Волинський національний університет імені Лесі Українки
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
нормативної навчальної дисципліни
КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Інформаційна безпека (2020 р.)
Форма навчання	Денна
Розробник (викладач)	Марчук Михайло Володимирович, доктор фізико-математичних наук, професор
Контактна інформація	mv_marchuk@gmail.com
Програма навчальної дисципліни	Програма навчальної дисципліни розміщена на сторінці кафедри комп'ютерних наук та кібербезпеки на офіційному сайті ВНУ імені Лесі Українки
Семестр, курс	8 семестр, 4 курс
Обсяг дисципліни	Загальний обсяг: 120 годин, 4 кредити Аудиторних занять: 54 год, з них 24 год. лекції, 30 лабораторні роботи Самостійна робота: 58 години Консультації: 8 год.
Форма контролю	Екзамен
Час занять	Аудиторні заняття проводяться за розкладом: http://194.44.187.20/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Мова навчання	Українська
Анотація дисципліни	Даний курс призначений для надання студентам теоретичних знань про засоби і методи організаційного захисту інформації; формування у студентів категоріальних понять з принципів побудови КСЗІ; формування у студентів уміння аналізу ефективності КСЗІ; стимулювання студентів до активної аналітико-пошукової роботи, що спрямована на визначення ефективних шляхів застосування систем технічного захисту інформації, як складової КСЗІ.
Мета вивчення дисципліни	Метою навчальної дисципліни є формування у майбутніх фахівців здатності впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
Результати навчання	*Загальні компетентності:* • Здатність застосовувати знання у практичних ситуаціях. . • Знання та розуміння предметної області та розуміння професії. • Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

	• Здатність до пошуку, оброблення та аналізу інформації. *Фахові компетентності:* • Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін. • Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою та/або кібербезпекою. *Програмні результати навчання:* • Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. • Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. • Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. • Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах дотримання режиму секретності із фіксуванням результатів у відповідних документах. • Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних)

Структура навчальної дисципліни

Назви змістових модулів і тем	Усього	Лек.	Лаб.	Сам. роб.	Конс.	Бали
1	165	26	30	100	9	100
Змістовий модуль 1.						
Тема 1 Створення комплексних систем захисту інформації.	12	2	2	8		
Тема 2. Загальні положення про комплексні системи захисту інформації.	13	2	2	8	1	
Тема 3. Заходи захисту інформації в КСЗІ	13	2	2	8	1	

Тема 4. Порядок здійснення захисту інформації на об’єктах інформаційної діяльності	16	2	4	9	1	
Тема 5. Атестація системи захисту інформації	12	2	2	8		
Тема 6. Захист інформації від витоку технічними каналами	14	2	2	9	1	
Разом за модулем 1	80	12	14	50	4	
Змістовий модуль 2.						
Тема 7. Захист інформації під час використання засобів копіювально-розмножувальної техніки	13	2	2	8	1	
Тема 8. Захист інформації в комп’ютерній системі підприємства	13	2	2	8	1	
Тема 9. Захист ІзОД В КС підприємства	13	2	2	8	1	
Тема 10. Захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах	16	4	2	9	1	
Тема 11. Захист інформації web-сторінки підприємства від несанкціонованого доступу	16	2	4	9	1	
Тема 12. Підрозділ захисту інформації на підприємстві	14	2	4	8		
Разом за модулем 2	85	14	16	50	5	
Модульна контрольна робота №1						30
Модульна контрольна робота №2						30

Самостійа робота студентів

№	Тематика	Кількість годин
1	Поняття КСЗІ, їх призначення та функці	11
2	Формування загальних вимог до КСЗІ	11
3	Обґрунтування необхідності створення КСЗІ	11
4	Обстеження середовищ функціонування	11
5	Формування завдання на створення КСЗІ.	11
6	Розробка політики безпеки інформації.	11
7	Розробка технічного завдання на створення КСЗІ	12

8	Розробка проекту КСЗІ.	11
9	Введення КСЗІ в дію та оцінка захищеності інформації. Супроводження КСЗІ	**11**

Оцінювання

При вивченні дисципліни студент виконує такі види робіт: опрацювання теоретичного матеріалу та виконання лабораторних робіт, виконання індивідуальних завдань, написання тестів.

