МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)

М. В. Афанасьєв

ОСНОВИ ПОБУДОВИ ТА ЗАХИСТУ СУЧАСНИХ ОПЕРАЦІЙНИХ СИСТЕМ

робоча програма навчальної дисципліни

Галузь знань	**12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"**
Спеціальність	**125 "Кібербезпека"**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**"КІБЕРБЕЗПЕКА"**

Вид дисципліни	**Базова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри *кібербезпеки*
та інформаційних технологій Євсеєв С.П.

Харків
ХНЕУ ім. С. Кузнеця
2019

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки
та інформаційних технологій
Протокол № 1 від 26.08.2019 р.

Розробник:
Шматко О.В., к.т.н., доц. кафедри КІТ
Погасій С. С., к.е.н., старший викладач кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

1. Вступ

Анотація навчальної дисципліни:

Дисципліна “ Основи побудови та захисту сучасних операційних систем ” є базовою навчально дисципліною за спеціальністю “ Кібербезпека ”. Вона викладається у першому семестрі бакалаврату в обсязі 150 год.(5 кредитів ECTS), зокрема: лекції – 32 год., лабораторні – 32 год., самостійна робота – 86 год, консультації – 4 год. У курсі передбачено два змістових модулі та одна модульна контрольна робота. Завершується дисципліна іспитом.

Предметом навчальної вивчення навчальної дисципліни є теоретичні концепції та методології, принципи функціонування, захисту даних, вибору і практичної реалізації складових сучасних операційних систем.

Мета навчальної дисципліни:

є засвоєння теоретичних основ побудови, принципів проектування, конфігурування й застосування різних сучасних операційних систем, які забезпечують організацію обчислювальних процесів у корпоративних інформаційних системах економічного, управлінського, виробничого, наукового й іншого призначення, а також надання практичних навичок щодо захисту даних в сучасних операційних систем.

Головне завдання курсу – освоєння принципів використання системного програмного забезпечення, операційної системи персонального комп’ютера (сервера) для підтримання його в робочому стані; знання основних понять теорії побудови операційних систем; визначення статичних та динамічних характеристик об’єктів архітектури сучасних операційних системи; запобігання шляхів несанкціонованого доступу (НСД) до даних в операційній системі; вживання заходів протидії проникненню шкідливого програмного забезпечення до операційної системи та відновлення її працездатності після його знешкодження; ознайомлення з методологічними основами розробки та функціонування операційних систем.;

Курс	**1**	
Семестр	**1**	
Кількість кредитів ECTS	**5**	
Аудиторні навчальні заняття	**Лекції**	**32**
	семінарські, практичні	**-**
	Лабораторні	**32**
Самостійна робота		**86**
Форма підсумкового контролю	**Іспит**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	**Наступні дисципліни**
Математичні основи криптології	Основи криптографічного захисту
Основи теорії інформації	Забезпечення інформаційної безпеки
Основи побудови та функціонування мікропроцесорних систем	Основи планування та адміністрування служб доступу до інформаційних ресурсів

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
Здатність до забезпечення безпеки мережевих ресурсів та криптографічного захисту інформації в системах інформаційної та/або кібербезпеки	вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.
Здатність розв'язувати спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та\або кібербезпеки.	знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи

3. Програма навчальної дисципліни

Змістовий модуль 1. Основи побудови та функціонування сучасних операційних систем.

Тема 1. Вступ до сучасних операційних систем. Архітектура та ресурси сучасних ОС.

Історія розвитку та виникнення сучасних ОС. Поняття операційної системи, її призначення. Операційна система як розширена машина. Операційна система як розподілювач ресурсів.

Ядро операційної системи та його функції. Допоміжні модулі операційної системи. Ядро в привілеєвому режимі та в режимі користувача. Обмін між додатками при використанні ядра в привілеєвому режимі. Інтерфейс прикладного програмування.

Реалізація архітектури операційних систем. Монолітні системи. Багаторівневі системи. Мікроядерна архітектура. Базові механізми ядра. Менеджери ресурсів. Інтерфейс системних викликів. Апаратна залежність та переносність операційної системи. Типові засоби апаратної підтримки. Машинно-залежні компоненти операційної системи. Ресурси операційної системи.

