МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

Факультет комп'ютерно-інформаційних технологій

Кафедра комп'ютерно інформаційних систем та технологій

Затверджую
Декан ФКІТ
Чолишкіна О.І.
"20"серпня 2020 р.

Схвалено на засіданні кафедри

Протокол № 12 від 20 серпня 2020 р.
Завідувач кафедри Кавун С.В.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології захисту інформації

спеціальності: 122 Комп'ютерні науки
(шифр і назва спеціальності)

освітнього рівня Бакалавр
(назва освітнього рівня, ОКР)

освітньої програми: Комп'ютерні науки

спеціалізації: _____
(за наявності) (назва спеціалізації)

Київ МАУП 2020

Розробник (-и) силабусу навчальної дисципліни:
Рябий Мирослав Олександрович, кандидат технічних наук, доцент кафедри інформаційної безпеки

Викладач:
Рябий Мирослав Олександрович, кандидат технічних наук, доцент кафедри інформаційної безпеки

Силабус розглянуто і затверджено на засіданні кафедри КІСТ
Протокол від 20 серпня 2020 № 12

Завідувач кафедри _____ Кавун С.В.
(підпис)

Силабус погоджено з гарантом (керівником) освітньої програми 122 Комп'ютерні науки
(шифр, назва освітньої програми)

20.08. 2020 р.

Керівник (гарант) освітньої програми _____
(підпис)

Пролонговано:

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

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

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

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

ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом» http://maup.com.ua/
Факультет комп'ютерно-інформаційних технологій http://itmaup.com.ua
Кафедра комп'ютерних інформаційних систем та технологій
http://itmaup.com.ua/?page_id=589

Назва дисципліни	Технології захисту інформації
Викладач (-і)	Рябий М.О
Портфоліо викладача (-ів)	*http://itmaup.com.ua/?page_id=589*
Контактний тел.	*+380978806524*
E-mail:	
Сторінка дисципліни на сайті	*http://itmaup.com.ua/?page_id=1725*
Консультації	*Пн: 11:30-12:50* *корпус 24, аудиторія 4*

1. Коротка анотація до дисципліни. Викладання дисципліни «Технології захисту інформації»є навчання студентів базовими знаннями з проблем захисту інформаційних ресурсів у системах телекомунікації та мережах від порушення її конфіденційності, цілісності та доступності;етапів створення комплексної системи захисту інформації(КСЗІ), формування вимог до КСЗІ, вимогам щодо захисту інформації від несанкціонованого доступу(НСД), проектування КСЗІ в інформаційно-телекомунікаційних системах (ІКС), введення КСЗІ в ІКС в дію та її супровід;технології проєктування систем інформаційної безпеки згідно з ISO/IEC15408;дослідженню та застосуванню функції та механізмів захисту інформації, адміністрування засобів безпеки, вивчення студентами протоколів керування криптографічними ключами, поділу секрету, ідентифікації та автентифікації, схем композиційної , колективної, сліпого підпису на основі ДСТУ 4145–2002

2. Мета та завдання дисципліни. Метою є формування у студентів знань та навичок етапів створення КСЗІ, методів з захисту інформаційних ресурсів у системах від порушення її конфіденційності, цілісності та доступностіта використання їх у своїй професійній та повсякденній діяльності.

Цілі курсу:

·визначати види, джерела та носії інформації, що підлягає захисту;
·визначать види інформації, що захищається технічними засобами;
·принципи, засоби та етапи створення КСЗІ;
·вимоги щодо захисту інформації від НСД;
·технології проєктування систем інформаційної безпеки;
·визначати функціїта механізмибезпеки до інформації;
·застосовувати протоколи керування криптографічними ключами;
·застосовувати протоколи ідентифікації та автентифікації;
·застосовувати протоколи розподілу секрету;
·застосовувати різновиді схеми електронно-цифровихпідпису

3. Формат курсу. У межах дисципліни «Технології захисту інформації»студенти зі спеціальності 122 Комп'ютерні науки є навчання принципам побудови комплексних систем