Рівень знань студента оцінюється в балах, фіксується в журналі після вивчення змістового модуля. Підсумкова оцінка за національною шкалою за семестр заноситься в заліково-екзаменаційну відомість.

Усі види навчальної діяльності студента оцінюються певною кількістю балів. Підсумковий контроль здійснюється у формі екзамену. Сумарна кількість балів, яку студент отримує при засвоєнні змістових модулів за 100-бальною шкалою, визначає його підсумкову оцінку.

Дисципліна складається з двох змістових модулів. Підсумкова оцінка за 100-бальною шкалою складається із сумарної кількості балів за:

1. поточне оцінювання (максимум 40 балів);
2. Модульний контроль (максимум 60 балів);

2. екзамен (максимум 60 балів).

Поточний контроль, який має на меті перевірку рівня знань студента, здійснюється викладачем упродовж семестру у межах змістових модулів. Поточний контроль включає оцінку поточної роботи студента у ході виконання лабораторних робіт. Максимальна кількість балів за результатами поточного контролю становить 40 балів.

Підсумковий контроль, який здійснюється викладачем, має на меті перевірку рівня знань студента під час виконання екзаменаційного тесту, виконання практичного завдання та усної відповіді. Максимальна кількість балів, яку студент може набрати за екзамен, становить 60 балів, з яких по 10 балів – це оцінка за кожну із двох модульних контрольних робіт.

Поточний контроль (мах = 40 балів)		**Модульний контроль/екзамен (мах = 60 балів)**			**Загальна кількість балів**
Змістовий модуль 1	**Змістовий модуль 2**	**МКР 1**	**МКР 2**	**Екзамен**	
20	20	30	30	60	100

Підсумковий контроль

Екзамен складається з трьох частин: 1) написання екзаменаційного тесту (максимум – 20 балів); 2) виконання практичного завдання (максимум 10 балів) та 3) усна відповідь (максимум – 10 балів).

В оцінці знань студентів враховується:

1) достатність обсягу відповіді (повна, недостатньо повна, неповна);

2) обізнаність з основними поняттями, принципами, законами, правилами навчальної дисципліни;

3) логічність викладу матеріалу;

4) обґрунтованість власних міркувань;

5) уміння інтегрувати та диференціювати знання теоретичного матеріалу та застосовувати їх при виконанні практичних завдань.

Відповідь вважається *повною* (*40 балів*), якщо студент повністю оволодів матеріалом, обізнаний з усіма поняттями і термінами навчального курсу і адекватно оперує ними під час відповідей на поставлені питання, а також посилається на наукові дослідження з навчальної дисципліни, ознайомлений зі спеціальною літературою; демонструє здатність аналізувати факти, аргументувати власні судження теоретичними і фактичними положеннями, підсумувати сказане висновками.

Відповідь вважається *недостатньо повною* (*36 балів*) за умов непоганого володіння знаннями з навчального предмету. Відповідь студента має бути правильною й обгрунтованою. Студент повинен продемонструвати знання теоретичного матеріалу, навички самостійної навчально-пізнавальної діяльності, здатність викладати матеріал в певній логічній послідовності. Допускаються незначні помилки, які не впливають на загальне розуміння викладеного матеріалу.

Відповідь вважається *неповною* (*32 бали*), якщо продемонстровані знання з предмету носять фрагментарний і поверхневий характер. Теоретичні і фактичні знання відтворюються репродуктивно, без глибокого осмислення, аналізу, порівняння, узагальнення. Студент обізнаний з літературними джерелами з навчальної дисципліни, але не може дати достатньо критичної їх оцінки; допускає суттєві помилки, які порушують логіку викладення матеріалу.

Екзамен вважається *нескладеним (нижче 24 балів),* за умов неправильної або неповної відповіді, яка свідчить про нерозуміння поставленого завдання. Студент не володіє понятійно-категоріальним апаратом, необізнаний з джерельною базою з навчальної дисципліни і допускає грубі помилки у викладенні матеріалу.