Тема 2. Планування та керування процесами та потоками

Процеси. Функції процесів. Ідентифікатори додатків. Командний рядок процесу. Змінні оточення. Стан процесу. Обробка помилок. Робочі каталоги процесу. Створення і завершення процесів. Захист процесів від нерентабельного коду. Обробка помилок та виключень.

Потоки. Умови створення потоків. Стек потоку. Стан потоку. Періоди виконання потоку. Створення і завершення потоків. Розподіл процесорного часу між потоками. Зміна класу пріоритету потоку. Затримка та поновлення виконання потоку.

Планування та диспетчеризація потоків. Види планування. Стратегії планування. Витісняльна і невитісняльна багатозадачність. Алгоритми планування потоків. Квантування. Планування потоків в системах реального часу.

Тема 3. Керування оперативною пам'яттю

Методи розподілу пам'яті. Сегментація пам'яті. Сторінкова організація пам'яті. Сторінково-сегментна організація пам'яті. Технологія віртуальної пам'яті. Стопінг. Логічна і фізична адресація пам'яті. Віртуальна пам'ять.

Динамічний розподіл пам'яті. Пули пам'яті. Куча за замовчуванням. Створення додаткового пулу пам'яті. Виділення та звільнення пам'яті в кучі. Перевірка коректності даних, які розміщені в кучі. Отримання інформації про захист сторінок пам'яті.

Віртуальна пам'ять. Завантаження сторінок на вимогу. Алгоритми заміщення сторінок. Зберігання сторінок на диску. Пробуксовування і керування резидентною

множиною. Реалізація керування віртуальною пам'яттю в операційних системах Windows і Linux.

Тема 4. Логічна та фізична організація файлових систем

Поняття файлу і файлової системи. Організація інформації у файловій системі. Зв'язки. Імена та атрибути файлів. Операції над файлами і каталогами.

Фізична організація файлової системи. Базові відомості про дискові пристрої. Розміщення інформації у файлових системах. Надійність та продуктивність файлових систем. Файлові системи FAT, NTFS, HPFS, ext3fs та UFS. Особливості кешування.

Тема 5. Реалізація файлових систем

Виконувані файли. Загальні принципи компонування. Статичне та динамічне компонування. Структура виконуваних файлів. Секції виконуваних файлів. Формати ELF та PE.

Системний реєстр Windows. Логічна структура реєстру. Фізична організація реєстру. Програмний інтерфейс реєстру. Складання reg-файлів.

Використання редактору реєстру. Відновлення реєстру. Експорт реєстру. Імпорт реєстру. Документування інформації в журналах. Робота з журналом. Джерела повідомлень. Складання файлів повідомлень.

Служби Windows. Доступ та адміністрування служб операційної системи.

Змістовий модуль 2. Основи безпеки та захисту сучасних операційних систем

Тема 6. Комплексна система захисту даних операційної системи

Основні завдання забезпечення безпеки. Модель загроз для операційної системи. Монітор безпеки. Підсистема локальної автентифікації. База даних політики Lsass. Диспетчер облікових записів безпеки (SAM). База даних SAM. Інтерактивний диспетчер входу в систему. Користувацький інтерфейс входу в систему. Постачальники облікових даних. Служба мережного входу до системи. Kernel Security Device Driver.

Тема 7. Автентифікація та управління доступом до операційної системи

Принципи автентифікації і керування доступом. Типи об’єктів, які захищаються. Автентифікація з використанням паролів. Схема автентифікації "оклик-відгук". Автентифікація з використанням фізичного об'єкта. Автентифікація з використанням біометричних даних.

Формування списків управління доступом. Реалізація захисту особистих об’єктів. Облікові записи користувачів. Аудит. Загальні принципи організації аудиту. Робота із системним журналом Linux. Журнал подій Windows.

Тема 8. Шкідливе програмне забезпечення в операційних системах

Організацій несанкціонованого доступу до даних операційної системи. Атакуюче програмне забезпечення. Віруси. Умовно-небезпечні програми. Троянські коні. Хробаки. Програми-шпигуни. Руткіти. Антивірусні і анти-антивірусні технології.

