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

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

ФІЗИЧНІ ОСНОВИ ТЕХНІЧНИХ ЗАСОБІВ РОЗВІДКИ

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 природоохоронних технологій,
екології та безпеки життєдіяльності Юрій БУЦ

Харків
2020

ЗАТВЕРДЖЕНО

на засіданні кафедри *природоохоронних технологій, екології та безпеки життєдіяльності*

Протокол № 1 від 25.08.2020 р.

Розробник:

Гоков О. М., к.ф.-м.н., доцент кафедри природоохоронних технологій, екології та безпеки життєдіяльності.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри розробника РПТК	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Навчальна дисципліна “Фізичні основи технічних засобів розвідки” є базовою навчальною дисципліною та вивчається згідно з навчальним планом підготовки фахівців освітнього ступеню "бакалавр" спеціальність 125 «Кібербезпека» галузі знань 12 "Інформаційні технології" денної форми навчання. Фізика належить до числа фундаментальних наук, що становлять основу теоретичної підготовки фахівців різних напрямів, і грає роль тієї бази, без якої неможлива успішна діяльність в будь-якій області сучасної науки і техніки. Найважливіші досягнення фізичної науки складають фундаментальну базу сучасних наукоємних технологій, на основі яких виробляється всіляка продукція, у тому числі і вироби інформаційних технологій та різних технічних засобів розвідки. У наш час знання з фізичної науки і засновані на них сучасні технології формують новий спосіб життя, і високоосвічена людина не може дистанціюватися від фундаментальних знань про навколишній світ, не ризикуючи виявитися безпорадним в професійній діяльності.

Подано тематичний план навчальної дисципліни та її зміст за модулями і темами. Вміщено плани лекцій і лабораторних робіт, матеріал щодо закріплення знань (самостійну роботу, контрольні запитання), критерії оцінювання знань студентів, професійні компетентності, якими повинен володіти студент після вивчення дисципліни.

Мета навчальної дисципліни: формування у студентів системи фундаментальних теоретичних знань, прикладних вмінь щодо використання базових фундаментальних фізичних понять стосовно виробів інформаційних технологій та різних технічних засобів розвідки, практичної роботи з широким колом сучасних фізичних і електронних пристроїв, розвиток самостійного мислення у студентів, необхідних для їх майбутньої професійної діяльності.

Характеристика навчальної дисципліни

Курс	**1**
Семестр	**2**
Кількість кредитів ECTS	**4**
Форма підсумкового контролю	**залік**

Структурно-логічна схема вивчення навчальної дисципліни

Пререквізити	Постреквізити
Базові знання з предметів середньої освіти До початку вивчення дисципліни студенти повинні оволодіти загальними правилами і технікою роботи з електронними документами пакету Microsoft Office.	Інформаційні системи та інтернет технології
	Організаційне забезпечення захисту інформації
	Інформаційна безпека держави
	Основи технічного захисту інформації
	Безпека в інформаційно-комунікаційних системах

Компетентності та результати навчання за навчальною дисципліною

Компетентності	Результати навчання
КФ 2. Здатність до використання інформаційно комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.	РН–10. виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН–11. виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах; 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–15. використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; 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–31. застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН–41. забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН–53. вирішувати задачі аналізу програмного коду на наявність можливих загроз.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно 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 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 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 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; 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 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; 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 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз;
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)	РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–12 розробляти моделі загроз та порушника; РН–16 реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; 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;
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою 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–12 розробляти моделі загроз та порушника; РН–13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–16 реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; 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–30 здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; 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–53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Програма навчальної дисципліни

Змістовий модуль 1. Фізичні основи технічної розвідки 1.
Тема 1. Технічна розвідка. Основні цілі, принципи та завдання
Тема 2. Фізичні основи захисту від фотографічної і оптико-електронної розвідки.
Тема 3. Фізичні основи захисту від радіоелектронної розвідки.
Тема 4. Фізичні основи захисту від акустичної та гідро акустичної розвідки.
Змістовий модуль 2. Фізичні основи технічної розвідки 2.
Тема 5. Фізичні основи захисту від радіаційної розвідки.
Тема 6. Фізичні основи захисту від хімічної розвідки.
Тема 7. Фізичні основи захисту від сейсмічної розвідки.
Тема 8. Фізичні основи захисту від магнітометричної розвідки.
Тема 9. Фізичні основи захисту від комп'ютерної розвідки.

Методи навчання та викладання

Розподіл методів навчання і викладання за темами навчальної дисципліни

Тема	Практичне застосування навчальних технологій
Тема 1. Технічна розвідка. Основні цілі, принципи та завдання	Дискусії, презентації, ілюстрації
Тема 2. Фізичні основи захисту від фотографічної і оптико-електронної розвідки	Дискусії, презентації, ілюстрації
Тема 3. Фізичні основи захисту від радіоелектронної розвідки	Робота в малих групах з питання: " Фізичні основи захисту від радіоелектронної розвідки". Презентації, ілюстрації
Тема 4. Фізичні основи захисту від акустичної та гідро акустичної розвідки	Робота в малих групах з питання: " Фізичні основи захисту від акустичної та гідро акустичної розвідки". Презентації, ілюстрації
Тема 5. Фізичні основи захисту від радіаційної розвідки	Робота в малих групах з питання: "Фізичні основи захисту від радіаційної розвідки". Презентації, ілюстрації
Тема 6. Фізичні основи захисту від хімічної розвідки	Дискусії, презентації, ілюстрації

Тема 7. Фізичні основи захисту від сейсмічної розвідки	Дискусії, презентації, ілюстрації
Тема 8. Фізичні основи захисту від магнітометричної розвідки	Робота в малих групах з питання: "Фізичні основи захисту від магнітометричної розвідки". Презентації, ілюстрації
Тема 9. Фізичні основи захисту від комп'ютерної розвідки	Робота в малих групах з питання: "Фізичні основи захисту від комп'ютерної розвідки". Презентації, ілюстрації

Порядок оцінювання результатів навчання

ХНЕУ ім. С. Кузнеця використовує накопичувальну (100-бальну) систему оцінювання.

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні заняття, а також виконання самостійної роботи. Контрольні заходи містять: *поточний контроль*, що здійснюється протягом семестру під час проведення лекційних, лабораторних занять і оцінюється сумою набраних балів; *модульний контроль*, що проводиться з урахуванням поточного контролю за відповідний змістовий модуль і має на меті інтегроване оцінювання результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля.

Протягом семестру студент може одержати за роботу:

на лекційних заняттях максимально – 12 балів;

на лабораторних заняттях максимально – 76 балів (62 бали за виконання індивідуальних завдань, 9 балів за підготовку презентацій та 5 балів за підготовку есе).

Виконання індивідуальних завдань дає можливість студенту одержати максимально 10 балів за роботу.

Поточний тестовий контроль у межах дисципліни проводиться у письмовій формі декілька разів за семестр. Тест включає запитання одиничного і множинного вибору щодо перевірки знань основних категорій навчальної дисципліни.

Письмова контрольна робота проводиться 2 рази за семестр та включає практичні завдання різного рівня складності відповідно до тем змістового модуля. Білет складається з теоретичних і практичних завдань.

Протягом семестру студент може одержати за 2 письмові контрольні роботи 12 балів.

Загальними критеріями, за якими здійснюється оцінювання поза аудиторної 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 лекційних та лабораторних заняттях.

Критеріями оцінювання есе та презентації є:

здатність проводити критичне та незалежне оцінювання певних питань;

вміння пояснювати альтернативні погляди та наявність власної точки зору, позиції на певне проблемне питання;

якість і чіткість викладення міркувань;

логіка та обґрунтованість висновків щодо конкретної проблеми;

самостійність виконання роботи;

грамотність подачі матеріалу;

використання методів та способів порівняння, узагальнення понять та явищ;

оформлення роботи.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі поточного контролю під час проведення лекційних і лабораторних занять, виконання поточних контрольних робіт та індивідуальних завдань і оцінюється сумою набраних балів (максимальна сума – 100 балів).

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. Виставлення підсумкової оцінки здійснюється за шкалою, наведеною в таблиці «Шкала оцінювання: національна та ЄКТС».

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		

Рейтинг-план навчальної дисципліни

Тема	**Форми та види навчання**		**Форми оцінювання**	**Max бал**
Тема 1	***Аудиторна робота***			
	Лекція	Проблемна лекція "Технічна розвідка. Основні цілі, принципи та завдання"	Участь у виконанні практичних завдань	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою	Перевірка ДЗ	
Тема 2	***Аудиторна робота***			
	Лекція	Лекція "Фізичні основи захисту від фотографічної розвідки"	Участь у виконанні практичних завдань. Обговорення питань за темою	1
	Лекція	Лекція "Фізичні основи захисту від оптико-електронної розвідки"	Участь у виконанні практичних завдань	1

	Лабораторне заняття	Лабораторна робота №1 "Визначення кривизни лінзи за допомогою кілець Ньютона. Визначення періода дифракційної гратки. Дослідження поляризації світла. Закон Малюса".	Участь у виконанні практичних завдань. Обговорення питань за темою	6
	Лабораторне заняття	Лабораторна робота № 2 "Визначення довжини звукових хвиль або частоти звуку та показника адіабати"	Участь у виконанні практичних завдань	6
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою	Перевірка ДЗ	
Тема 3	***Аудиторна робота***			
	Лекція	Лекція "Фізичні основи захисту від радіоелектронної розвідки"	Обговорення питань за темою	1
	Лекція	Лекція "Фізичні основи захисту від радіоелектронної розвідки ".	Обговорення питань за темою	1
	Лабораторне заняття	Лабораторна робота № 3. "Вивчення методів статистичного аналізу радіодіапазону і виявлення радіомікрофонів закладок за допомогою комп'ютеризованих комплексів RS turbo, RS turbo Mobile-L. Виявлення сигналів лінійних і мережевих закладок"	Участь у виконанні практичних завдань.	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою	Перевірка ДЗ	
Тема 4	***Аудиторна робота***			
	Лекція	Лекція "Фізичні основи захисту від акустичної розвідки"	Обговорення питань за темою	1
	Лекція	Лекція "Фізичні основи захисту від гідро акустичної розвідки"	Обговорення питань за темою	1
	Лабораторне заняття	Лабораторна робота №4. "Вивчення можливостей виявлення оптичних сигналів передавачів ІК-діапазону за допомогою комплексів «RS turbo», «RS turbo Mobile-L». Вивчення призначення комплексу Спрут-7 "	Участь у виконанні практичних завдань.	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою	Перевірка есе і ДЗ	5
Тема 5	***Аудиторна робота***			
	Лекція	Лекція. "Фізичні основи захисту від радіаційної розвідки"	Обговорення питань за темою	1

