,14 ,17, 18.</p> | Лекція 9 2 год | 10 | Лекція-візуалізація |
| | Практичне заняття 6 2 год | | Методика створення КСЗІ в ІТС. Методика створення КТЗІ. |
| | Лабораторна а 6. 2 год. | | Розробка Акту категоріювання ОІД. Розробка Акту обстеження ОІД. |
| | Самостійна робота | | Нормативні документи проектування систем захисту інформації. |

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Навчальна лабораторія засобів контролю доступу «HIKVISION»
- Програмне забезпечення.WindowsXP, 8,10, MicrosoftOffice.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Закони України:

1. Закон України «Про інформацію» від 02.10.1992 № 2657-ХІІ
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
3. Закон України «Про державну таємницю» від 21.01.1994 № 3855-ХІІ
4. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

Укази президента:

5. № 685/2021Указ президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».
6. Указ президента України №685/2021. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію

інформаційної безпеки". від 28 грудня 2021 року

Постанова Кабінету Міністрів України

7. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373
8. Постанова Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.2010 № 518.

Нормативні документи

9. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу
10. НД 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. <https://zakon.rada.gov.ua/rada/show/v0215519-13>.
11. <http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art id=120206&cat id=89769&ctime=1421836194327>
12. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
13. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Перед проектні роботи.
14. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.
15. НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення
16. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
17. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

Основна

18. Хорев А.А. Захист інформації від витоку по технічним каналам. Ч.1. Технічні канали витоку інформації. Навчальний посібник. — К.:, 2015. — 320 с.
19. Максименко Г.А., Хорошко В.О. Методи виявлення, обробки та ідентифікації сигналів радіозакладних приладів. - К.: ООО „Поліграф Консалтинг”, 2004.-317 ст.
20. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методи та засоби захисту інформації. – К: Арий, 2015, т. 1, 2 - 806 ст.
21. Хорошко В.О., Чирков Д.В., Браїловський М.М. Основи захисту інформації, навчальний посібник. – К.: НАУ, 2014. – 87.

***КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання студентом 30 балів у сукупності за всіма темами дисципліни

| Форми контролю | Види навчальної роботи | Оцінювання |
|----------------|------------------------|------------|
|----------------|------------------------|------------|

| | | | |
|--|--|---|---|
| ПОТОЧНИЙ КОНТРОЛЬ | • присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу) | за кожне відвідування 0,5 бала | |
| | • звіт про виконання практичного завдання | за кожен звіт максимум 1 бал | |
| | • Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом. | Звільняється від екзамену | |
| Додаткова оцінка | • Модульний контроль № 1 «Загальна характеристика систем управління доступом» | максимальна оцінка – 15 балів | |
| РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ) | Модульний контроль № 2 «Засоби СКУД»» | максимальна оцінка – 15 балів | |
| | Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо. | Звільняється від іспиту | |
| | Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій формі. | 30 балів | |
| | Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо. | Звільняється від іспиту | |
| Додаткова оцінка | Метою екзамену є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Екзамен проходить у письмовій формі. | 30 балів | |
| ПІДСУМКОВЕ ОЦІНЮВАННЯ екзамен | Метою екзамену є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Екзамен проходить у письмовій формі. | 30 балів | |
| ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ | | | Кри |
| бали | Студент 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 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- | Високий Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції аспіранта в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні | Оцінка /затис в екзаменаційній відомості |

| | | | |
|--------|---|--|--------------------------------|
| | 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. | питань, що відносяться до дисципліни, яка вивчається. | |
| 90-100 | Студент 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 вивченні дисципліни | Відмінно / Зараховано (А) |
| 82-89 | Студент 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 (В) |
| 75-81 | Студент 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 розглядалися 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 | Добре / Зараховано (С) |
| 64-74 | Студент 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 (D) |
| 60-63 | Студент 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 вивченні дисципліни | Задовільно / Зараховано (Е) |
| 5 - 5 | Студент повністю не виконав вимог робочої програми навчальної дисципліни. | Незадовільний | Незадовільно з |

| | | | |
|---|--|--|---|
| | Його знання на підсумкових етапах навчання є фрагментарними. Аспірант не допущений до здачі заліку. | Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни | можливістю повторного складання) / Не зараховано (FX) <i>В залікову книжку не проставляється</i> |
| 3 | | | |