Інсайдерські атаки на операційну систему. Логічні бомби. Лазівки в програмному коді. Фальсифікація входу до операційної системи. Атаки, які використовують переповнення буфера. Атаки, які використовують форматуючий рядок. Атаки, що використовують переповнення цілочисельних значень. Атаки, які використовують впровадження програмного коду. Атаки, пов'язані з ескалацією привілеїв.

Тема 9. Криптопровайдери та захист даних на транспортному рівні

Принципи шифрування даних на файлових системах. Створення криптопровайдеру. Гібридні криптосистеми. Цифрові підписи. Електронний підпис бінарних програм. Сертифікати. Шифрувальна файлова система Windows. Захист інформації на мережному рівні. Захист інформації на транспортному рівні.

Тема 10. Стандарти оцінювання безпеки операційних систем

Критерії оцінювання захищеності операційних систем. Політики безпеки в операційній системі. Міжнародні та відомчі стандарти оцінювання безпеки операційних систем.

Теми лабораторних робіт

Лабораторна робота №1. Розгортання ОС Ubuntu на виртуальній машині.

Лабораторна робота №2. Дослідження основ роботи з командною строкою та файловою системою ОС Ubuntu.

Лабораторна робота №3. Дослідження інструментів керування та захисту процессів ОС.

Лабораторна робота №4. Дослідження інструментів керування та захисту пам'яті ОС.

Лабораторна робота №5. Дослідження механізмів захисту ресурсів сучасної ОС.

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця, контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних, практичних, семінарських, лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

модульний контроль, що проводиться у формі колоквіуму як проміжний мініекзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті *інтегровану* оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час лабораторних занять та виконання індивідуальних завдань проводиться за такими критеріями:

розуміння, ступінь засвоєння теорії та методології проблем, що розглядаються; ступінь засвоєння фактичного матеріалу навчальної дисципліни; ознайомлення з рекомендованою літературою, а також із сучасною літературою з питань, що розглядаються; вміння поєднувати теорію з практикою при розгляді виробничих ситуацій, розв'язанні задач, проведенні розрахунків у процесі виконання індивідуальних завдань та завдань, винесених на розгляд в аудиторії; логіка, структура, стиль викладу матеріалу в письмових роботах і при виступах в аудиторії, вміння обґрунтовувати свою позицію, здійснювати узагальнення інформації та робити висновки; арифметична правильність виконання індивідуального та комплексного розрахункового завдання; здатність проводити критичну та незалежну оцінку певних проблемних питань; вміння пояснювати альтернативні погляди та наявність власної точки зору, позиції на певне проблемне питання; застосування аналітичних підходів; якість і чіткість викладення міркувань; логіка, структуризація та обґрунтованість висновків щодо конкретної про-

блеми; самостійність виконання роботи; грамотність подачі матеріалу; використання методів порівняння, узагальнення понять та явищ; оформлення роботи.

Загальними критеріями, за якими здійснюється оцінювання позааудиторної самостійної роботи студентів, є: глибина і міцність знань, рівень мислення, вміння систематизувати знання за окремими темами, вміння робити обґрунтовані висновки, володіння категорійним апаратом, навички і прийоми виконання практичних завдань, вміння знаходити необхідну інформацію, здійснювати її систематизацію та обробку, самореалізація на лабораторних заняттях.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 3 практичних ситуацій (одне стереотипне, одне діагностичне та одне евристичне завдання), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності".

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Розподіл балів за тижнями

Теми змістового модуля			Лекційні заняття	Лабораторні заняття	Письмова контрольна робота	Усього
Змістовний модуль	Тема	Тиждень				
Змістовий модуль 1.	1	1	1			1
		2	1	4		5
	2	3	1			1
		4	1	4		5
		5	1			1
		6	1	4		5
	3	7	1			1
		8	1	4	8	17
	4	9	1			1
	5	10	1	4		5
Змістовий модуль 2.	6	11	1			1
	7	12	1	4		5
	8	13	1			1
	9	14	1	4		5
	10	15	1			1
		16	1	4		5
	Іспит					40
Усього			16	32	8	100

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	Зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