	Лабораторне заняття	Лабораторна робота № 5 "Реєстрація радіоактивного фону з допомогою лічильника Гейгера – Мюллера. Вимірювання коефіцієнта поглинання β-часток".	Участь у виконанні практичних завдань.	10
		Контрольна робота		6
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою	Перевірка ДЗ	
Тема 6	***Аудиторна робота***			
	Лекція	Лекція "Фізичні основи захисту від хімічної розвідки".	Обговорення питань за темою	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою	Перевірка ДЗ	
Тема 7	***Аудиторна робота***			
	Лекція	Лекція. "Фізичні основи захисту від сейсмічної розвідки"	Обговорення питань за темою	1
	Лабораторне заняття	Лабораторна робота № 6 "Вивчення методик застосування комплексу Спрут-7 при оцінці захищеності приміщення від витоку мовної інформації по вібро акустичному каналу і по каналам акустоелектричних перетворень "	Участь у виконанні практичних завдань.	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою	Перевірка ДЗ	
Тема 8	***Аудиторна робота***			
	Лекція	Лекція. "Фізичні основи захисту від магнітометричної розвідки"	Обговорення питань за темою	1
	Лабораторне заняття	Лабораторна робота № 7 "Вивчення характеристик змінного струму, RLC-кіл, Вивчення переходних і загасаючих коливань в електричних колах "	Участь у виконанні практичних завдань.	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до контрольної роботи.	Перевірка презентації та ДЗ	9
Тема 9	***Аудиторна робота***			
	Лекція	Лекція "Фізичні основи захисту від комп'ютерної розвідки"	Обговорення питань за темою	1
		Контрольна робота		6
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою	Перевірка ДЗ	

1. Рекомендована література

Основна

1. Бузов Г. А. Защита от утечки информации по техническим каналам: учебное пособие. / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев – Москва : Горячая линия – Телеком, 2005. – 416 с.

2. Гоков О. М. Фізика [Електронний ресурс] : навч. посіб. / О. М. Гоков ; Харківський національний економічний університет ім. С. Кузнеця. – Х. : ХНЕУ ім. С. Кузнеця, 2019. - 292 с.

3. Гурвич И.И. Сейсмическая разведка. / И.И. Гурвич, Г.Н. Боганик. – Москва : Недра. – 1980. – 178 с.

4. Зайцев А.П.. Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации. / А.П. Зайцев, А.А. Шелупанов – Изд. Томского гос. ун-та систем управления и радиоэлектроники, 2004. – 197 с.

5. Меньшаков Ю.К. Основы защиты от технических разведок: Учеб. пособие. / Ю.К. Меньшаков – Москва : МГТУ им. Н.Э. Баумана, – 2011. – 339 с.

Додаткова

6. Анин Б.Ю. Защита компьютерной информации / Б.Ю. Анин. – Санкт Петербург : БХВ-Петербург, 2000. – 384 с.

7. Детлаф А. А. Курс физики: учеб. Пособ. для втузов, 4-е изд., испр. / А. А. Детлаф, Б. М. Яворский. – Москва: Высшая школа, 2002. – 718 с.

8. Пасечник И.П. Характеристики сейсмических волн при ядерных взрывах и землятресениях. Москва :. «Наука». – 1970. – 132 с.

9. Электроакустика и звуковое вещание: Учебное пособие для вузов / И.А. Алдошина, Э.И. Вологдин, А.П. Ефимов и др.; Под ред. Ю.А. Ковалгина. – Москва : Горячая линия – Телеком, Радио и связь, 2007. – 872 с.

Інформаційні ресурси в Інтернеті

10. Электронный учебник физики. [Електронний ресурс]. – Режим доступу : http://physbook.ru/.

11. Сайт ПНС ХНЕУ ім. С. Кузнеця. [Електронний ресурс]. – Режим доступу : https://pns.hneu.edu.ua/course/view.php?id=4351.

12. Технические средства и методы защиты информации: учебник для вузов [Електронний ресурс]. – Режим доступу : http://window.edu.ru/catalog/pdf2txt/611/-63611/33810?p_page=3.