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

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
_____
02071 Микола 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***

Статус дисципліни	***базова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Сергій ЄВСЕЄВ*

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 2 від 31.08.2020 р.

Розробник:
Алексієв В.О., д.т.н., проф. кафедри кібербезпеки та інформаційних технологій.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

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

Анотація навчальної дисципліни

Мета навчальної дисципліни "*Основи побудови та захисту сучасних операційних систем*" 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; запобігання шляхів несанкціонованого доступу до даних операційної системи; вживання заходів протидії проникненню шкідливого програмного забезпечення до середовища операційної системи.

Характеристика навчальної дисципліни

Курс	**2/2**
Семестр	**3/5**
Кількість кредитів ECTS	**5**
Форма підсумкового контролю	**Залік/Іспит**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Інформаційні системи та інтернет технології, введення в мережі	Основи планування та адміністрування служб доступу до інформаційних ресурсів
Комплексні системи захисту інформації	Організаційне забезпечення захисту інформації
	Дипломне проектування

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	РН–9. впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–17 забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН–18 використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН–19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН–21 вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

	РН–22 вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–24 вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН–25 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; РН–26 впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН–27 вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН–28 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; РН–29 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; РН–32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН–34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35 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; РН–42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН–47 вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН–48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;

	РН–49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН–50 забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН–51 підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН–52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН–53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Програма навчальної дисципліни

Змістовий модуль Основи побудови сучасних операційних систем.

Тема 1. *Вступ. Основні терміни, історія розвитку та визначення операційної системи.*

Тема 2. *Основи побудови сучасних операційних систем, Структура операційної системи, системні визови.*

Тема 3. *Багатозадачність. Процеси та потоки.*

Тема 4. *Управління памяттю та файлові системи.*

Змістовий модуль 2. Практика застосування та безпека операційних систем.

Тема 5. *Безпека операційних систем.*

Тема 6. *Автентифікація та управління доступом до операційної системи.*

Тема 7. *Шкідливе програмне забезпечення в операційних системах.*

Тема 8. *Перспективи розвитку операційних систем та засобів їх безпеки.*

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються проблемні лекції, презентації, бесіди, індивідуальні та групові проєкти, майстер-класи.

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою.

Контрольні заходи у випадку якщо вивчення дисципліни закінчується заліком включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що дозволяє студенту поставити залік, – 60 балів);

2)) підсумковий/семестровий контроль, що проводиться у формі заліку, відповідно до графіку навчального процесу.

Контрольні заходи у випадку якщо вивчення дисципліни закінчується іспитом включають:

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

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

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

– знати особливості побудови сучасних операційних систем, загальну структуру операційної системи, системні визови;

– розуміти основи багатозадачності та особливості роботи з процесами й потоками в операційних системах;

– мати уявлення щодо управління памяттю та з організації структури файлових систем;

– вміти налагоджувати контур безпеки на рівні операційних систем;

– знати технології автентифікація та управління доступом до операційної системи;

– блокувати шкідливе програмне забезпечення в операційних системах та налагоджувати системи, що постраждали від втручання;

– формулювати напрямки та орієнтуватися у перспективі розвитку операційних систем та засобів їх безпеки.

За дисципліною передбачені такі методи поточного формативного оцінювання: опитування та усні коментарі викладача за його результатами, настанови викладачів в процесі виконання лабораторних завдань, формування навичок самооцінювання та обговорення студентами виконаних лабораторних завдань, контроль самостійного виконання індивідуального завдання.

Всі роботи повинні бути виконані самостійно з метою розвитку творчого підходу до рішення задач.

У випадку, якщо вивчення дисципліни закінчується заліком, розподіл балів за видами проведення занять наступний.

Лекційні заняття: максимальна кількість балів становить 47 (робота на лекціях – 47), а мінімальна – 30.

Лабораторні заняття: максимальна кількість балів становить 53 (виконання лабораторних робіт – 2, захист лабораторних робіт – 25, контрольні роботи – 26), а мінімальна – 30.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до контрольних робіт з дисципліни, в технологічній карті бали на цій вид робіт не виділені.

У випадку, якщо вивчення дисципліни закінчується іспитом, розподіл балів за видами проведення занять наступний.

Лекційні заняття: максимальна кількість балів становить 7 (робота на лекціях – 7), а мінімальна – 5.

Лабораторні заняття: максимальна кількість балів становить 53 (виконання лабораторних робіт – 2, захист лабораторних робіт – 25, контрольні роботи – 26), а мінімальна – 30.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до екзамену з дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль, який закінчується заліком, проводиться з урахуванням отриманих балів у продовж семестру.

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням 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.

Підсумковий контроль, який проводиться з урахуванням іспиту.

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. Оцінювання кожного завдання екзаменаційного білету наступне: перше завдання – це 20 тестових завдань закритої форми, виконання його оцінюється 20 балами; друге завдання – присвячене розробленню структурної схеми архітектури рівня операційної системи, виконання його оцінюється 10 балами; третє завдання – евристичне щодо вибору оптимального рішення з організації безпеки, виконання його оцінюється 10 балами.

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.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

Форми оцінювання та розподіл балів наведено у таблицях "Рейтинг-план навчальної дисципліни".