5. Рекомендована література

5.1 Основна

1. Таненбаум Э. Современные операционные системы. – СПб.: Питер, 2010. – 1120 с.
2. Таненбаум Э., Бос Х. Современные операционные системы. – СПб.: Питер, 2015. – 1120 с.:
3. Шеховцов В.А. Операційні системи. – К.: Видавнича група BHV, 2005. – 576 с.
4. Таненбаум Э., Вудхалл А. Операционные системы. Разработка и реализация. Классика CS. – СПб.: Питер, 2007. – 704 с.
5. Третяк В.Ф. Основи операційних систем. Навчальний посібник / В.Ф. Третяк, Д.Ю.Голубничий, С.В. Кавун. – Харків, Вид. ХНЕУ, 2005. – 228 с.
6. Рихтер Дж. Windows для профессионалов: создание эффективных Win32-приложений с учетом специфики 64-разрядной версии Windows. Пер. с англ. – СПб.: Питер, 2006. – 752 с.
7. Бовет, Д. Ядро Linux.: Пер. с англ. / Бовет Д., Чезати М. — СПб.: БХВ-Петербург, 2007. – 1104 с.
8. Руссинович М., Соломон Д. Внутреннее устройство Microsoft Windows. Ч.1/Пер. с англ. – СПб.: Питер, 2013. – 800 с.
9. Руссинович М., Соломон Д., Ионеску А. Внутреннее устройство Microsoft Windows. Ч.2. Основные подсистемы ОС /Пер. с англ. – СПб.: Питер, 2014. – 672 с.

5.2 Додаткова

10. Саймон Р. Windows 2003 API. Энциклопедия программиста. Пер. с англ. /Р. Саймон. – К.: ООО "ДиасофтЮП", 2004. – 1088 с.
11. Побегайло А.П. Системное программирование в Windows. – СПб.: БХВ-Петербург, 2006. – 1056 с.
12. Руссинович М., Маргозис А. Утилиты Sysinternals. Справочник администратора. – М.: Русская редакція, 2011. – 480 с.
13. Бэкон Дж., Харрис Т. Операционные системы. – К.: Издат.группа BHV; СПб.: Питер, 2004. – 800 с.

14. Колісниченко Д.Н. Руткіти під Windows. – К.: Наука і техніка, 2006. – 320 с.
15. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. – СПб.: Питер, 2002. – 544 с.
16. Голубничий Д.Ю. Системне програмування і операційні системи. Ч.1. Навчальний посібник. / Д.Ю. Голубничий, В.Ф. Третяк. - Харків: Вид. ХДЕУ, 2004. – 192 с.
17. Голубничий Д.Ю. Системне програмування та операційні системи. Ч.2. Навчальний посібник. / Д.Ю. Голубничий, В.Ф. Третяк, С.В. Кавун. - Харків: Вид. ХНЕУ, 2005. – 264 с.
18. Сорокина С.И. Программирование драйверов и систем безопасности: Учебное пособие /С. И. Сорокина, А. Ю. Тихонов, А. Ю. Щербаков – СПб.: БХВ-Петербург, 2003. – 256 с.
19. Джонсон М. Разработка приложений в среде Linux.: Пер. с англ./ М. Джонсон, Э. Троян. – М. : ООО "И.Д. Вильямс", 2007. – 544 с.
20. Секунов Н.Ю. Программирование на C++ в Linux. – СПб.: БХВ-Петербург, 2004. – 368 с.

5.3 Інформаційні ресурси в Інтернеті

21. Каталог образовательных ресурсов (Федерация Интернет образования) [Электронный ресурс]. – Режим доступа : http://www.catalog.alledu.ru/predmet/.
22. Архів комп'ютерної документації [Электронный ресурс]. – Режим доступа : http://infocity.kiev.ua/.
23. Открытые системы [Электронный ресурс]. – Режим доступа : http://www.osp.ru.
24. Windows Sysinternals [Электронный ресурс]. – Режим доступа : http://technet.microsoft.com/ru-ru/sysinternals.
25. Выбор операционной системы для сервера [Электронный ресурс]. – Режим доступа : http://www.pub2me.net.
26. Windows [Электронный ресурс]. – Режим доступа : http://windows.microsoft.com/ru-ru/windows/home.
27. Operating systems [Электронный ресурс]. – Режим доступа : http://osys.ru.
28. Портал знаний. Операционные системы и память [Электронный ресурс]. – Режим доступа : http://www.znannya.org.
29. Операционные системы – Linux [Электронный ресурс]. – Режим доступа : http://www.libkruz.com.