Політика викладача щодо студента

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загальноприйнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування.

Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу.

Політика щодо академічної доброчесності

Під час навчання учасники освітнього процесу зобов’язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності.

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання студенти не користуються забороненими засобами (мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси), самостійно виконують запропоновані завдання.

Політика щодо дедлайнів та перескладання

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона вивчають теоретичний матеріал самостійно використовуючи навчальні посібники, конспекти лекцій, виконують всі завдання для аудиторних занять, всі домашні завдання. Прозвітуватися про виконання завдань можна у встановлені викладачем терміни під час консультацій.

Перескладання модулів відбувається із дозволу викладача за наявності поважних причин (наприклад, лікарняний).

Рекомендована література та інтернет-ресурси

1. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

2. Логінова Н. І. правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с., іл.

3. Остапов С. Е. технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

4. Девянин П. Н. Модели безопасности компьютерных систем : учебное пособие для студ. Высш. Учеб. Заведений – М. : Издательский центр "Академия", 2005. – 144 с.

5. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. / В. В. Домарев. – К. : ТИД "ДС", 2004. – 688 с.

6. Завгородний В. И. Комплексная система защиты в компьютерных системах : Учебное пособие. - М. : Логос; ПБОЮЛ Н. А. Егоров, 2001. – 264 с.

7. Курило А. П. Аудит информационной безопасности. / [Курило А. П., Зуфиров С. Л., Голованов В. Б. и др.]. – М. : Издательская группа "БДЦ-пресс", 2006. – 304 с.

8. Малюк А. А. Информационная безопасность : концептуальне и методологические основы защиты информации : учебное пособие для вузов. – М. : Горячая линия – Телеком, 2004. – 280 с.

9. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.

10. Мишин Е. Т. Построение систем физической защиты потенциально опасных объектов. / Е. Т. Мишин, Е. Е. Соколов. – М. : "Радио и связь", 2005. – 200 с.

11. Яремчук Ю. Є. Дослідження комбінаційних характеристик вітчизняних радіо непрозорих тканин М1, М2 та М3 / Ю. Є. Яремчук, В. С. Катаєв, В. В. Сінюгін // Реєстрація, зберігання та обробка даних. – 2015. – Том 17. №3 – С. 56-65.

12. Яремчук Ю. Є. Дослідженняя характеристик вітчизняних радіо непрозорих тканин Н1, Н2 та Н3 при різних комбінаціях їхнього застосування / Ю. Є. Яремчук, В. С. Катаєв, М. Ю.

Гижко, П. В. Павловський // Реєстрація, зберігання та обробка даних. – 2016. – Том 18, № 1. – С. 42-51.

13. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

14. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

15. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Перед проектні роботи.

16. НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі".

17. НД ТЗІ 2.7-011-2012 "Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв".

18. ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення".

19. Белов Е. Б. Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М. : Горячая линия-Телеком. 2006. – 544 с., ил.

20. Проектування комплексних систем захисту інформації : методичні вказівки, завдання на контрольну та курсову роботи / Уклад. : В. С. Орленко, В. О. Хорошко, Д. В. Чирков. – К. : ДУІКТ, 2005. – 14 с.

22. Семененко В. А. Информационная безопасность : учебное пособие / В. А. Семененко. - М. : МГИУ, 2006. – 277 с.

23. Скиба В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. - СПб. : Питер, 2008. – 320 с., ил.

24. Соколов А. В. Методы информационной защиты объектов и компьютерных сетей / А. В. Соколов, О. М. Степанюк. – М. : ООО Фирма "Издательство АСТ" ; СПб : ООО Издательство "Полигон", 2000. – 272 с.

25. Шумский А. А. Системній анализ в защите информации : учебное пособие для студентов вузов, обучающихся по спеціальностям в обл. информ. Безопасности / А. А. Шумский, А. А. Шелупанов. – М. : Гелиос АРВ, 2005. – 342 с.

Силабус навчальної дисципліни, затверджено на засіданні кафедри

Комп'ютерних наук та кібербезпеки
протокол № 3 від 05.10.2020р.

Завідувач кафедри:  Сачук Ю.В.