захисту інформації та дослідженню, застосуванню функції та механізмів захисту інформації, що передбачає цикл лабораторних робіт та комплексне завдання.
У межах теоретичної частини забезпечуються знання:
·етапів створення КСЗІ;
·формування вимог до КСЗІ;
·технології проєктування систем інформаційної безпеки згідно з ISO/IEC15408
;·функції (сервіси) та механізмів безпеки;
·адміністрування засобів безпеки;
·видів криптографічних протоколів Проходження практичної частини курсу формує вміння:
·розроблення та впровадження заходів із захисту інформації;
·оцінювання рівня гарантій та функціональні послуги безпеки в засобах захисту інформації від НСД;
·застосовувати порядок створення КСЗІ вимогам нормативних документів;
·виконувати захист мережі та конфігурування AAA(authentication, authorization, accounting);
·виконувати розрахунки для протоколів розподілу секрету, перевіряти розділення секрету;
·виконувати розрахунки для протоколів ідентифікації;
·виконувати розрахунки для протоколів розподілу ключів та виконувати їхній криптоаналіз;
·виконувати розрахунки для схем електронно-цифрового підпису, перевірку підпису.4. Результати навчання
Вивчення навчальної дисципліни передбачає формування та розвиток у студентів компетентностей:загальних:
·здатність до абстрактного мислення, аналізу та синтезу;
·здатність застосовувати знання у практичних ситуаціях;
·знання та розуміння предметної області та розуміння професійної діяльності;
·здатність вчитися й оволодівати сучасними знаннями;
·здатність до пошуку, оброблення та аналізу інформації з різних джерел;
·здатність генерувати нові ідеї (креативність);
·здатність працювати в команді;
·здатність бути критичним і самокритичним;
·здатність приймати обґрунтовані рішення;
·здатність оцінювати та забезпечувати якість виконуваних робіт. фахових:
·здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури;
·здатність до аналізу загроз та проєктування засобів захисту інформації в інформаційних системах, що передбачає знання організаційних, технічних, алгоритмічних та інших методів побудови сучасних систем захисту інформації;
·здатність забезпечувати якість комп’ютерних систем та оцінювати їхні показники якості з використанням відповідних моделей та засобів на всіх етапах розробки;
·здатність до аналізу видів, джерел та носії інформації, що підлягає захисту, вибору ефективних методів та алгоритмів захисту;
·здатність здійснювати моніторинг та адміністрування загальними системними ресурсами з використанням методів та програмних засобів контролю та керування;
·здатність до системного мислення, застосування методології системного аналізу для дослідження складних проблем різної природи, методів формалізації та розв’язування системних задач;
·здатність застосовувати теоретичні та практичні основи методології та технології моделювання для дослідження характеристик і поведінки складних об'єктів і систем, проводити обчислювальні експерименти з обробкою й аналізом результатів;
·здатність до системного мислення, застосування методології системного аналізу для дослідження з проблем захисту інформаційних ресурсів у системах телекомунікації та мережах від порушення її конфіденційності, цілісності та доступності;

·здатність застосовувати теоретичні та практичні основи для впровадження заходів із захисту інформації;
·здатність до математичного формулювання та досліджування криптографічних протоколів, обґрунтовування вибору методів і підходів для розв’язування теоретичних і прикладних задач;
·здатність використовувати сучасні методи математичного моделювання та дослідження сучасних систем захисту інформації.
Вивчення даної дисципліни деталізує такі програмні результати навчання:
·застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній галузі комп'ютерних наук;
·використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв’язання задач теоретичного та прикладного характеру в процесі проєктування та реалізації об’єктів інформатизації;
·проєктувати, розробляти та аналізувати алгоритми розв’язання обчислювальних та логічних задач, оцінювати ефективність та складність алгоритмів на основі застосування формальних моделей алгоритмів та обчислюваних функцій;
·розуміти принципи моделювання організаційно-технічних систем і операцій; використовувати методи дослідження операцій, розв’язання одно–та багатокритеріальних оптимізаційних задач лінійного, цілочисельного, нелінійного, стохастичного програмування;
·розробляти програмні моделі предметних середовищ, вибирати парадигму програмування з позицій зручності та якості застосування для реалізації методів та алгоритмів розв’язання задач в галузі комп’ютерних наук;
·розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних;
·застосовувати знання теоретичних засад теорії інформації і кодування, основних методів оцінки кількості інформації, сучасних алгоритмів кодування для джерел повідомлень і засобів передачі даних каналами зв’язку, методів та алгоритмів стиснення даних,принципів побудови завадостійких кодів та їхнє використання в сучасних комп'ютерних інформаційних системах

4. Програмні результати навчання (інтегральні, фахові компетентності).

