Волинський національний університет імені Лесі Українки

Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативної навчальної дисципліни

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	Інформаційна безпека (2020 р.)
Форма навчання	Денна
Розробник (викладач)	Прус Руслана Богданівна, кандидат технічних наук
Контактна інформація	prus.ruslana@vnu.edu.ua
Програма навчальної дисципліни	Програма навчальної дисципліни розміщена на сторінці кафедри комп'ютерних наук та кібербезпеки на офіційному сайті ВНУ імені Лесі Українки
Семестр, курс	7 семестр, 4 курс
Обсяг дисципліни	Загальний обсяг: 135 годин, 4,5 кредити Аудиторних занять: 54, з них 24 лекції, 30 лабораторні роботи Самостійна робота: 72 години Консультації: 9 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	Курс ознайомить студентів з основами виявлення та реагування на загрози кібербезпеки, вибору комплексу заходів та засобів, що спрямовані на захист комп'ютерів, обчислювальних мереж від несанкціонованого доступу та інших дій, пов'язаних з крадіжкою, блокуванням, пошкодженням, руйнуванням та знищенням як випадкового, так і цілеспрямованого впливу. Програма та тематичний план дисципліни орієнтовані на глибоке та ґрунтовне засвоєння студентами основних понять щодо програмно-апаратного захисту інформації, налаштуванню системи контролю доступу та побудови політики безпеки, ідентифікації та аутентифікації користувачів комп'ютерних систем, засобів і методів обмеження доступу до програм, методів та засобів криптографічного захисту інформації, захисту програм від модифікації, знищення та несанкціонованого копіювання
Мета вивчення дисципліни	Метою викладання навчальної дисципліни є навчання студентів принципам забезпечення кібербезпеки як однієї з найважливіших сфер діяльності в умовах формування інформаційного суспільства, опанування основними термінами та категоріями захисту інформації у інформаційно-комунікаційних системах на рівні їх тлумачення та відтворення для практичного застосування та втілення у процесі професійної діяльності. Основними завданнями вивчення дисципліни «Захист інформації в інформаційно-комунікаційних системах» є: • надати вичерпну та актуальну інформацію про комплекс сучасних

	методів та засобів захисту інформації від НСД; • сформувати у студентів високий рівень компетентності у сфері захисту інформації у інформаційно-комунікаційних системах; • сформувати у студентів уміння розуміти та розв'язувати поставлені перед ним задачі вибору технічних та програмних засобів захисту інформації • сформувати у студентів навики пошуку нових шляхів розв'язання поставлених перед ними задач із врахуванням зміни технологій та вимог суспільства; • залучити майбутніх фахівців до опрацювання спеціальної науково-методичної літератури, що має стати джерелом постійної роботи над собою з метою підвищення рівня професійної кваліфікації.
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 до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах • Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки • Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження • 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 • Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. *Програмні результати навчання:* • Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності • Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем • Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах • Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту • Впроваджувати заходи та забезпечувати реалізацію процесів

	попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем • Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах • Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки • Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів • Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем • Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем • Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки • Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних) • Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах

Структура навчальної дисципліни

Назви змістових модулів і тем	**Усього**	**Лек.**	**Лаб.**	**Сам. роб.**	**Конс.**	**Бали**
1	135	24	30	72	9	100
Змістовий модуль 1. Основи безпеки інформації в інформаційно-телекомунікаційних системах						
Тема 1. Правові та організаційні засади захисту інформації в інформаційних системах	9	2	2	5		2
Тема 2. Основні загрози безпеці інформації в інформаційно-комунікаційних системах(ІКТ)	10	2	2	5	1	2
Тема 3. Засоби антивірусного захисту інформації у інформаційно-телекомунікаційних мережах	9	2	2	5		4
Тема 4. Системи контролю та керування доступом	10	2	2	5	1	4

Тема 5. Захист інформації на рівні операційної системи	10	2	2	5	1	4
Тема 6. Безпека в інформаційних мережах	12	2	4	5	1	4
Разом за модулем 1	**60**	**12**	**14**	**30**	**4**	20
Змістовий модуль 2. Методи та засоби захисту інформації у ІКТ						
Тема 7. Програмні методи та засоби захисту інформації в ІКС	11	2	2	6	1	4
Тема 8. Технічний захист інформації в ІКС	9	2	2	5		4
Тема 9. Апаратно-програмні методи та засоби захисту інформації в ІКС	15	4	4	6	1	4
Тема 10. Криптографічні методи захисту інформації в ІКС	11	2	2	6	1	4
Тема 11. Створення, введення в дію та супроводження захищених систем	10	2	2	5	1	4
Разом за модулем 2	**56**	**12**	**12**	**28**	4	20
Модульна контрольна робота №1	6		2	4		10
Модульна контрольна робота №2	6		2	4		10
Екзамен	7			6	1	40
Разом за 7 семестр:	**135**	**24**	**30**	**72**	9	100

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. 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	10	10	40	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. Information technology. Security techniques. Information security management systems – Requirements: ISO/IEC 27001:2017
2. Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів: ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT)
3. Про захист інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. No 80/94-ВР: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua
4. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. – К. ДСТСЗІ СБ України, 1999 – 16 с.
5. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. — [Чинний від 28.04.1999]. — К.: ДСТСЗІ СБУ, 1999. — No 22. — (Нормативний документ системи технічного захисту інформації): https://tzi.com.ua/downloads/1.1-003-99.pdf
6. Nagle F., Ransbotham S., Westerman G. The Effects of Security Management on Security Events, WEIS, 2017.
7. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2014. – 251 с.
8. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К. : «МК-Прес», 2005. – 432 с.

9. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ “ПоліграфКонсалтинг”, 2004. – 216 с.

10. Грайворонський М.В., Новіков О.М Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

11. Гулак Г.М./ Основи криптографічного захисту інформації/ Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є./ Вінниця ВНТУ- 2012, 198 с.

12. Домарев В.В. Безопасность информационных технологий. Системный поход. – К.: ТИД ДС, 2004.

13. Домарев В.В. Моделирование процессов создания и оценки эффективности систем защиты информации, Информатика в машиностроении». – 2010.

14. Зубок М.І., Позднишев Є.В., Яременко С.М. Безпека бізнесу: Навчальний посібник. – К.: КНЕУ, 2008.

15. Зубок М.І. Основи безпеки комерційної діяльності підприємств та банків. – К.: КНТЕУ, 2005.

16. Конахович Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов. – К.: “МК–Пресс”, 2005. – 288 с.

17. Корченко О.Г. Системи захисту інформації: Монографія / О.Г. Корченко. – К.: НАУ, 2004. – 264 с.

18. Логінова Н. І. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса: Фенікс, 2015. – 264 с.

19. Смірнов С.А. Основи безпеки в комп’ютерних мережах. Навчальний посібник/ Смірнов С.А., Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Коваленко А.С. – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.

20. Тарнавський, Ю. А. Технології захисту інформації/ Тарнавський, Ю. А. - Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.

21. Хорошко В.О. Основи інформаційної безпеки: підручник / В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест; за ред. В.О. Хорошка. – К.: ДУІКТ, 2008. – 186 с.