Волинський національний університет імені Лесі Українки

Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативної навчальної дисципліни

ЗАХИСТ ІНФОРМАЦІЇ В ОПЕРАЦІЙНИХ 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)	Марчук Михайло Володимирович, доктор фізико-математичних наук, професор
Контактна інформація	mv_marchuk@ukr.net
Програма навчальної дисципліни	Програма навчальної дисципліни розміщена на сторінці кафедри комп'ютерних наук та кібербезпеки на офіційному сайті ВНУ імені Лесі Українки
Семестр, курс	6 семестр, 3 курс
Обсяг дисципліни	Загальний обсяг: 120 годин, 4 кредити Аудиторних занять: 54 год, з них 20 год. лекції, 40 лабораторні роботи Самостійна робота: 51 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	Даний курс призначений здобувачам для вивчення сучасних інформаційних технологій у галузі інформаційної безпеки та методів захисту інформації в різних операційних системах; підготовка фахівців з розробки та впровадження технологій комп'ютерного захисту інформації, забезпечення цілісності даних, конфіденційності, контролю передачі інформації, ідентифікації, аутентифікації, криптографії, інтегрованих систем, політики безпеки в операційних системах.
Мета вивчення дисципліни	Мета навчальної дисципліни «Захист інформації в інформаційних системах»– формування теоретичних знань щодо можливих небезпек і ступеня ризику втрат інформації, а також практичних навичок щодо забезпечення захисту програмної продукції..
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 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. *Програмні результати навчання:* • Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. • Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. • вирішувати задачі управління процедурами ідентифікації, аутентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. • Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. • Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових. • 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.

Структура навчальної дисципліни

Назви змістових модулів і тем	Усього	Лек.	Лаб.	Сам. роб.	Конс.	Бали
1	120	20	40	51	9	100
Змістовий модуль 1.						

Тема 1. Поняття, функції та класифікація операційних систем. Поняття архітектури операційної системи.	7	1	2	4		2
Тема 2. Операційна система та її оточення. Архітектура Windows. Поняття процесу та потоку, їх стани.	9	1	4	4		4
Тема 3. Реалізація планування процесів та потоків у Windows.	11	2	4	4	1	4
Тема 4. Організація файлових систем. Розміщення інформації у файлових системах. Реалізація файлових систем лінії FAT	12	2	4	5	1	4
Тема 5. Реалізація файлових систем NTFS. Функції ОС по управлінню пам'яттю.	11	2	4	4	1	4
Тема 6. Сегментна модель організації оперативної памяті. Сторінкова модель організації оперативної пам'яті.	10	2	2	5	1	2
Разом за модулем 1	60	10	20	26	4	20
Змістовий модуль 2.						
Тема 7. Архітектура операційної системи Linux. Файлові системи Linux..	7	1	2	4		2
Тема 8. Система команд по управлінню файлами в Linux. Графічні середовища Linux.	9	1	2	5	1	2
Тема 9. Конфігурація системи адміністрування. Методологія побудови мережевих систем. Архітектура засобів адміністрування операційної системи.	11	2	4	4	1	4
Тема 10. Керування пристроями та інформацією в мережі. Захист користувачів. Active Directory, групові політики та доменна структура.	11	2	4	4	1	4
Тема 11. Захист операційних систем від несанкціонованого доступу, захист інформаційних систем на основі еталонної моделі взаємодії відкритих операційних систем.	11	2	4	4	1	4
Тема 12. Захист потоків даних в операційних, інформаційних, системах.	11	2	4	4	1	4
Разом за модулем 2	60	10	20	25	5	20

Модульна контрольна робота №1		30
Модульна контрольна робота №2		30

Самостійа робота студентів

№	Тематика	Кількість годин
1	Сервіси і механізми захисту	8
2	Використовувати функції Microsoft CryptoAPI для розробки прикладного ПЗ	8
3	Протоколи автентифікації	8
4	Реалізація міжмережного екрану та сніффера	9
5	Захист програмного забезпечення від несанкціонованого використання та копіювання	9
6	Захист програм від несанкціонованої експлуатації за рахунок прив'язки до носія інформації	9

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. Зімчук І. В. Операційні системи : конспект лекцій / І.В. Зімчук, Т.М.Шапар, І. А. Охрімчук.–Житомир : ЖВІ, 2018. – 208 с.: іл.
2. Шеховцев В.А. Операційні системи.- К.: Видавнича група BHV, 2005.- 576с.
3. Бондаренко М. Ф. Операційні системи : навч. посібник / М. Ф. Бондаренко, О. Г. Качко. – Х. : Компанія СМІТ, 2008. – 432с.
4. Герасимчук О. О. Операційні системи : конспект лекцій для студентів спеціальності 121 «Інженерія програмного забезпечення» денної та заочної форм навчання / О. О. Герасимчук. – Луцьк : Луцький НТУ, 2016. – 200с.
5. Операційні системи та системи програмування : навч. посібник /
6. В. П. Харченко, Є. А. Знаковська, В. А. Бородін. – К. : Вид-во Нац. авіац. ун-ту «НАУ-друк», 2012. – 360с.
7. Адміністрування комп’ютерних мереж та операційних систем: методичне видання для студентів за спеціальністю 121 «Інженерія програмного забезпечення» факультету інформаційних технологій УжНУ / Розробник: к.т.н., доц. Поліщук В.В. – Ужгород: 2019. – 60 с.
8. Захарченко С. М., Суприган О. І. Основи системного адміністрування комп’ютерних мереж на базі OS Windows. Навчальний посібник. – Вінниця: ВНТУ, 2008.–100 с.
9. Unix : руководство системного администратора. Для профессиона лов / [Э. Немет, Г.Снайдер, С.Сибасс, Т.Хейн]. — 3-е изд. — СПб. : Пи тер ; К. : Изд. группа BHV, 2005.

Силабус навчальної дисципліни, затверджено на засіданні кафедри

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

Завідувач кафедри:  Сачук Ю.В.