Вивчення навчальної дисципліни передбачає формування та розвиток у студентів компетентностей:

загальних:
- здатність до абстрактного мислення, аналізу та синтезу;
- здатність застосовувати знання у практичних ситуаціях.

фахових:
- здатність до математичного формулювання та досліджування неперервних та дискретних математичних моделей, обґрунтовування вибору методів і підходів для розв’язування теоретичних і прикладних задач у галузі комп’ютерних наук, аналізу та інтерпретування;
- здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проєктування, розроблення й аналізу алгоритмів, оцінювання їхньої ефективності та складності, розв’язності та нерозв’язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем.

5. Опис навчальної дисципліни*:*

Найменування показників	**Характеристика дисципліни за формами навчання**	
	денна	**заочна**
Технології захисту інформації		
Курс	**4**	**4**
Семестр	**8**	**8**
Обсяг кредитів	**3**	**3**
Обсяг годин, в тому числі:	**90**	**90**

Аудиторні	**34**	**6**
Модульний контроль	**2**	**-**
Семестровий контроль	**2**	**2**
Самостійна робота	**56**	**84**
Форма семестрового контролю	***Іспит***	***Іспит***

6. Статус дисципліни: *обов'язкова*
7. Пререквізити - вивчення дисципліни грунтується на вивченні організації баз даних та знань та комп'ютерних мереж.
8. Технічне й програмне забезпечення /обладнання - Студенти отримують практичні навички щодо захисту мережі та конфігурування AAA (authentication, authorization, accounting) в середовищі Packet Tracer. Дослідження криптографічних протоколів за допомогою пакета Security Protocol Animator для AVISPA (AutomatedValidationofInternetSecurityProtocolsandApplications) Ознайомитися із наявними в Інституті програмами і сервісами можна: ауд. No5: Тищенко Максим Вадимович

9. Політика курсу - Для успішного проходження курсу та складання контрольних заходів необхідним є виконання таких обов'язків: - не запізнюватися на заняття; - не пропускати заняття (як лабораторні, практичні так і лекційні), у разі хвороби мати довідку або її ксерокопію; - самостійно опрацьовувати весь лекційний матеріал та ресурси для самостійної роботи; - конструктивно підтримувати зворотній зв'язок з викладачем на всіх етапах проходження курсу; - своєчасно й самостійно виконувати всі передбачені програмою лабораторні та практичні завдання; - не користуватися мобільним телефоном під час аудиторних занять; - брати очну участь у контрольних заходах; - будь-яке відтворення результатів чужої праці, в тому числі використання завантажених з інтернету матеріалів, як власних результатів, кваліфікується як порушення норм і правил академічної доброчесності та передбачає притягнення до відповідальності у порядку, визначеному чинним законодавством.

10. Схема курсу (Навчально-методична карта дисципліни) (див. приклад у додатку)

‘

НАВЧАЛЬНО-МЕТОДИЧНА КАРТА ДИСЦИПЛІНИ *«Технології захисту інформації»*

Разом: 90 год., з них 17 год. – лекції, 17 год. – практична робота; самостійна робота – 56 год., модульний контроль – 2 год

Кількість балів за семестр	**100**			
Модулі	**Змістовий модуль I**			
Назва модуля	Архітектурні принципи побудови системи захисту			
Лекції	1	2	3	4
Теми лекцій	Основи, напрямки й етапи побудови систем захисту інформації. Матриця інформаційної безпеки. Подання елементів матриці	Порядок проведення робіт із створення комплексної системи захисту інформації	Технологія проектування систем інформаційної безпеки ISO/IEC15408. Функціональні вимоги безпеки, адекватності, профілю захисту та проекту	Функції (сервіси) безпеки. Механізми безпеки. Адміністрування засобів безпеки
Практичні заняття	1	2	3	4
Теми практичних занять	Питання передпроектної організації захисту інформації. Основні принципи побудови системи захисту.Аналіз погроз інформації в системах телекомунікації. Основні шляхи витоку інформації	Оцінка якості системи захисту інформації на основі аналізу профілю безпеки. Розрахунок оцінки захищеності	Програмно-технічні методи й засоби захисту інформації	Оцінка якості системи захисту інформації на основі аналізу профілю безпеки. Розрахунок узагальнених кількісних оцінок профілю безпеки
Поточний контроль	модульна контрольна робота №1 (20 балів)			
Модулі	**Змістовий модуль II**			
Назва модуля	Криптографічні протоколи			
Лекції	5	6	7	8
Теми лекцій	Види криптографічних протоколів. Основні атаки на	Схема поділу секрету Блеклі, Шаміра. Перевірка розділення секрету Фельдмана, Петерсена	Протоколи ідентифікації та автентифікації. Схеми композиційної, колективної та	Протоколи керування криптографічними ключами.

	безпеку криптографічних протоколів. Схема поділу секрету		сліпої підпису на основі ДСТУ 4145–2002.	Криптографічні протоколи на еліптичних кривих
Практичні заняття	5	6	7	8
Теми практичних занять	Схема поділу секрету Міньотта. Модифікована схема поділу секрету Міньотта. Схема поділу секрету Асмута-Блума. Карніна–Гріна–Хеллмана	Конфігурація мережі на маршрутизаторах Cisco.Захист привілейованого режиму та режиму конфігурації мережі на маршрутизаторах Cisco(програма симуляції Packet Tracer)	Протокол Фіата–Шаміра. Протокол ідентифікації Фейга–Фіата–Шаміра. Протокол ідентифікації Шнорра. Протокол Brickell–Mccurley. Протокол Окамото. Протокол GQ. Протокол GQ із ключами, що залежать від ідентифікаторів. Паралельна схема ідентифікації з нульовою передачею знань	Протокол Шаміра,MTI/A0, STS. Протокол відкритого розподілу ключів KEA, MQV, Girault, Kerberos
Поточний контроль	модульна контрольна робота №2 (20 балів)			
Підсумковий контроль	**Іспит**			

‘

11. Система оцінювання навчальних досягнень

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	4	4	4	4
Відвідування практичних занять	1	4	4	4	4
Виконання практичних завдань	10	3	30	3	30
Виконання завдань для самостійної роботи (*додавати завдання за потребою*)	5	1	5	1	5
Виконання модульної роботи	20	1	20	1	20
Разом за кожним модулем		-	63	-	63
Максимальна кількість балів					**126**
126:100=1,26. Студент набрав Х балів; Розрахунок: Х:1,26 = загальна кількість балів.					
Усього за навчальною дисципліною					**100**

12. Завдання для самостійної роботи та критерії її оцінювання

№ з/п	Зміст самостійної роботи студента	Обсяг СРС (годин)
1.	Опрацювання лекційного матеріалу	16
2.	Підготовка до практичних занять	32
3.	Підготовка до модульних контрольних робот №1, №2	8
Усього за навчальною дисципліною		**56**

Критерії оцінювання:

- змістовність – 1 бал
- відповідність темі та стилю оформлення – 1 бал

13. Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється шляхом написання модульної контрольної роботи.

Студентами пропонуються варіанти МКР, кожен білет містить по 2 теоретичних запитання та 2 практичних завдання.

Критерії оцінювання:

- виконання МКР – максимум 20 балів.

Критеріями оцінки правильності виконання модульних контрольних завдань є:

№ п\п	**Критерії оцінки знань студента виявлених під час проведення модульного контролю**	**кількість балів**
1.	студент в процесі письмової відповіді дає правильні відповіді на **всі поставлені запитання**, виявляє високий рівень знань теоретичного та практичного матеріалу. Викладає свою відповідь системно та логічно, упевнено і правильно аргументує власну позицію, робить висновки, тощо.	**20 балів**

2.	студент має належний рівень знань теоретичного та практичного матеріалу, на поставлені запитання відповіді дає, переважно, правильні, однак допускає певні неточності у визначеннях, не завжди належно (коректно) аргументує відповідь або правильно відповідає лише **на половину поставлених запитань**, тощо.	**15 бали**
3	студент має задовільний рівень знань теоретичного та практичного матеріалу, на поставлені запитання відповідає, але не на всі, допускає певні неточності у визначеннях базових категорій, не завжди належно (коректно) аргументує або правильно дає відповідь на **1/3 (одну третину)** поставлених запитань тощо.	**10 бали**
4.	студент дає неправильні відповіді на поставлені запитання, виявляє неналежний рівень знань теоретичного та практичного матеріалу, неспроможний послідовно і правильно аргументувати свою відповідь або взагалі **не в змозі відповісти на поставлені запитання**, тощо.	**0 балів**

14. Форми проведення семестрового контролю та критерії оцінювання: *Іспит*

15. Орієнтовний перелік питань для семестрового комплексного контролю.

1. Основи, напрямки й етапи побудови систем захисту інформації
2. Матриця інформаційної безпеки
3. Подання елементів матриці
4. Порядок проведення робіт із створення комплексної системи захисту інформації
5. Технологія проектування систем інформаційної безпеки ISO/IEC15408
6. Функціональні вимоги безпеки, адекватності, профілю захисту та проекту
7. Функції (сервіси) безпеки
8. Механізми безпеки
9. Адміністрування засобів безпеки
10. Види криптографічних протоколів
11. Основні атаки на безпеку криптографічних протоколів
12. Схема поділу секрету
13. Схема поділу секрету Блеклі, Шаміра
14. Перевірка розділення секрету Фельдмана, Петерсена
15. Протоколи ідентифікації та автентифікації
16. Протоколи керування криптографічними ключами
17. Криптографічні протоколи на еліптичних кривих
18. Схеми композиційної, колективної та сліпої підпису на основі ДСТУ 4145–2002
19. Основні принципи побудови системи захисту
20. Аналіз погроз інформації в системах телекомунікації
21. Основні шляхи витоку інформації
22. Оцінка якості системи захисту інформації на основі аналізу профілю безпеки
23. Розрахунок оцінки захищеності
24. . Програмно -технічні методи й засоби захисту інформації
25. Схема поділу секрету Міньотта
26. Модифікована схема поділу секрету Міньотта
27. Конфігурація мережі на маршрутизаторах Cisco

28. Захист привілейованого режиму та режиму конфігурації мережі на маршрутизаторах Cisco

29. Дослідження геш-функції MD5

30. SHA

16. Шкала відповідності оцінок

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	зараховано
82-89	**B**	добре	
75-81	**C**		
68-74	**D**	задовільно	
60-67	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

17. Рекомендовані джерела (література):

1. Захарченко М.В. Асиметричні методи шифрування в телекомунікація: навч. посіб. / М. В. Захарченко, А. В. Онацький, Л. Г. Йона, Т.М. Шінкарчук. – Одеса: ОНАЗ ім. О. С. Попова, 2011. – 184 с.
2. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости / Черемушкин А. В. – М.: «Академия», 2009. – 272 с.
3. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности / Запечников С. В. – М.: Горячая линия-Телеком, 2007. – 320 с.
4. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно- телекомунікаційній системі. – Затверджено наказом ДСТСЗІ СБ України № 125 від 8.11.2005. – (Серія видань "Нормативний документ").
5. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – М.: ДиаСофт, 2002.
6. Packet Tracer. [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/ru_ua/training-events/netacad/training-courses/cisco-packet-tracer.html
7. AVISPA. [Електронний ресурс]. – Режим доступу: http://www.avispa-project.org/
8. ДСТУ 4145–2002. [Електронний ресурс]. – Режим доступу:

https://dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798

Електронні джерела:

1. http://www.dut.edu.ua/uploads/ l_491_94183247.pdf
2. https://litmy.ru/knigi/seti/ 176809-kriptograficheskie-protokoly-osnovnye-svoystva-i-uyazvimosti.htm
3. http://www.dut.edu.ua/uploads/l_1066_65357958.pdf4.
4. http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=388355.
5. http://it-ebooks.ru/publ/it_secutity/it_security/15-1-0-5266.
6. https://www.cisco.com/c/ru_ua/training-events/netacad/training-courses/cisco-packet-tracer.html7.
7. https://www.iso.org/8.https://www.pdfdrive.com9.http://www.avispa-project.org/10. https://dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798