Міністерство освіти і науки України

Східноєвропейський національний університет імені Лесі Українки

Кафедра національної безпеки

ЗАТВЕРДЖЕНО
Проректор з навчальної, науково-
педагогічної роботи та рекрутації,
проф. Гаврилюк С. В. _____
Протокол № 2 від 17.10. 2018 р.

ПРОГРАМА

вибіркової навчальної дисципліни

Захист інформації в корпоративних мережах

підготовки бакалавра
галузь знань 12 Інформаційні технології
спеціальність 125 Кібербезпека
освітня програма Інформаційна безпека

Луцьк – 2018

Програма навчальної дисципліни «Захист інформації в корпоративних мережах» підготовки бакалаврів, галузі знань 1701 Інформаційна безпека, спеціальність 6.170103 Управління інформаційною безпекою.
"__"_____, 2018 р. - 10 с.

***Розробник:* Сачук Юрій Володимирович**, *кандидат фізико-математичних наук, старший викладач кафедри національної безпеки.*

Рецензент: Мекуш Оксана Григорьіна кандидат фізико-математичних наук, доцент *кафедри національної безпеки.*

Програма навчальної дисципліни затверджена на засіданні кафедри національної безпеки
протокол № 2 від 2.10 2018 р.
Завідувач кафедри _____ (Нахов М.А.)

Програма навчальної дисципліни
схвалена науково-методичною комісією факультету історії, політології та національної безпеки
протокол № 3 від 5.10 2018 р.

Голова науково-методичної
комісії факультету _____ (.)

Програма навчальної дисципліни схвалена науково-методичною радою Східноєвропейського національного університету імені Лесі Українки

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітня програма, освітній ступінь</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td rowspan="3">Нормативна</td></tr>
<tr><td rowspan="2">Денна форма навчання</td><td>Шифр і назва галузі знань:
1701 Інформаційна безпека</td></tr>
<tr><td>Напрям підготовки:
6.170103 Управління інформаційною безпекою</td></tr>
<tr><td rowspan="4">Кількість годин/кредитів 150/5</td><td rowspan="4"></td><td>Рік навчання: третій</td></tr>
<tr><td>Семестр: шостий</td></tr>
<tr><td>Лекції: 36 год.</td></tr>
<tr><td>Практичні (семінари): 36 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: є</td><td rowspan="3">Освітній ступінь
бакалавр</td><td>Самостійна робота: 68 год.</td></tr>
<tr><td>Консультації: 10 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
</table>

2. АНОТАЦІЯ КУРСУ

Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області інформаційної та кібербезпеки. На базі здобутих знань та умінь фахівець зможе вирішувати професійні задачі, що базуються на сучасних технологіях та методах захисту інформації у сучасних корпоративних систем та мереж.

Мета навчальної дисципліни: розкриття сучасних методів захисту інформації в комп’ютерних системах та мережах і ознайомлення з особливостями їх апаратної та програмної реалізацій.

3. КОМПЕТЕНЦІЇ

До кінця навчання студенти будуть компетентними у таких питаннях:

– вмітимуть виконати аналіз безпеки комп'ютерної системи або мережі та усунути можливі шляхи несанкціонованого доступу;

- вмітимуть перевірити надійність захисту інформації та стійкості його щодо хакерських атак шляхом моделювання загроз;

- знатимуть, як здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації;

- знатимуть, як підібрати комплекс необхідних апаратно-програмних засобів для захисту комп’ютерної системи та мережі.

- навчаться виконувати адміністрування прав доступу до комп´ютерної системи та мережі з метою перешкоди призначення невиправданих привілеїв;

- володітимуть навичками, як підібрати тип та структуру локальної комп’ютерної мережі;

4. ІНФОРМАЦІЙНИЙ ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1.

БЕЗПЕКА ІНФОРМАЦІЙНИХ РЕСУРСІВ

Тема 1. Поняття корпоративної мережі. Основні визначення.