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

Рейтинг-план навчальної дисципліни (залік)

Тема	**Форми та види навчання**		**Форми оцінювання**	**Max бал**
Тема 1	***Аудиторна робота***			
	Лекція	Проблемна лекція *"Введення. Основні терміни та визначення."*	Робота на лекції	6
Тема 2.	***Аудиторна робота***			
	Лекція	Лекція *"Основи побудови сучасних операційних систем, Структура операційної системи, системні визови."*	Робота на лекції	6

	Лабораторне заняття	Лабораторна робота №1 *"Установка та розгортання операційних систем родини Windows."*	Виконання лабораторної роботи	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *"Багатозадачність. Процеси та потоки."*	Робота на лекції	7
	Лабораторне заняття	Лабораторна робота №2 *"Тестування на проникнення операційної системи родини Windows."*	Захист лабораторної роботи № 1	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Лекція	Лекція *" Управління памяттю та файлові системи. "*	Робота на лекції	7
	Лабораторне заняття	Лабораторна робота №2 *"Тестування на проникнення операційної системи родини Windows."*	Захист лабораторної роботи № 2	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 5	***Аудиторна робота***			
	Лекція	Лекція *"Безпека операційних систем"*	Робота на лекції	7
	Лабораторне заняття	Лабораторна робота №3. *"Установка та розгортання операційних систем родини Linux."*	Виконання лабораторної роботи	1
Тема 6	***Аудиторна робота***			
	Лекція	Лекція*" Автентифікація та управління доступом до операційної системи."*	Робота на лекції	7
	Лабораторне заняття	Лабораторна робота №3. *"Установка та розгортання операційних систем родини*	Захист лабораторної роботи № 3	5

		Linux."		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену		
Тема 7	***Аудиторна робота***			
	Лекція	Лекція *"Шкідливе програмне забезпечення в операційних системах."*	Контрольна робота	26
	Лабораторне заняття	Лабораторна робота №4. *"Тестування на проникнення операційної системи родини Linux."*	Захист лабораторної роботи № 4	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція *"Перспективи розвитку операційних систем та засобів їх безпеки."*	Робота на лекції	7
	Лабораторне заняття	Лабораторна робота №5. "Особливості та ризики завантаження операційних систем".	Захист лабораторної роботи № 5	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену		

Рейтинг-план навчальної дисципліни (іспит)

Тема	**Форми та види навчання**		**Форми оцінювання**	**Max бал**
Тема 1	***Аудиторна робота***			
	Лекція	Проблемна лекція *"Введення. Основні терміни та визначення."*	Робота на лекції	1
Тема 2.	***Аудиторна робота***			
	Лекція	Лекція *"Основи побудови сучасних операційних систем, Структура операційної системи, системні визови."*	Робота на лекції	1

	Лабораторне заняття	Лабораторна робота №1 *"Установка та розгортання операційних систем родини Windows."*	Виконання лабораторної роботи	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *"Багатозадачність. Процеси та потоки."*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №2 *"Тестування на проникнення операційної системи родини Windows."*	Захист лабораторної роботи № 1	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Лекція	Лекція *" Управління памяттю та файлові системи. "*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №2 *"Тестування на проникнення операційної системи родини Windows."*	Захист лабораторної роботи № 2	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 5	***Аудиторна робота***			
	Лекція	Лекція *"Безпека операційних систем"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №3. *"Установка та розгортання операційних систем родини Linux."*	Виконання лабораторної роботи	1
Тема 6	***Аудиторна робота***			
	Лекція	Лекція*" Автентифікація та управління доступом до операційної системи."*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №3. *"Установка та розгортання операційних систем родини*	Захист лабораторної роботи № 3	5

		Linux."		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену		
Тема 7	***Аудиторна робота***			
	Лекція	Лекція *"Шкідливе програмне забезпечення в операційних системах."*	Контрольна робота	26
	Лабораторне заняття	Лабораторна робота №4. *"Тестування на проникнення операційної системи родини Linux."*	Захист лабораторної роботи № 4	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція *"Перспективи розвитку операційних систем та засобів їх безпеки."*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №5. "Особливості та ризики завантаження операційних систем".	Захист лабораторної роботи № 5	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену		
Екзамен				40

Рекомендована література

Основна

1. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ-2000», 2020 . – 678 с.

2.. Алексієв В. О. Застосування GRID-технології у транспортному ВНЗ : навч.-метод. посіб. / В. О. Алексієв.– Х. : ХНАДУ, 2008. – 208 с.

4. Таненбаум Э., Бос Х. Современные операционные системы. – СПб.: Питер, 2015. – 1120 с.

5. Таненбаум Э., Вудхалл А. Операционные системы. Разработка и реализация. Классика CS. – СПб.: Питер, 2007. – 704 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. 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.

8. Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. Kali Linux. Тестирование на проникновение и безопасность. – СПб.: Питер, 2020. – 448 с.

9. Unix и Linux. Руководство системного администратора / [Э. Немет, Г. Снайдер, Т. Хейн и др.] – М. : ИД "Вильямс", 2012. – 1312 с.

10. Ed Jorgensen. x86-64 Assembly Language Programming with Ubuntu, 2019. – 357 p. [Electronic resource]. –Access mode http://www.egr.unlv.edu/~ed/x86.html.

Додаткова

11. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. – СПб.: Питер, 2002. – 544 с.

12. Голубничий Д.Ю. Системне програмування і операційні системи. Ч.1. Навчальний посібник. / Д.Ю. Голубничий, В.Ф. Третяк. - Харків: Вид. ХДЕУ, 2004. – 192 с.

13. 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.

14. 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.

15. Джонсон М. Разработка приложений в среде Linux.: Пер. с англ./ М. Джонсон, Э. Троян. – М. : ООО "И.Д. Вильямс", 2007. – 544 с.

16. Секунов Н.Ю. Программирование на C++ в Linux. – СПб.: БХВ-Петербург, 2004. – 368 с.

Інтернет ресурси

17. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною «Основи побудови та захисту сучасних операційних систем» https://pns.hneu.edu.ua/course/view.php?id=4930.