МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

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

_____ М. В. Афанасьєв

ОСНОВИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

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(-и):
Корольов Р.В., к.т.н., доцент 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:

Подано тематичний план навчальної дисципліни й її змістовність за модулями та темами, вміщено плани лекцій і лабораторних занять, матеріал щодо закріплення знань (завдання для самостійної роботи, контрольні запитання), методичні рекомендації та оцінювання знань студентів.

На сучасному етапі серед основних реальних та потенційних загроз національній безпеці України в інформаційній сфері є розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави.

Серед загроз, які можуть призвести до розголошення інформації, за своїми небезпечними наслідками особливе місце займають несанкціонований доступ до інформації, яка обробляється та циркулює на об’єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, а також витік інформації технічними каналами.

Саме з метою протидії зазначеним загрозам в Україні створена та функціонує система технічного захисту інформації, яка дозволяє вирішувати практично весь комплекс завдань з технічного захисту інформації на об’єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах державних органів, підприємств, установ та організацій.

Система являє собою сукупність організаційних структур, поєднаних цілями і завданнями захисту інформації, нормативно-правової та матеріально-технічної бази і спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Мета навчальної дисципліни: метою дисципліни "Основи технічного захисту інформації” є отримання студентами необхідних базових знань, щодо порядку створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Основними завданнями вивчення дисципліни є систематизація інформації, щодо розроблення, впровадження та експлуатації систем технічного захисту інформації на об’єктах інформаційної діяльності.

Курс	**4**	
Семестр	**1**	
Кількість кредитів ECTS	**5**	
Аудиторні навчальні заняття	**лекції**	**32**
	семінарські, практичні	**–**
	лабораторні	**32**
Самостійна робота		**86**
Форма підсумкового контролю	**екзамен**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Основи криптографічного захисту	Проектування систем захисту мереж наступного покоління
Основи побудови та захисту сучасних операційних систем	
Комплексні системи захисту інформації	

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності	Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки
Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів
Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем	Здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж
Здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов	Виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп'ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу

3. Програма навчальної дисципліни

Змістовий модуль 1. Концептуальні засади забезпечення інформаційної безпеки України

Тема 1. Основні поняття та категорії. Інформаційна безпека як складова національної безпеки. Нормативно-правове забезпечення інформаційної безпеки.

Основні поняття, категорії, визначення і терміни. Види інформації за режимом доступу. Класифікація інформації у відповідності до Закону України "Про інформацію". Поняття технічного захисту інформації. Загрози безпеці інформації.

Змістовий модуль 2. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів її витоку.

Тема 2. Поняття технічного каналу витоку інформації. Організаційно-технічні заходи щодо технічного захисту інформації на об'єкті.

Класифікація технічних каналів витоку інформації. Класифікація видів інформації, що може бути об'єктом злочинних посягань. Загальний підхід до технічного захисту інформації. Фізичні основи утворення технічних каналів витоку інформації. Організаційно-технічні заходи щодо технічного захисту інформації на об'єкті.

Змістовий модуль 3. Методи та засоби блокування технічних каналів витоку інформації.

Тема 3. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами.

Основні загальні положення технічного захисту інформації. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації. Захист акустичної інформації від зняття радіозакладними пристроями. Методи пошуку радіозакладних пристроїв. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами.

Змістовий модуль 4. Методологія захисту інформації в комп'ютерних системах і мережах.

Тема 4. Кібербезпека і центр моніторингу та управління безпекою (SOC).

Відмінні риси різних прикладів подій кібербезпеки. Мотивація хакерів в конкретних подіях безпеки. Призначення центру моніторингу та управління безпекою (SOC).

Тема 5. Операційна система Windows. Забезпечення захисту кінцевих пристроїв, що працюють під управлінням ОС Windows.

Принципи роботи операційної системи Windows. Захист кінцевих пристроїв, що працюють під управлінням ОС Windows. Процедури налаштування і моніторингу ОС Windows.

Тема 6. Огляд ОС Linux. Основні завдання, пов'язані з інформаційною безпекою, на хості під управлінням ОС Linux.

Основні завдання адміністрування Linux. Основні завдання, пов'язані з інформаційною безпекою, на хості під управлінням ОС Linux. Інструменти для виявлення шкідливого ПО на хості під управлінням ОС Linux.

Тема 7. Мережеві протоколи Ethernet і IP.

Основні принципи передачі даних по мережі. Використання протоколів Ethernet, IPv4 та IPv6 для передачі даних по мережі.

Тема 8. Мережеві пристрої зв'язку. Інфраструктура забезпечення мережевої безпеки.

Забезпечення обміну даними мережевими пристроями по дротової і бездротової мережі. Забезпечення безпеки мережі пристроями та службами.