Інформаційна безпека. Об'єктами інформаційної безпеки. Суб'єкти інформаційної безпеки. Інформаційне забезпечення інформаційної безпеки. Інформаційна кооперація. Інформаційна зброя корпоративних мереж та систем. Комп'ютерні віруси. Теорія інформаційної. Теорія захисту інформації.

Тема 2. Загрози інформаційній безпеці.

Основні загрози інформаційній безпеці. Організаційно-технічні фактори загроз інформаційній безпеці. Загрози у корпоративних системах та мережах передачі даних. Канал витоку інформації.

Тема 3. Моделі порушень інформаційних ресурсів.

Кваліфікація порушника. Рівень знань порушника. Ступінь ризику. Цілі і мета порушника.

Тема 4. Методи і засоби організації інформаційної безпеки.

Забезпечення інформаційної безпеки. Специфічні принципи забезпечення інформаційної безпеки. Інформованість об'єктів безпеки. Служб інформаційної безпеки.

Тема 5. Інформаційна система як об'єкт захисту.

Інформаційний захист. Радіоелектронний захист. Конфіденційність інформації (даних) в інформаційній системі. Цілісність даних. Семантична цілісність даних. Цілісність інформації. Цілісність бази даних. Цілісність системи. Захищена інформаційна система. Напрями забезпечення безпеки інформації. Активне перехоплення. Пасивне перехоплення. Пряме перехоплення. Непряме перехоплення.

Тема 6. Рівні захисту інформаційних систем.
Основні принципи захисту інформації.

Локальний рівень. Мережевий рівень. Рівень користувача. Рівні доступу до інформації. Принцип виправданості доступу. Принцип достатньої глибини контролю доступу. Принцип розмежування інформаційних потоків. Принцип персональної відповідальності. Принцип цілісності засобів захисту. Розмежування і контроль доступу до інформації.

Тема 7. Інформаційна безпека захищених корпоративних мереж зв'язку.

Нормативні документи системи ТЗІ. Стан нормативної бази системи ТЗІ. Модель програмно-керованої АТС відповідно до нормативних документів системи ТЗІ в Україні. Модель цифрової АТС як програмно-апаратного комплексу. Апаратна структура ЦАТС.

Змістовий модуль 2.

МЕТОДИ ТА СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ.

Тема 8. Аналіз моделей захисту інформації в інформаційних мережах держави.

Моделі захисту інформації, інформаційні мережі держави, загроза, несанкціонований доступ, багаторівневий захист, інформаційна система, джерело загроз.

Тема 9. Методи моделювання систем захисту інформації для корпоративних мереж зв'язку

Математичні методи моделювання складних систем. Математичний апарат теорії мереж Петрі. Процес імітаційного моделювання систем захисту інформації в корпоративних мережах зв'язку.

Тема 10. Способи захисту каналів корпоративних мереж на базі VPN-рішень.

VPN. Функції й компоненти мережі VPN. Виявлення структури і основних властивостей незахищеної мережі. Методи реалізації VPN мереж.

Тема 11. Особливості передачі інформації в бездротових мережах. Завадостійкі способи кодування в каналах бездротовогозв'язку.

WI-FI. Кодування джерела інформації. Модулятор. Демодулятор. Декодер каналу зв'язку. Технології виявлення помилок. Методи корекції помилок. Станція інформаційної мережі бездротового зв'язку. Комутатори бездротової мережі.

Тема 12. Організація мереж бездротового зв'язку.

Циклічній надлишковий контроль. Ad-Hoc-режим. Режим Infrastructure Mode. Інтеграція бездротового сегмента. Бездротовий доступ до дротової мережі. Режими WDS і WDS WITH AP. Багатоканальний розподіл ресурсу зв'язку. Множинний доступ з кодовим розділенням.

Тема 13. Організація криптографічного захисту інформації.

Основи криптографічного захисту. Поняття криптографії. Криптографічні методи. Алгоритми організації цифрового підпису. Шифр Ель-Гамаля. Шифр Ривеста-Шамира-Адлемана (RSA). Засоби криптографічного захисту інформаційно-комунікаційних систем. Модуль генератора випадкових чисел.

Тема 14. Основи захисту від руйнівних програмних впливів.

Захист програмного забезпечення. Класифікація комп'ютерних вірусів. Методи та засоби захисту програмного забезпечення. Методи боротьби з вірусами. Системний підхід до захисту ПЗ.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Денна форма навчання

№ п/п	Назва теми	Кількість годин, відведених на: аудиторні та позааудиторні заняття (денна форма)				
		Лекції	Практичні	Сам. роб.	Консультації	Усього
Змістовий модуль 1. БЕЗПЕКА ІНФОРМАЦІЙНИХ РЕСУРСІВ						
1	Поняття корпоративної мережі. Основні визначення.	**2**	**2**	**4**		**8**
2	Загрози інформаційній безпеці.	**2**	**2**	**4**		**8**
3	Моделі порушень інформаційних ресурсів.	**2**	**2**	**4**		**8**
4	Методи і засоби організації інформаційної безпеки.	**2**	**4**	**6**	**1**	**13**
5	Інформаційна система як об'єкт захисту	**4**	**2**	**4**		**10**
6	Рівні захисту інформаційних систем. Основні принципи захисту інформації.	**2**	**4**	**8**	**1**	**15**
7	Інформаційна безпека захищених корпоративних мереж зв'язку.	**2**	**2**	**10**	**1**	**15**
Разом за змістовим модулем 1		**16**	**18**	**40**	**3**	**77**
Змістовий модуль 2. МЕТОДИ ТА СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ.						
8	Аналіз моделей захисту інформації в інформаційних	**2**	**2**	**4**	**1**	**11**

	мережах держави.					
9	Методи моделювання систем захисту інформації для корпоративних мереж зв'язку.	**2**	**4**	**4**	**1**	**11**
10	Способи захисту каналів корпоративних мереж на базі VPN-рішень.	**2**	**2**	**4**	**1**	**9**
11	Особливості передачі інформації в бездротових мережах. Завадостійкі способи кодування в каналах бездротовогозв'язку.	**4**	**2**	**4**	**1**	**11**
12	Організація мереж бездротового зв'язку.	**4**	**2**	**4**	**1**	**11**
13	Організація криптографічного захисту інформації.	**4**	**4**	**4**	**1**	**13**
14	Основи захисту від руйнівних програмних впливів.	**2**	**2**	**4**	**1**	**9**
Разом за змістовим модулем 2		**20**	**18**	**28**	**7**	**73**
Усього годин:		**36**	**36**	**68**	**10**	**150**

5. ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

№ з/п	Тема
1.	Модель взаємодії відкритих системи OSI
2.	Організація інформаційних систем передачі даних
3.	Ієрархічна технологія серверної взаємодії
4.	Розподілена обробка інформації на основі мігруючих програм
5.	Сучасні системи серверної взаємодії.

6. РОЗПОДІЛ БАЛІВ ТА КРИТЕРІЇ ОЦІНЮВАННЯ

Підсумкова оцінка за 100-бальною шкалою складається із сумарної кількості балів за:

- поточне оцінювання з відповідних тем (максимум 40 балів);
- модульні контрольні роботи (максимум 60 балів).

Поточний контроль (мах - 40 балів)		**Модульний контроль (мах - 60 балів)**		**Загальна кількість балів**
Модуль 1		**Модуль 2**		
Змістовий модуль 1	**Змістовий модуль 2**	**МКР 1**	**МКР 2**	
12	28	30	30	100

Оцінювання навчальної роботи студента поточний контроль

Модуль № 1	**Модуль № 2**

Вид навчальної роботи	Max кількість балів	Вид навчальної роботи	Max кількість балів
Виконання та захист практичної роботи № 1	2	Виконання та захист практичної роботи № 7	2
Виконання та захист практичної роботи № 2	2	Виконання та захист практичної роботи № 8	2
Виконання та захист практичної роботи № 3	2	Виконання та захист практичної роботи № 9	2
Виконання та захист практичної роботи № 4	2	Виконання та захист практичної роботи № 10	2
Виконання та захист практичної роботи №5	2	Виконання та захист практичної роботи № 11	2
Виконання та захист практичної роботи № 6	2	Виконання та захист практичної роботи № 12	4
		Виконання та захист практичної роботи № 13	2
		Виконання та захист практичної роботи № 14	4
		Виконання та захист практичної роботи № 15	4
		Виконання та захист практичної роботи № 16	4
Усього за модулем № 1	**12**	**Усього за модулем № 2**	**28**

Шкала оцінювання

Оцінка в балах за всі види навчальної діяльності	**Оцінка**	
	для екзамену	**для заліку**
90 – 100	Відмінно	Зараховано
82 – 89	Дуже добре	
75 - 81	Добре	
67 -74	Задовільно	

60 - 66	Достатньо	
1 – 59	Незадовільно	Незараховано (з можливістю повторного складання)

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна література:

1. Алишов Н.И. Организации безопасности информационных ресурсов в системах телекоммуникаций // Праці 4-ї Міжнародної науково-техничної конференції по телекомунікаціям ―Телеком-99. – Одеса , 1999. – С. 112-115.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учеб.
3. пособие. – М.: Гелиос АРВ, 2002. – 480 с.
4. Анин Б. Защита компьютерной информации. — СПб.: БХВ-Петербург, 2000. – 384 с.
5. Бабак В.П., Теоритичні основи захисту інформації : Підручник. – К.: НАУ, 2008. – 752 с.
6. Бабак В.П., Корченко О.Г. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів / – К.: НАУ, 2003. – 670 с.
7. Бабаш А. В., Шанкин Г. П. Криптография. - М.: СОЛОН-Р, 2002. - 512 с.
8. Бабичев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учеб. курс. – М.: Горячая линия – Телеком, 2002. – 175 с
9. Баранов В.Л. Використання системноаналогових обчислювальних структур для адаптивної маршрутизації / Баранов В.Л., Мартинова О.П., Данилівна Г.В., Подлєсних Є.Г. Гончарова Л.Л./ Науково-технічний журнал. Інформаційно-керуючі системи на залізничному транспорті. – 2008. – № 1, – С. 24-28.
10. Блэк Ю. Сети ЭВМ: протоколы, стандарты, интер-фейсы. М.: Мир, 2002.
11. Бородин Г. А. Коды для полупроводниковых ЗУ, исправляющие однократную и обнаруживающие многократную ошибку // Зарубежная радиоэлектроника. – 1988. – №4. — С. 38 – 56.
12. Баричев С. Криптография без секретов. - М.: Радио и связь 1995 – 204 с.
13. Баричев С. Серов Р. Основы современной криптогра-фии. – М.: ЗАО «Издательство БИНОМ», 2003. – 152с.
14. Бугрименко Д. Многоуровневый модульный дизайн современных безопасных ЛВС с высокой доступностью. – М.:CiscoExpo2006, 2006 – 85с.
15. Бугрименко Д. Многоуровневый модульный дизайн современных безопасных ЛВС свысокой доступностью. – М.:CiscoExpo2006, 2006 – 85с.
16. Бугрименко Д. Технологии виртуализациикорпоративных ЛВС. - М.:CiscoExpo2006, 2006 – 74с.
17. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учеб. пособие. – М.: Горячая линия – Телеком, 2005. – 416 с.
18. Бунин С.Г., Войтер А.П. Вычислительные системы с пакетной радиосвязью. – Киев: Техніка, 1989. – 223 с.
19. Вайнстейн А. Основы теории информации. Пер з англ. - М.: 1960. – 360 с.
20. 30.Гончарова Л.Л. Комп'ютерні методи організації мікропроцесорних систем контролю і прогнозу залишкового ресурсу енергетичних об'єктів / Гончарова Л.Л. // Збірник наукових праць. «Моделювання та інформаційні технології», Інститут проблем моделювання в енергетиці – 2009.– № 53 – С. 103-108
21. 31.Гончарова Л.Л. Информационные технологии мониторинга режимов электрических сетей на основе дифференциальных Т-моделей. / Гончарова Л.Л. // Науково-технічний журнал.
22. Інформаційно-керуючі системи на залізничному транспорті. – 2009.– № 4 – С. 93-97
23. Гончарова Л.Л. Современные методы компьютерного анализа режимов функционирования сложных электрических объектов./ Гончарова Л.Л.// Зб. наук. праць. ІПМЕ НАН України –Вип-56. – К: - 2010. С. 17– 24.
24. Колмогоров А.Н. Теория информации и теория алгоритмов. М.: ―Наука, 1987. 304 с.

25. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия. — СПб.: БХВ-Петербург, 2003. - 752 с.
26. Миано Дж. Форматы и алгоритмы изображений в действии. Учеб. Пособ. – М.: Издательство Триумф, 2003 – 336 с.
27. Моисеев Д. Безопасность в компьютерных сетях. Microsoft Internet Security Framework: протоколы SSL и PCT. На сайті http://www.osp.ru/os
28. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Крипто-графия. – С.-Пб.: Изд-во Лань, 2000. –218 с.
29. Хетагуров Д.А., Руднев Ю.П. Повышение надежности цифровых устройств методами избыточного кодирования. – М.: ―Энергия, 1974. – 290 с.

8. Додаткова література:

9. Autonomic Systems: Concept for Self-Managing IT Infrastructure White Paper. Fujitsu Siemens Computers, March 2003.
10. Brassard G. Modern Cryptology. - N.Y.: Springer-Verlag, 1988. - 107 p.
11. Cisco Systems, Designing a Campus Network for High Availability. – 2006 – 60c.
12. Cisco Systems, Campus Design: Analyzing the Impact of Emerging Technologies on Campus Design. – 2006. – 91c.
13. Cisco Systems, Understanding Rapid Spanning Tree Protocol (802.1w) (Document ID: 24062). -2006. – 14c.
14. Cisco Systems, Understanding Multiple Spanning Tree Protocol (802.1s) (Document ID: 24248). – 2005. – 14c.
15. David Hucaby. CCNP Self-Study: CCNP BCMSN Exam Certification Guide, Third Edition. – Cisco Press, 2005. – 624c.
16. Dave Hucaby, Steve McQuerry. Cisco Field Manual: Catalyst Switch Configuration. – Cisco Press, 2002. – 560c.
17. Eric Ouellet, Robert Padjen, Arthur Pfund, Ron Fuller, Tim Blankenship ―Building a Cisco Wireless LAN‖ - Syngress Publishing, Inc, 2002.

9 . ПЕРЕЛІК ПИТАНЬ ДО ЗАЛІКУ

1. Дайте визначення інформаційній безпеці.
2. Назвіть об’єкти інформаційної безпеки.
3. Визначте інтереси держави в інформаційній сфері.
4. Перерахуйте основні загрози інформаційним ресурсам КМ.
5. Назвіть основні локальні фактори загроз інформаційній безпеці.
6. Які існують канали витоку інформації?
7. Основні характеристики побудови моделі порушника.
8. Основні положення методів і засобів забезпечення інформаційної безпеки.
9. Дайте визначення, що таке комп’ютерні віруси.
10. Розкрийте поняття «цілісність».
11. Розкрийте поняття «доступність».
12. Розкрийте поняття конфіденційності інформації.
13. Назвіть основні напрями забезпечення безпеки інформації.
14. Як класифікуються атаки за автоматизацією системи?
15. Як класифікуються атаки за ініціалізаційною умовою?
16. Як реалізується атаки зі зворотним зв’язком?
17. Чи можливо реалізувати мономономні атаки з кількох джерел?
18. На чому ґрунтується пігібекінгові атаки?
19. Що можна віднести до неспецифічних категорій НСД?
20. Як класифікуються атаки за засобами захисту від НСД?
21. Що відноситься до засобів несанкціонованого доступу?
22. Розкрийте поняття «інформаційна боротьба».
23. Назвіть основні характеристики інформаційної системи.
24. Розкрийте зміст моделі системи захисту інформації.
25. Якими показниками може бути оцінено якість розподілу доступу?
26. Назвіть основні принципи та рівні захисту інформаційних систем.

27. Які існують основні принципи захисту інформації?
28. Назвіть основні переваги застосування бездротових локальних мереж та їх особливість.
29. Наведіть теоретичні основи передачі даних в бездротових мережах.
30. Що називають локальною безпровідною мережею з (Ad-Hoc) режимом?
31. Яку функцію виконують бездротові інтерфейсні адаптери?
32. Назвіть види модуляції в системах бездротового зв'язку.
33. Яка різниця між фазовою і частотною модуляцією, принципи використання у БСМ?
34. Охарактеризуйте технологію розширення спектру бездротових мереж.
35. Назвіть основні характеристики системи зв'язку множинногодоступу та її архітектури.
36. Що таке супутникова комутація? Які існують її методи?
37. Розкрийте поняття «матриця інформаційного обміну».
38. Охарактеризуйте систему множинного доступу.
39. Опишіть схему роботи SCPC-системи.
40. Розкрийте суть поняття системи повного доступу (TES-система).
41. Назвіть моделі і системи шифрування.
42. Що таке «ключ»?
43. Чим відрізняється «криптографія» від «криптоаналізу»?
44. Що таке «криптографічна система шифрування»?
45. Який процес, обернений до шифрування?
46. Які існують вимоги до сучасних криптографічних систем захисту інформації?
47. Як класифікуються криптографічні методи?
48. Що називається «функцією-пасткою»?
49. Алгоритм шифрування Ель-Гамаля.
50. Дайте визначення «цифровому підпису».
51. Назвіть стандарт цифрового підпису (алгоритм DSS).
52. Поясніть, як відбувається в межах криптографії захист прав на цифрову інтелектуальну власність.
53. Як класифікуються спектральні методи цифрової криптографії?
54. Що називається «хеш-функцією»?
55. Які повноваження має центр сертифікації?
56. Які існують основні види атак на криптографічну систему?
57. Які існують основні типи криптоаналітичного розкриття інформації?
58. Мета та задачі захисту ПЗ.
59. Загрози інформаційним ресурсам та ПЗ. Класифікація.
60. Наведіть класифікацію комп'ютерних вірусів.
61. Назвіть ознаки класифікації комп'ютерних вірусів.
62. Поясніть принцип дії стелс-вірусів і поліморфних вірусів.
63. Приведіть структуру файлового вірусу і поясніть алгоритм його роботи.
64. У чому полягають особливості алгоритмів функціонування макровірусів і завантажувальних вірусів?
65. Дайте характеристику методів виявлення вірусів.
66. Назвіть методи видалення наслідків зараження вірусами.
67. Перерахуйте профілактичні заходи запобігання зараженню вірусами ІКСМ.
68. Порядок дій користувача при виявленні зараження ЕОМ вірусами.
69. Дайте коротку характеристику основних засобів захисту програмного забезпечення.
70. Методи та засоби захисту програмного забезпечення.
71. Класифікація методів захисту програмного забезпечення.
72. Класифікація засобів захисту програмного забезпечення.
73. Приведіть приклади програмних кодів вірусів.
74. Наведіть приклади програмних кодів виявлення вірусів.
75. Що таке «системний підхід до захисту ПЗ»?
76. Багаторівневі системи захисту інформаційних ресурсів та ПЗ.