Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра автоматизації проектування енергетичних процесів і систем

НАУКОВО-ДОСЛІДНА РОБОТА ЗА ТЕМОЮ МАГІСТЕРСЬКОЇ ДИСЕРТАЦІЇ.

ЧАСТИНА 2. НАУКОВО-ДОСЛІДНА РОБОТА ЗА ТЕМОЮ МАГІСТЕРСЬКОЇ ДИСЕРТАЦІЇ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	другий (магістерській)
Галузь знань	*12 Інформаційні технології*
Спеціальність	*121 Інженерія програмного забезпечення*
Освітня програма	*Інженерія програмного забезпечення інтелектуальних кібер-фізичних систем і веб-технологій*
Статус дисципліни	*вибіркова*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*1 курс весняний семестр*
Обсяг дисципліни	*2 кредити (60 год), серед них 18 годин практичних занять, 41 годин самостійної роботи, 1 година залік*
Семестровий контроль/ контрольні заходи	*Залік*
Розклад занять	*Науково-педагогічний працівник*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Практика:* *д.т.н., професор Гаврилко Євген Володимирович, gev.1964@ukr.net, тел. 067-506-91-85*
Розміщення курсу	*Googleclassroom, Zoom, Кампус.*

Програманавчальної дисципліни

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

Для отримання науково-освітнього рівня магістра потрібно написати магістерську дисертацію – самостійну науково-дослідницьку роботу, яка виконує кваліфікаційну функцію, тобто готується з метою публічного захисту. Автор має володіти вмінням демонстрації власної наукової кваліфікації, бути спроможним самостійно провадити науковий пошук і розв'язувати конкретні наукові завдання. Зважаючи на науковий зміст подібної випускної праці, вона має характеризуватись внутрішньою єдністю й відображати хід та результати розробки вибраної теми. Магістерська дисертація носить узагальнюючий характер, оскільки є своєрідним підсумком підготовки магістра та має вміщувати самостійні оригінальні наукові дослідження студента. Зміст кожної частини магістерської дисертації визначається її темою. Вибір теми, етапи підготовки, пошук бібліографічних джерел для здійснення та вивчення розлогого літературного огляду й добір

фактичного матеріалу, методика написання, правила оформлення та захисту магістерської дисертації потребують пильної уваги, бо їх правильне виконання є запорукою її успішного захисту.

Метою навчальної дисципліни є формування у студентів методологічної культури та цілісної системи знань, умінь і навичок з організації і проведення науково-дослідної роботу у професійній галузі.

Предметом вивчення є організація науково-дослідної діяльності у професійно-орієнтованих напрямках, формування компетентностей і професійних навиків самостійної наукової роботи відповідно до вимог та у зв'язку з підготовкою до написання магістерської дисертації.

Програмні результати

Результатом вивчення навчальної дисципліни є формування у студентів **компетентностей**:

- здатність до самостійного освоєння нових методів дослідження, зміні наукового й науково-виробничого профілю своєї діяльності (ЗК3);
- здатність генерувати нові ідеї й нестандартні підходи до їх реалізації (креативність), досліджувати проблеми з використанням системного аналізу, синтезу та інших методів (ЗК4);
- здатність організовувати розвиток творчої ініціативи, раціоналізації, винахідництва, впровадження досягнень вітчизняної та закордонної науки, техніки, використання передового досвіду, що забезпечують ефективну роботу підрозділу, вести науково-дослідну діяльність у міжнародному середовищі (ЗК5);
- здатність аналізувати, верифікувати, оцінювати повноту інформації в ході професійної діяльності, при необхідності доповнювати й синтезувати відсутню інформацію й працювати в умовах невизначеності (ЗК7);
- здатність удосконалювати й розвивати свій інтелектуальний і культурний рівень, будувати траєкторію професійного розвитку й кар'єри (ЗК10);
- здатність організовувати та проводити наукові дослідження, пов'язані з розробленням проектів і програм, проводити роботи зі стандартизації систем та процесів, готувати науково-технічні публікації за результатами виконаних досліджень (ФК2);
- здатність керувати ІТ проектами з використанням стандартів PMBOK, програмно реалізувати принципи дій та архітектури проектованих інформаційних систем і об'єктів з обґрунтуванням прийнятих технічних рішень (ФК10).

Згідно з вимогами програми навчальної дисципліни студенти після вивчення дисципліни мають продемонструвати такі результати навчання:

***знання*:**

- сутності наукового дослідження;
- методів аналізу літературних та інших інформаційних джерел;
- способів подання наукової інформації;
- методів отримання вихідних даних в науковому дослідженні та спостереження експерименту;
- методів логічної та математичної обробки даних;

- загальних теоретичні відомостей щодо принципів наукових досліджень підходу до проектування інформаційних систем, типових структур інформаційних систем;
- змістовного вибору необхідного підходу для формалізованого опису системи, процесу, об'єкту;
- методів регенерування нових ідей;
- правил написання наукової праці та підготовка її до публікації.

уміння:

- обирати (пропонувати, формулювати) тему наукового дослідження;
- формулювати об'єкт, предмет, мету, завдання, гіпотезу дослідження;
- обирати комплекс методів, адекватних меті й завданням дослідження;
- визначати склад основних сутностей, основних відношень та будувати UML-діаграми предметної області, використовуючи нормативні документи, за допомогою інструментальних засобів моделювання та проектування інформаційних систем;
- на підставі уявлень про методи проведення наукових досліджень обирати оптимальну методологію проведення досліджень;
- формувати структуру бази даних, аналізуючи інформаційні потоки за допомогою відповідних інструментальних засобів;
- формалізувати в системній постановці прикладних задач;
- аналізувати та інтерпретувати одержані результати;
- чітко, ясно й аргументовано викладати наукову інформацію та висновки.

досвід:

- самостійної роботи з джерелами інформації;
- використання стандартних методів виконання наукової роботи;
- систематизація й аналіз результатів наукових досліджень;
- оформлення результатів наукової роботи;
- підготовки до публікацій у фахових журналах результатів досліджень;
- проведення разом з науковим керівником науково-дослідної роботи;
- ділових комунікацій у професійній сфері, ділового спілкування.

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

У структурно-логічній схемі навчання зазначений кредитний модуль розміщується тоді, коли студенти мають науково-методичну підготовку до вирішення завдань в галузі інформаційних технологій, отриману в процесі вивчення попередніх дисциплін рівня «Бакалавр», та набули певного досвіду у програмуванні.

Навчальна дисципліна «Наукова робота за темою магістерської дисертації-1. Основи наукових досліджень» забезпечує проходження переддипломної практики та написання магістерської дисертації.

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

Пререквізити дисципліни. Знання та вміння, отримані при вивченні дисциплін: Науково-дослідна робота за темою магістерської дисертації. Частина 1.

***Постреквізити дисципліни*.** Отримані знання при вивченні дисципліни «Науково-дослідна робота за темою магістерської дисертації. Частина 1,2.» формує базові знання для вивчення дисциплін, пов'язаних з моделюванням, чисельним розв'язком обчислювальних задач, оптимізації та розробки програмного забезпечення систем захисту інформації.

4. Зміст навчальної дисципліни

Розділ 1. Політики безпеки і приватності в Інтернеті.

Основні поняття і аналіз загроз інформаційної безпеки. Основні поняття захисту інформації і інформаційної безпеки. Аналіз загроз інформаційної безпеки. Основні методи реалізації загроз інформаційної безпеки. Компоненти забезпечення безпеки інформаційної системи. Способи забезпечення комп'ютерної безпеки. Стандарти оцінки безпеки інформаційних систем. Загальні методи забезпечення інформаційної безпеки. Класифікація захисту сучасних операційних систем.

Проблеми інформаційної безпеки мереж. Введення в мережевий інформаційний обмін. Використання мережі Інтернет. Поняття захищеної операційної системи. Аналіз загроз мережевої безпеки. Проблеми безпеки IP- мереж. 2.1.2. Модель ISO/OSI і стек протоколів TCP/IP. Загрози і уразливості дротяних корпоративних мереж. Загрози і уразливості безпровідних мереж. Забезпечення інформаційної безпеки мереж. Способи забезпечення інформаційної безпеки. Шляхи рішення проблем захисту інформації в мережах.

Політики безпеки. Основні поняття політики безпеки. Структура політики безпеки організації. Процедури безпеки.

Стандарти інформаційної безпеки. Роль стандартів інформаційної безпеки. Міжнародні стандарти інформаційної безпеки. Вітчизняні стандарти безпеки інформаційних технологій.

Розділ 2. Криптографічний захист інформації.

Принципи криптографічного захисту інформації. Основні поняття криптографічного захисту інформації. Симетричні криптосистеми шифрування. Асиметричні криптосистеми шифрування. Комбінована криптосистема шифрування. Електронний цифровий підпис і функція хешування. Управління крипто ключами.

Криптографічні алгоритми. Класифікація криптографічних алгоритмів. Симетричні алгоритми шифрування. Асиметричні крипто алгоритми. Хешування.

Технології аутентифікації. Аутентифікація, авторизація і адміністрування дій користувачів. Методи аутентифікації, що використовують паролі і PINкоди. Строга аутентифікація. Біометрична аутентифікація користувача.

Забезпечення безпеки операційних систем. Проблеми забезпечення безпеки ОС. Поняття захищеної ОС. Архітектура підсистеми захисту ОС.

Розділ 3. Мережевий захист інформації.

Технологій міжмережевих екранів. Функції МЕ. Фільтрація трафіку. Особливості функціонування МЕ на різних рівнях моделі OSI. Схеми мережевого захисту на базі МЕ.

Основи технології віртуальних захищених мереж VPN. Концепція побудови віртуальних захищених мереж VPN.VPN рішення для побудови захищених мереж. Переваги застосування технологій VPN

Захист на канальному і сеансовому рівнях. Протоколи формування захищених каналів на канальному рівні. Протоколи формування захищених каналів на сеансовому рівні. Захист безпровідних мереж

Захист на мережевому рівні — протокол IPSec. Архітектура засобів безпеки IPSec. Захист передаваних даних за допомогою протоколів AH і ESP. Протокол управління криптоключами IKE. Особливості реалізації засобів IPSec.

Інфраструктура захисту на прикладному рівні. Управління ідентифікацією і доступом. Організація захищеного віддаленого доступу. Управління доступом за схемою одноразового входу з авторизацією Single Sign - On (SSO). Протокол Kerberos. Інфраструктура управління відкритими ключами PKI.

Аналіз захищеності в Інтернеті. Концепція адаптивного управління безпекою. Технологія аналізу захищеності. Технології виявлення атак.

Захист від комп'ютерних вірусів. Комп'ютерні віруси і проблеми антивірусного захисту. Антивірусні програми і комплекси. Побудова системи антивірусного захисту корпоративної мережі

Методи управління засобами мережевої безпеки. Завдання управління системою мережевої безпеки. Архітектура управління засобами мережевої безпеки. Функціонування системи управління засобами безпеки. Аудит і моніторинг безпеки

3. Заплановані види навчальної діяльності та методи навчання

Планується проведення навчальних занять у виді лекцій та лабораторних занять. Основний змістовний матеріал дисципліни викладається на лекціях. Лабораторні заняття проводяться з метою закріплення знань з основних тем дисципліни; формування у студентів навичок і вмінь з використання технологій захисту інформації.

5. Навчальні матеріали та ресурси

Основна література

Основна література

1.Бабайлов, Василь Кузьмич. Методологія наукових досліджень: навчальний посібник /В.К. Бабайлов ; Міністерство освіти і науки України, Харківський національний автомобільно-дорожній університет. – Харків :О.В. Бровін,2019. – 148 с.
https://opac.kpi.ua/F/?func=direct&doc_number=000608222&local_base=KPI01

2. Берко, Андрій Юліанович. Організація наукових досліджень, написання та захист магістерської дисертаці: навчальний посібник /А.Ю. Берко, Є.В. Буров, О.М. Верес, А.В. Катренко, П.О. Кравець, Ю.В. Нікольський, В.В. Пасічник ; Міністерство освіти і науки України. – Львів :Видавництво "Новий світ-2000",2021. – 280 с.
https://opac.kpi.ua/F/?func=direct&doc_number=000637215&local_base=KPI01

3. Бодров, Володимир Григорович. Методологічне та інструментальне забезпечення наукових досліджень :навчальний посібник /В.Г. Бодров, Л.Л. Лазебник, С.В. Онишко, В.А. Рожко, О.А. Шевчук ; за редакцією О.А. Шевчука ; Університет державної фіскальної служби України. – Ірпінь :Університет ДФС України, 2020. – 323 с.
https://opac.kpi.ua/F/?func=direct&doc_number=000629207&local_base=KPI01

4. Волянська, Яна Богданівна. Основи наукових досліджень : навчальний посібник / Я.Б. Волянська, С.М. Волянський ; Міністерство освіти і науки України, - Миколаїв : Іліон, 2017. - 216 с.
https://opac.kpi.ua/F/?func=direct&doc_number=000597888&local_base=KPI01

5. Костін, Юрій Дмитрович. Теорія і методологія наукових досліджень : навчальний посібник для студентів (магістрів) усіх форм навчання / Ю.Д. Костін, Т.В. Полозова, І.А. Шейко, Д.Ю. Костін ; Міністерство освіти і науки України, Харківський національний університет радіоелектроніки. - Харків : ХНУРЕ, 2021. - 152 сторінки.
https://opac.kpi.ua/F/?func=direct&doc_number=000634072&local_base=KPI01

6. Магістерська робота: методика підготовки : посібник / Т.О. Долбенко [та ін.] ; Міністерство культури України ; Київський національний університет культури і мистецтв. - Київ : Ліра-К, 2017. - 140 с.
https://opac.kpi.ua/F/?func=direct&doc_number=000586118&local_base=KPI01

7. Медвідь, Вікторія Юріївна. Методологія та організація наукових досліджень (у структурно-логічних схемах і таблицях) : навчальний посібник / В.Ю. Медвідь, Ю.І. Данько, І.І. Коблянська. - Суми : Університетська книга, 2020. - 218 сторінок : рисунки, таблиці, схеми.
https://opac.kpi.ua/F/?func=direct&doc_number=000629382&local_base=KPI01

8. Методичні рекомендації до порядку виконання та захисту кваліфікаційної роботи здобувачів освітнього ступеня "Магістр" спеціальності 125 "Кібербезпека" освітньо-професійної програми "Системи технічного захисту інформації, автоматизація її обробки" / укладачі: П.М. Павленко, В.В. Козловський, С.В. Лазаренко, В.О. Темніков, А.В. Темніков ; Міністерство освіти і науки України, Національний авіаційний університет. - Київ : НАУ, 2020. - 111 сторінок : рисунки, таблиці.
https://opac.kpi.ua/F/?func=direct&doc_number=000629193&local_base=KPI01

9. Нікітін, Олександр Костянтинович. Магістерська дисертація: організація, вимоги до структури, змісту та оформлення : навчальний посібник для здобувачів ступеня магістра за освітньо-професійними програмами спеціальностей 151 "Автоматизація та комп'ютерно-інтегровані технології" та 152 "Метрологія та інформаційно-вимірювальна техніка" / О.К. Нікітін, В.М. Зайцев ; Міністерство освіти і науки України, Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського". - Київ : КПІ імені Ігоря Сікорського, 2019. - 106 сторінок : рисунки, таблиці.
https://opac.kpi.ua/F/?func=direct&doc_number=000605227&local_base=KPI01

10. Невлюдов, Ігор Шакирович Основи наукових досліджень : навчальний посібник / І.Ш. Невлюдов, Ю.М. Олександров, А.О. Андрусевич, О.О. Чала ; Міністерство освіти і науки України, Харківський національний університет радіоелектроніки. - Харків : А.М. Панов, 2019. - 390 сторінок. рисунки, таблиці, портрети.

https://opac.kpi.ua/F/?func=direct&doc_number=000629136&local_base=KPI01

11. Основи наукових досліджень :навчальний посібник для студентів закладів вищої освіти /укладачі: М.В. Кудла, В.О. Коблик ; Міністерство освіти і науки України, Уманський педагогічний університет імені Павла Тичини. – Умань :Видавець М.М. Сочінський,2021. – 185 с.
https://opac.kpi.ua/F/?func=direct&doc_number=000635088&local_base=KPI01

12. Основи науково-дослідної роботи : навчальний посібник для вищих навчальних закладів / Ю.І. Палеха, Н.О. Леміш ; Міністерство освіти і науки, молоді та спорту України. - Київ : Ліра-К, 2017. - 332 с. : портр.
https://opac.kpi.ua/F/?func=direct&doc_number=000586150&local_base=KPI01

13.Організація наукових досліджень, написання та захист магістерської дисертації :навчальний посібник /А.Ю. Берко, Є.В. Буров, О.М. Верес, А.В. Катренко, П.О. Кравець, Ю.В. Нікольський, В.В. Пасічник ; Міністерство освіти і науки України. – Львів :Видавництво "Новий світ-2000",2019. – 284 с.
https://opac.kpi.ua/F/?func=direct&doc_number=000637215&local_base=KPI01

14. Партико, Зіновій Васильович. Основи наукових досліджень: підготовка дисертації : навчальний посібник / З.В. Партико. - Київ : Ліра-К, 2018. - 231 с. : іл.
https://opac.kpi.ua/F/?func=direct&doc_number=000594640&local_base=KPI01

ELAKPI – Електронний архів наукових та освітніх матеріалів КПІ ім. Ігоря Сікорського https://ela.kpi.ua/

15. Науково дослідна робота за темою магістерської дисертації. Основи наукових досліджень. Робоча програма навчальної дисципліни (Силабус) [Електронний ресурс] / КПІ ім. Ігоря Сікорського ; уклад. Н. І. Чичикало. – Електронні текстові дані (1 файл: 104,42 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 22 с.
https://ela.kpi.ua/handle/123456789/42333

16. Наукові дослідження за темою магістерської дисертації. Практикум [Електронний ресурс] : навчальний посібник / КПІ ім. Ігоря Сікорського; уклад. В. В. Кирик. – Електронні текстові данні (1 файл: 1,17 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 59 с.
https://ela.kpi.ua/handle/123456789/41697

17. Науково-дослідна робота за темою магістерської дисертації: методичні вказівки до виконання самостійних робіт [Електронний ресурс] : навч. посіб. для здобувачів ступеня магістра за освітньою програмою «Комп'ютерне моделювання фізичних процесів» / Д. В. Савченко, Ф. М. Гарєєва ; КПІ ім. Ігоря Сікорського. – Електронні текстові данні (1 файл: 2,4 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 70 с.
https://ela.kpi.ua/handle/123456789/45636

18. Основи наукових досліджень [Електронний ресурс] : методичні вказівки до курсу / КПІ ім. Ігоря Сікорського ; уклад.: Н. А. Панченко, В. С. Ткач. – Електронні текстові дані (1 файл: 135,5 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 13 с.
https://ela.kpi.ua/handle/123456789/25478
19. Основи наукових досліджень [Електронний ресурс] : навчальний посібник / І. М. Астрелін, А. Л. Концевой, С. А. Концевой ; КПІ ім. Ігоря Сікорського. – Електронні текстові данні (1 файл: 11,38 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2017. – 315 с.
https://ela.kpi.ua/handle/123456789/20579

20. Основи наукових досліджень [Електронний ресурс] : навчальний посібник / О. М. Сінчук, Т. М. Берідзе, М. Л. Барановська, О. В. Данілін, Д. О. Кальмус. – Електронні текстові дані (1 файл: 1,88 Мбайт). – Кременчук : ПП Щербатих О. В., 2022. – 196 с.
https://ela.kpi.ua/handle/123456789/47228

Навчальний контент

6. Методика опанування навчальної дисципліни(освітнього компонента)

Розділ 1. Політики безпеки і приватності в Інтернеті.

Тема 1.1. Основні поняття і аналіз загроз інформаційної безпеки

Основні поняття захисту інформації і інформаційної безпеки. Аналіз загроз інформаційної безпеки. Основні методи реалізації загроз інформаційної безпеки. Компоненти забезпечення безпеки інформаційної системи. Способи забезпечення комп'ютерної безпеки. Стандарти оцінки безпеки інформаційних систем. Загальні методи забезпечення інформаційної безпеки. Класифікація захисту сучасних операційних систем.

Тема 1.2. Проблеми інформаційної безпеки мереж.

Введення в мережевий інформаційний обмін. Використання мережі Інтернет. Поняття захищеної операційної системи. Аналіз загроз мережевої безпеки. Проблеми безпеки IP- мереж. 2.1.2. Модель ISO/OSI і стек протоколів TCP/IP. Загрози і уразливості дротяних корпоративних мереж. Загрози і уразливості безпровідних мереж. Забезпечення інформаційної безпеки мереж. Способи забезпечення інформаційної безпеки. Шляхи рішення проблем захисту інформації в мережах.

Тема 1.3. Політики безпеки.

Основні поняття політики безпеки. Структура політики безпеки організації. Процедури безпеки.

Тема 1.4. Стандарти інформаційної безпеки.

Роль стандартів інформаційної безпеки. Міжнародні стандарти інформаційної безпеки. Вітчизняні стандарти безпеки інформаційних технологій.

Розділ 2. Криптографічний захист інформації.

Тема 2.1. Принципи криптографічного захисту інформації

Основні поняття криптографічного захисту інформації. Симетричні криптосистеми шифрування. Асиметричні криптосистеми шифрування. Комбінована криптосистема шифрування. Електронний цифровий підпис і функція хешування. Управління крипто ключами.

Тема 2.2. Криптографічні алгоритми.

Класифікація криптографічних алгоритмів. Симетричні алгоритми шифрування. Асиметричні крипто алгоритми. Хешування.

Тема 2.3. Технології аутентифікації

Аутентифікація, авторизація і адміністрування дій користувачів. Методи аутентифікації, що використовують паролі і PINкоди. Строга аутентифікація. Біометрична аутентифікація користувача.

Тема 2.4. Забезпечення безпеки операційних систем.

Проблеми забезпечення безпеки ОС. Поняття захищеної ОС. Архітектура підсистеми захисту ОС.

Розділ 3. Мережевий захист інформації.

Тема 3.1. Технологій міжмережевих екранів.

Функції МЕ. Фільтрація трафіку. Особливості функціонування МЕ на різних рівнях моделі OSI. Схеми мережевого захисту на базі МЕ.

Тема 3.2. Основи технології віртуальних захищених мереж VPN

Концепція побудови віртуальних захищених мереж VPN.VPN рішення для побудови захищених мереж. Переваги застосування технологій VPN

Тема 3.3. Захист на канальному і сеансовому рівнях.

Протоколи формування захищених каналів на канальному рівні. Протоколи формування захищених каналів на сеансовому рівні. Захист безпровідних мереж

Тема 3.4. Захист на мережевому рівні — протокол IPSec.

Архітектура засобів безпеки IPSec. Захист передаваних даних за допомогою протоколів AH і ESP. Протокол управління криптоключами IKE. Особливості реалізації засобів IPSec.

Тема 3.5. Інфраструктура захисту на прикладному рівні.

Управління ідентифікацією і доступом. Організація захищеного віддаленого доступу. Управління доступом за схемою одноразового входу з авторизацією Single Sign - On (SSO). Протокол Kerberos. Інфраструктура управління відкритими ключами PKI.

Розділ 4. Аналіз захищеності в Інтернеті

Тема 4.1. Концепція адаптивного управління безпекою. Технологія аналізу захищеності. Технології виявлення атак.

Тема 4.2. Захист від комп’ютерних вірусів

Комп'ютерні віруси і проблеми антивірусного захисту. Антивірусні програми і комплекси. Побудова системи антивірусного захисту корпоративної мережі

Тема 4.3. Методи управління засобами мережевої безпеки

Завдання управління системою мережевої безпеки. Архітектура управління засобами мережевої безпеки. Функціонування системи управління засобами безпеки. Аудит і моніторинг безпеки

3. Заплановані види навчальної діяльності та методи навчання

Планується проведення навчальних занять у виді лекцій та лабораторних занять. Основний змістовний матеріал дисципліни викладається на лекціях. Лабораторні заняття проводяться з метою закріплення знань з основних тем дисципліни; формування у студентів навичок і вмінь з використання технологій захисту інформації.

7. Самостійна робота студента

Розділ 1. Базова модель безпеки інформації.

Актуальність проблеми забезпечення безпеки програм та даних. (2 години) Загальна характеристика дисципліни. Нормативно-правова база для організації і проведення заходів щодо безпеки програм та даних. Шляхи витоку інформації і несанкціонованого доступу в інформаційних системах. Архітектура систем безпеки програм та даних.

Сервіси безпеки, механізми їх реалізації. Атаки. Модель мережевої взаємодії. Організаційно-технічні заходи щодо забезпечення безпекиОсновні механізми розгортання ОС, які застосовуються для ОС Microsoft (4 години): метод дублювання дисків з використанням утиліти Sysprep та метод віддаленої установки з використанням сервера віддаленої установки (RIS).

Безпека зберігання даних в ОС Microsoft. Технологія тіньового копіювання даних. Архівація даних. Створення відмовостійких томів для зберігання даних. Робота з томами RAID.

Центр забезпечення безпеки (Windows Security Center) в операційній системі Windows. Три основні компоненти безпеки ОС: брандмауер, антивірус, система автоматичного оновлення. Параметри безпеки. Налаштування безпеки Internet Explorer. Створення виключення для програми. Створення виключення для порту.

Основні механізми розгортання ОС, які застосовуються для ОС Microsoft: метод дублювання дисків з використанням утиліти Sysprep та метод віддаленої установки з використанням сервера віддаленої установки (RIS).

Забезпечення безпеки зберігання даних в ОС Microsoft. Ознайомлення з можливостями ОС Microsoft Windows 2003/XP/2007/2010 по забезпеченню безпеки зберігання даних в цілому, не дивлячись на їх важливість. Розглянуто рішення, що надаються ОС Microsoft Windows в цьому діапазоні: технологія тіньового копіювання даних; архівація даних; створення відмовостійких томів для зберігання даних.

Обмеження тіньового копіювання томів. Стратегії архівації (повна архівація, повна архівація з подальшою додатковою, повна архівація з подальшою різницевою, щоденна архівація). Відновлення даних. Види відмовостійких томів для зберігання даних. Класифікація RAID.

Центр забезпечення безпеки (Windows Security Center) в операційній системі Windows. Три основні компоненти безпеки ОС: брандмауер, антивірус, система автоматичного оновлення. Параметри безпеки. Налаштування безпеки Internet Explorer. Створення виключення для програми. Створення виключення для порту.

Windows Defender. Захист від шкідливого програмного забезпечення. Технологія безпеки, що захищає комп'ютер від програм-шпигунів і інших видів небажаних програм. Установка Windows Defender, вимоги до системи. Налаштування Windows Defender. Автоматична перевірка (Automatic scanning). Дії за умовчанням (Default actions). Параметри захисту в режимі реального часу (Real-time protection options). Виявлення підозрілих дій. Робота з карантином. Використання Провідника програмного забезпечення (Software Explorer).

Microsoft Baseline Security Analyzer і XSpider. Системи аналізу захищеності корпоративної мережі (виявлення уразливостей). Принципи роботи систем аналізу захищеності. Вибір комп'ютера і опцій сканування в програмі MBSA. Опис перевірок, виконуваних MBSA.

Сканер безпеки XSpider. Можливості програми: повна ідентифікація сервісів на випадкових портах; евристичний метод визначення типів і імен серверів (HTTP, FTP, SMTP, POP3, DNS, SSH) незалежно від їх відповіді на стандартні запити; обробка RPC- сервісів з їх повною ідентифікацією; проведення перевірок на нестандартні DoS-атаки.

Розділ 2. Криптографічні засоби захисту інформації з симетричним ключем.

DES (Data Encryption Standard) - Симетричний алгоритм шифрування. (4 години) Мережа Фейстеля. Схема шифрування алгоритму DES. Генерування ключів. Режими використання DES: ECB — Electronic Code Book, CBC — Cipher Block Chaining, CFB — Cipher Feed Back, OFB — Output Feed Back. Переваги і недоліки режимів.

Алгоритми блокового симетричного шифрування ДСТУ ГОСТ 28147:2009. Міжнародний стандарт симетричного шифрування AES (Advanced Encryption Standard). Загальноєвропейський стандарт шифрування IDEA (International Data Encryption Algorithm). Програмна реалізація симетричних криптографічних алгоритмів AES засобами .NET.

Розділ 3. Криптографічні засоби захисту інформації з відкритим ключем

RSA - криптографічний алгоритм з відкритим ключем. Необхідні поняття. Алгоритм створення відкритого і секретного ключів. Шифрування і дешифрування. Цифровий підпис. Швидкість роботи алгоритму RSA. Криптоаналіз RSA. Елементарні атаки.

GnuGPG -- інструмент для шифрування і цифрового підпису. Налаштування. Створення ключа. Обмін ключами. Захист листування.

Політика та контроль

8. Політика навчальної дисципліни (освітнього компонента)

Відвідування лекційних та практисчних занять є обов’язковим за винятком поважних причин (хвороби, форс-мажорних обставин).

В разі пропущення занять з поважних причин викладач надає можливість студенту виконати усі або деякі лабораторні завдання (винятком є виконання деяких завдань у зв’язку із закінченням навчального процесу).

В разі пропущення занять без поважних причин, а також через порушення граничноготерміну виконання завдання (deadline)студент може отримати зменшену кількість балів від максимальної оцінки за відповідне завдання.

Протягом семестру студенти:

- виконують та захищають лабораторні роботи у відповідні терміни,
- пишутьмодульнуконтрольну роботу,
- повинні позитивно закрити дві атестації (в кінці березня та в серединітравня),
- по закінченні навчального процесу складають залік.

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

Система рейтингових (вагових) балів та критерії оцінювання

Максимальна кількість балів з кредитного модуля дорівнює 100.

Рейтинг студента з дисципліни складається з балів, що він отримує за:

- виконання та захист лабораторних робіт,
- модульну контрольну роботу (МКР) тривалістю 1 акад. година.

1. <u>Виконання завдань лабораторних робіт</u>

Завдання лабораторної роботи являє собою індивідуальне виконання робіт, що пов'язані з рішенням на ЕОМ заданої задачі комп’ютерного моделювання.

Вагові бали завдань наведено у таблиці.

Види завдань	*Внесок до семестрового рейтингу балів*
Завдання №1. Симетричні криптосистеми. Алгоритм DES.	20
Завдання №2. Асиметричні криптосистеми. Алгоритм RSA.	20
Завдання №3. Електронно-цифровий підпис на основі алгоритму RSA	20

Максимальна кількість балів за всі завдання дорівнює 60 балів.

Критерії оцінювання

Підготовка до роботи (у відсотках від максимальної кількості балів за відповідну роботу):

- протокол відповідає вимогам, охайний – 20 %;
- протокол відповідає вимогам, але є чисельні виправлення – 10 %;

Виконання завдання лабораторної роботи:

- робота виконана повністю і вірно протягом відведеного часу – 50 %;
- робота виконана пізніше зазначеного терміну – 20 %;

Якість захисту роботи:

- студент вірно і повністю відповів на запитання – 30 %;
- студент при відповіді допустив несуттєві неточності – 20 %;
- студент при відповіді на запитання допустив суттєві неточності, але самостійно виправив їх – 10 %.

2. Модульний контроль

Ваговий бал – 40.

Контрольна робота складається з 20 тестових завдань. За кожну вірну відповідь на запитання надається 2 бали.

Сума вагових балів контрольних заходів протягом семестру складає:

R= 60 + 40 = 100 балів.

Необхідною умовою допуску до заліку є зарахування усіх лабораторних робіт, а також стартовий рейтинг (r_c) не менше 40% від R, тобто 40 балів.

Сума балів переводиться до залікової оцінки згідно з таблицею:

Бали (RD)	Традиційна оцінка
95..100	Відмінно
85…94	Дуже добре
75…84	Добре

65…74	Задовільно
60…64	Достатньо
RD<=60	Незадовільно
RD < 40 або не виконані інші умови допуску до заліку	Не допущений

Робочу програму навчальної дисципліни (силабус):

Складено, д.т.н., професор Гаврилко Є.В.

Ухвалено кафедрою ІПЗЕ (протокол № 28 від 15.05.2023)

Погоджено Методичною комісією НН ІАТЕ (протокол № 9 від26.05.2023)