Тема 9. Хакери та їх інструменти. Поширені загрози і атаки.

Процес розвитку мережевої безпеки. Типи інструментів атак, які використовуються хакерами. Шкідливе програмне забезпечення і поширені мережеві атаки.

Тема 10. Моніторинг мережі і засоби моніторингу. Атаки на базові функції.

Способи проведення моніторингу мережі. Уразливості TCP/IP, що дозволяють проведення мережевих атак. Уразливості до атак поширених мережевих додатків та служб.

Тема 11. Підходи до захисту безпеки мережі. Управління доступом як способу захисту мережі.

Загальний опис політики безпеки, нормативних вимог та стандартів. Управління доступом як способу захисту мережі. Опис джерел інформації, використовуваних для повідомлення про виникаючі загрози безпеки мережі

Тема 12. Використання засобів шифрування і розшифрування даних. Криптографія із загальними ключами.

Засоби шифрування і розшифрування даних. Роль криптографії в забезпеченні цілісності та автентичності даних. Прінципи функціонування інфраструктури відкритих ключів.

Тема 13. Захист кінцевих пристроїв. Оцінка вразливостей кінцевих пристроїв.

Способи усунення шкідливого програмного забезпечення. Використання virustotal.com для формування звіту аналізу шкідливого програмного забезпечення. Методи безпечного управління пристроями для захисту даних і ресурсів

Тема 14. Технології та протоколи. Файли журналів.

Вплив технології забезпечення безпеки на моніторинг безпеки. Опис типів файлів журналів, що використовуються в моніторингу безпеки.

Тема 15. Оцінка попереджень. Робота з даними безпеки мережі.

Опис процесу оцінки попереджень. Використання інструментів вирішення Security Onion для дослідження подій безпеки мережі. Опис інструментів моніторингу мережі, що поліпшують управління робочими процесами

Тема 16. Моделі реагування на інциденти та їх обробка.

Класифікація події вторгнення з використанням ромбовидної моделі. Застосування до події інформаційної безпеки стандартів, зазначених в NIST 800-61r2.

Теми лабораторних робіт.

Лабораторна робота 1. Встановлення віртуальної машини CyberOps Workstation.

Лабораторна робота 2. Створення облікових записів користувачів. Контроль і управління системними ресурсами Windows.

Лабораторна робота 3. Навігація в файловій системі Linux, настройка повноважень.

Лабораторна робота 4. Вивчення перехоплених пакетів TCP та UDP використовуючи програму Wireshark.

Лабораторна робота 5. Вивчення трафіку DNS. Атака на базу даних mySQL.

Лабораторна робота 6. Шифрування та розшифрування даних за допомогою OpenSSL. Шифрування та розшифрування даних за допомогою fcrackzip.

Лабораторна робота 7. Витяг виконуваного файлу з PCAP. Інтерпретація даних HTTP та DNS для ізоляції хакера.

Лабораторна робота 8. Скомпрометований хост, ізольований за методикою 5 елементів.

4. 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. 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, 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 міні-екзамен 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 проблеми; 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

(вказати засоби оцінювання згідно з технологічною картою)

Теми змістового модуля				Лекційні заняття	Захист лабораторних робіт	Експрес-опитування	Екзамен	Усього
	1	**Тема 1**	1 тиждень	1				1
	2	**Тема 2**	2 тиждень	1	5			6
	3	**Тема 3**	3 тиждень	1				1
	4	**Тема 4**	4 тиждень	1	5	2		8
		Тема 5	5 тиждень	1				1
		Тема 6	6 тиждень	1	5			6
		Тема 7	7 тиждень	1				1
		Тема 8	8 тиждень	1	5			6
		Тема 9	9 тиждень	1				1
		Тема 10	10 тиждень	1	5			6
		Тема 11	11 тиждень	1				1
		Тема 12	12 тиждень	1	5			6
		Тема 13	13 тиждень	1				1
		Тема 14	14 тиждень	1	5			6
		Тема 15	15 тиждень	1				1
		Тема 16	16 тиждень	1	5	2		8
		Екзамен					40	40
Усього				16	40	4	40	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. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
2. В.А.Хорошко, А.А.Чекатков. Методы и средства защиты информации.: К. - Юниор, 2003. – 504 с.
3. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997.
4. ДСТУ 3396.0-96.Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.
5. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.
6. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. № 200.
7. НД ТЗІ 1.1-002-99.Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.
8. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
9. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
10. НД ТЗІ 3.3-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації»
11. Положення про державний контроль за станом технічного захисту інформації від 16.05.2007 №87

12. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006.

5.2 Інформаційні ресурси в Інтернеті

13. 1.https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi//